
The Belden Firewall (TBF) Documentation

Release 25.07.1

Belden Inc.

Aug 28, 2025

CONTENTS:

1	General Explanations	1
1.1	Introduction	1
1.2	Architecture	1
1.3	Technology Stack	1
1.4	Default login	2
1.5	Default Firewall User	2
1.6	Breadcrumb	2
1.7	Search	2
1.8	Supported Browser	2
1.9	Current Appliances	3
1.10	Release Schedule	3
1.11	Default Firewall Rules	3
1.12	Default Services	4
2	XDP Accelerator	6
2.1	XDP Speedups	7
2.2	XDP DDoS Protection	8
3	Appliances User Manuals	9
3.1	VT AIR 100	9
3.2	VT AIR 300	22
3.3	VT AIR 310	39
3.4	VT AIR 500	56
3.5	VT AIR 600	68
3.6	VT AIR 1200	82
3.7	VT AIR 1500	95
3.8	VT AIR Amazon AWS	108
3.9	VT AIR Azure	131
3.10	IAF 240	153
4	Portal	154
4.1	First Steps	154
4.2	User Management	155
4.3	Device Management	156
4.4	Remote Access	158
4.5	Support	160
4.6	Downloads	160
5	CLI	161
6	Console Access	167
6.1	SSH	167
6.2	Serial	169
7	Dashboard	171

7.1	States Widget	173
7.2	Security Widget	173
8	System Settings	175
8.1	Global Settings	175
8.2	Licence	185
8.3	Portal Settings	185
8.4	Addons	186
8.5	Copyright	187
9	User Authentication	188
9.1	User	188
9.2	Groups	191
9.3	Authentication Server	192
9.4	Identity Awareness	194
10	Interfaces	196
10.1	Interfaces General	196
10.2	Assign Interfaces	197
10.3	Configure Interfaces	198
10.4	VLAN	201
10.5	QinQ	202
10.6	Bridge	203
10.7	Bond (Link Aggregation)	208
10.8	Tunnel	210
10.9	PPPoE	213
10.10	PPP	214
10.11	MacVLAN	216
10.12	SHDSL	217
10.13	VDSL	219
10.14	VRF	220
10.15	VXLAN	221
10.16	Interface Groups	223
11	Firewall	224
11.1	Firewall General	224
11.2	Network Objects	227
11.3	Firewall Rules (Forward and Input)	230
11.4	Global Firewall Rules (Forward and Input)	235
11.5	Bridge Firewall Rules (Forward)	235
11.6	DNAT (Prerouting)	237
11.7	SNAT (Postrouting)	240
11.8	BiNAT (Prerouting + Postrouting)	243
11.9	Firewall Rules Advanced	244
11.10	Firewall Time Control	246
11.11	App Control	246
11.12	DDoS Rules	252
11.13	Divider	253
11.14	Learning Mode	254
12	Enforcer	255
12.1	Enforcer General	255
12.2	AMP	255
12.3	DNP3	261
12.4	ENIP	273
12.5	GOOSE	294
12.6	IEC104	296
12.7	Modbus	300
12.8	OPC	304

13 Certificates	307
13.1 Certificate	307
13.2 CA	308
13.3 CSR	308
13.4 CRL	309
13.5 Let's Encrypt	310
14 Virtual IPs	313
14.1 VRRP	313
14.2 IP Alias	314
14.3 Custom VRRP Scripts	314
15 DynDNS	315
15.1 DynDNS	315
16 Routing	316
16.1 Routes	316
16.2 Routing Tables	317
16.3 Load Balancing	318
16.4 Gateway	319
16.5 MPLS	322
16.6 Dynamic	324
16.7 BFD	325
16.8 BGP	326
16.9 ISIS	328
16.10 OSPF	329
16.11 OSPFv6	331
16.12 Access List	333
16.13 Prefix List	333
16.14 Route Map	334
16.15 Use Cases	335
17 Services	337
17.1 Apcupsd	337
17.2 802.1X Authenticator	339
17.3 Avahi	340
17.4 Captive Portal	341
17.5 Cron	345
17.6 DHCP & RA	346
17.7 DNS	350
17.8 HAProxy	355
17.9 IGMPProxy	362
17.10 Intrusion Detection	362
17.11 Netflow	366
17.12 Ntopng	367
17.13 NTP	369
17.14 QoS	370
17.15 SNMP	372
17.16 Startup Scripts	373
17.17 Web Filter	374
17.18 UPnP & NAT-PMP	381
17.19 Web Application Firewall	382
17.20 ZeroTier	385
18 VPN	386
18.1 IPsec	386
18.2 OpenVPN	396
18.3 WireGuard	405
18.4 WebVPN	409

19 Apps	414
19.1 Settings	414
19.2 Images	415
19.3 Volumes	415
19.4 Containers	415
19.5 Running a new Application	416
19.6 Templates	418
19.7 Examples	418
20 High Availability	421
20.1 General High Availability	421
20.2 Configuration Sync	425
20.3 States Sync	426
20.4 VRRP Shared Virtual IP Address	426
20.5 DHCP High Availability	428
20.6 Setup Examples	429
21 Diagnostics	431
21.1 Diagnostics General	431
21.2 ARP & ND	431
21.3 Audit Log	432
21.4 802.1X Authenticator	433
21.5 BFD	433
21.6 BGP	434
21.7 Bond	434
21.8 Bridge	435
21.9 Captive Portal	435
21.10 DDoS	436
21.11 Debug Report	436
21.12 DHCP	437
21.13 DNS	439
21.14 DNS Domain	440
21.15 Dynamic Routing	440
21.16 Firewall	441
21.17 Gateways	443
21.18 GUI Logins	444
21.19 Hard Drives	444
21.20 HASync	447
21.21 Host Connections	447
21.22 Identity Awareness	448
21.23 Interfaces	448
21.24 Intrusion Detection	450
21.25 IPsec	453
21.26 ISIS	454
21.27 Logging	455
21.28 Cellular	456
21.29 MDRaid	458
21.30 MPLS	459
21.31 NTP	460
21.32 OpenVPN	461
21.33 OSPF	462
21.34 OSPFv6	462
21.35 QoS	462
21.36 Routes	463
21.37 Services	463
21.38 SFP	464
21.39 SHDSL	465
21.40 States	466

21.41 STP	467
21.42 Sysstat	468
21.43 System Actions	469
21.44 UPNP NAT	470
21.45 VDSL	470
21.46 Virtual IPs	471
21.47 VRF	473
21.48 VXLAN	473
21.49 Web Filter	474
21.50 Web Application Firewall	476
21.51 WireGuard	477
21.52 Worker Log	478
21.53 XDP	478
21.54 ZeroTier	479
22 Tools	481
22.1 ARPing	481
22.2 Backup & Restore	481
22.3 Web Console	482
22.4 Factory Defaults	483
22.5 File Manager	483
22.6 Iftop	483
22.7 LLDP	483
22.8 Patch	484
22.9 Ping	484
22.10 Restart	485
22.11 Script	485
22.12 Setup Wizard	486
22.13 Shutdown	486
22.14 TCPDump	486
22.15 Templates	488
22.16 Top	489
22.17 Traceroute	489
22.18 Wake-on-LAN	489
23 Configuration Examples	491
23.1 Windows Updates	491
23.2 IPv6 Multi WAN	491
23.3 Custom Scripts	492
24 API	494
24.1 General	494
25 Commands	497
25.1 Speedtest	497
25.2 Command Line Tools	498
25.3 XDP Command Line Tools	498
26 Roadmap	500
27 Changelog	501
27.1 Version 25.07	501
27.2 Version 25.04	501
27.3 Version 25.01	501
27.4 Version 24.10	502
27.5 Version 24.07	502
27.6 Version 24.04	503
27.7 Version 24.01	504
27.8 Version 23.10	505

27.9	Version 23.07	507
27.10	Version 23.04	508
27.11	Version 23.01	509
27.12	Version 22.10	509
27.13	Version 22.07	509
27.14	Version 22.04	510
27.15	Version 22.01	510
27.16	Version 21.10	511
27.17	Version 21.07	512
27.18	Version 2.2.9	512
27.19	Version 2.2.8	512
27.20	Version 2.2.7	513
27.21	Version 2.2.6	513
27.22	Version 2.2.5	514
27.23	Version 2.2.4	514
27.24	Version 2.2.3	515
27.25	Version 2.2.2	515
27.26	Version 2.2.1	516
27.27	Version 2.2.0	516
27.28	Version 2.1.3	516
27.29	Version 2.1.2	516
27.30	Version 2.1.1	517
27.31	Version 2.1.0	517
27.32	Version 2.0.0	517
27.33	Version 1.6.0	517
27.34	Version 1.5.0	518
27.35	Version 1.4.0	518
27.36	Version 1.3.0	518
27.37	Version 1.2.0	519
27.38	Version 1.1.0	519
27.39	Version 1.0.1	519
27.40	Version 1.0.0	519

28 Indices and tables

520

GENERAL EXPLANATIONS

1.1 Introduction

TBF Next Gen Firewall is a Linux based firewall system delivering high firewall throughput while containing large number of Features to manage your network.

TBF is equipped with a modern management WebGUI, REST API and command line.

1.2 Architecture

TBF runs on the Linux Operating System and it utilizes a custom Linux Kernel for maximum compatibility and network speed.

1.3 Technology Stack

TBF is designed and built using open source software projects including:

- [SNMPD](#) for SNMP
- [FRR](#) for routing protocols
- [Kea](#) for DHCP services
- [Unbound](#) for DNS
- [ntp.org](#) daemon for NTP
- [keepalived](#) for VRRP and HA Failover
- [Docker](#) for App Container
- [Suricata](#) for Intrusion Detection and App Control
- [Squid](#) as Web Filter
- [Coraza](#) as Web Application Firewall
- [HAProxy](#) as Reverse Proxy and Load Balancer
- [Apache Guacamole](#) as WebVPN
- [OpenVPN](#)
- [strongSwan](#) for IPsec key management
- [WireGuard](#)

1.4 Default login

The default login data for the WebGUI needs to be set the first time you log on. The WebGUI will force you to set a password for the default user **admin**.

For SSH or the console the user is **root**. The **root** and **admin** user share the same password, so you can use the SSH login only after the default has been set.

The initial password is private and the WebGUI is reachable at <https://192.168.1.1> .

Note: *VT AIR Amazon AWS* and *VT AIR Azure* have a different login mechanism

1.5 Default Firewall User

The following users are active on the firewall by default:

Name	Function	Description
admin	Web GUI Administrator	Webinterface Admin
hasync	Web GUI High Availability User	HA Config Sync User with random password
root	SSH Only User	Password is synced with admin user

1.6 Breadcrumb

Each page has a navigational breadcrumb with the current page in it. Depending on the page there are also additional shortcuts on the right upper corner.

Shortcuts include:

- Link to the Service Overview Page
- Link to the Service specific Diagnostic
- Link to the Logfile

1.7 Search

The search box in the upper navigation bar can search the menu and return page results. It **does not** search through **any saved data**. If you want to find a menu entry fast it is a good tool to use.

1.8 Supported Browser

TBF supports Chrome, Edge, Firefox and Safari. The Internet Explorer is not a supported browser and might have errors showing GUI features.

1.9 Current Appliances

Desktop

- *VT AIR 100*
- *VT AIR 500*
- *VT AIR 600*

Rack

- *VT AIR 1200*
- *VT AIR 1500*

Industrial

- *IAF 240*
- *VT AIR 300*
- *VT AIR 310*

1.10 Release Schedule

TBF is released quarterly and the version number reflects the month and year of the release. For example the release 2021.07.1 is released in July 2021.

Releases are in January, April, July and October and are numbered like the following by replacing YYYY with the year of the release:

- YYYY.01
- YYYY.04
- YYYY.07
- YYYY.10

The Kernel is updated on the 04 (April) and 10 (October) release. There are exceptions like critical security vulnerabilities or other major reasons where we are forced to release a Kernel update outside of the release schedule.

1.11 Default Firewall Rules

Only the **LAN Interface** has default firewall rules enabled.

Protocol	Source IP	Source Port	Destination IP	Destination Port	Description
TCP	Any	Any	LAN Address	22, 80, 443	Anti Lockout Rule
TCP/UDP	LAN Network	Any	LAN Address	53, 853	DNS Server
ICMP	LAN Network	-	LAN Address	-	ICMP to TBF
Any	Any	Any	Private Networks	Any	Access to Private IPs v4 and v6
Any	Any	Any	NOT Private Networks	Any	Access to Public IPs v4 and v6

The **WAN Interface** blocks all Traffic and has an explicit extra Firewall Rule to block Private IPs.
Please refer to the open ICMP and ICMPv6 ports below for all Interfaces.

1.12 Default Services

The following tables shows the Services and their open ports that are enabled in factory default settings on the TBF:

Service	Port	Protocol	Default Firewall Rule	Active Interface	Description
DNS	53	TCP and UDP	Yes on LAN Interface	LAN	DNS Server
DNS	853	TCP and UDP	Yes on LAN Interface	LAN	DNS Server TLS
HTTP	80	TCP	Yes on LAN Interface	Any	Web Server
HTTPS	443	TCP	Yes on LAN Interface	Any	Web Server
DHCP	67	UDP	Yes on LAN Interface (except IAF 240)	LAN	DHCP Server
SSH	22	TCP	Yes on LAN Interface	Any	SSH Server
NTP	123	UDP	No Blocked	Any	NTP Server
ICMP		ICMP	Yes on LAN Interface + See Table below	N/A	ICMP Messages
ICMPv6		ICMPv6	See Table below	N/A	ICMPv6 Messages

Open ICMP Types to the TBF Firewall:

ICMP Type	Input Interface	Description
All	LAN	LAN ICMP to TBF
Destination unreachable (3)	ALL	Destination Unreachable Message
Time exceeded (11)	ALL	Time exceeded Message
Parameter problem (12)	ALL	Parameter Problem

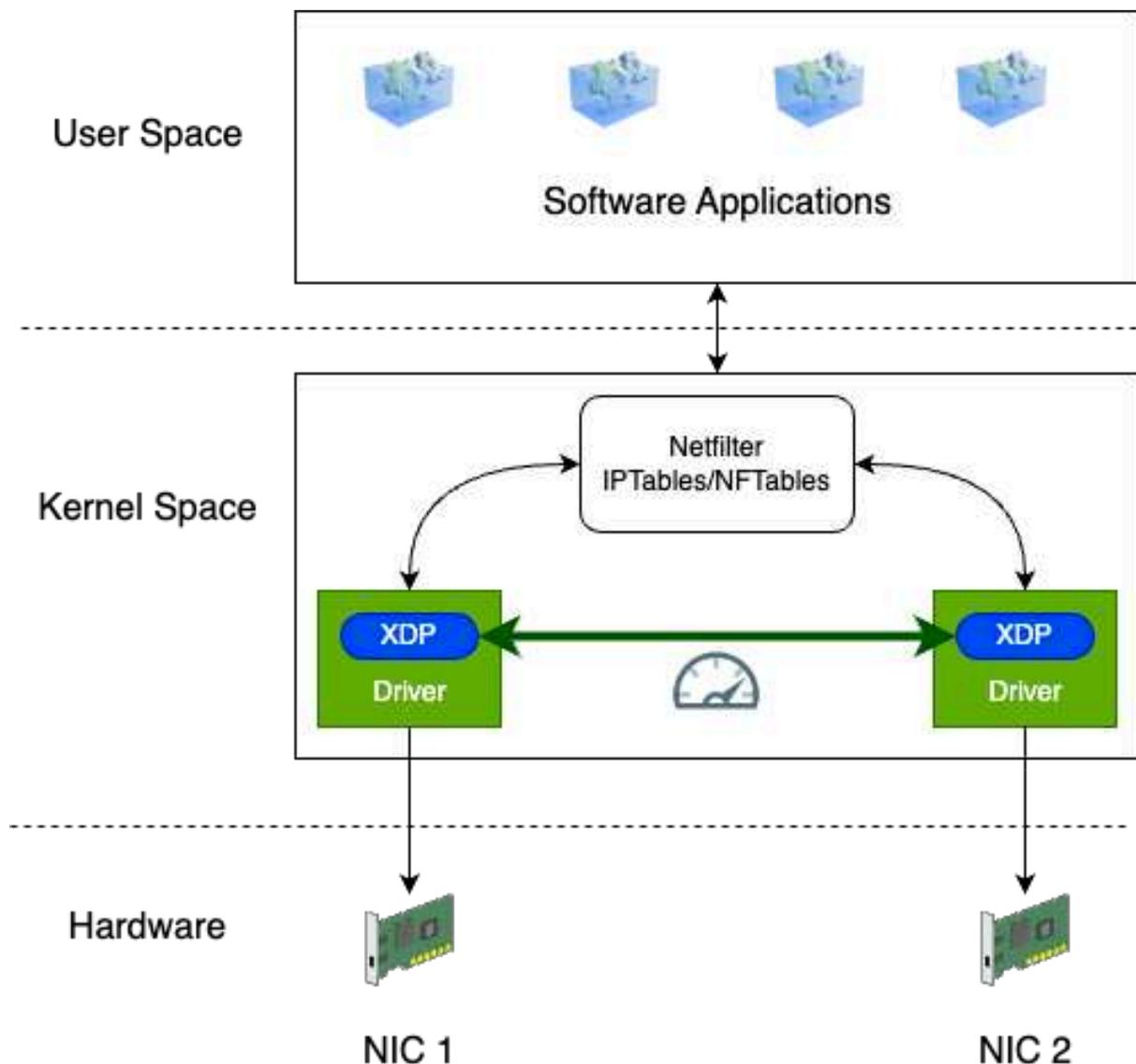
Open ICMPv6 Types to the TBF Firewall:

ICMPv6 Type	Input Interface	Description
Destination unreachable (1)	ALL	Destination Unreachable Message
Packet Too Big (2)	ALL	Packet Too Big
Time exceeded (3)	ALL	Time exceeded Message
Parameter problem (4)	ALL	Parameter Problem
Neighbor Solicitation (135)	ALL	Neighbour Solicitation
Neighbor Advertisement (136)	ALL	Neighbour Advertisement
Multicast Listener Query (130)	ALL	Multicast Listener Query
Multicast Listener Report (131)	ALL	Multicast Listener Report
Multicast Listener Done (132)	ALL	Multicast Listener Done
Multicast Listener Report v2 (143)	ALL	Multicast Listener Report
Multicast Router Advertisement (151)	ALL	Multicast Listener Report
Multicast Router Solicitation (152)	ALL	Multicast Listener Report
Multicast Router Termination (153)	ALL	Multicast Listener Report
Echo Reply (129)	ALL (fe80::/10, ff02::/16 <-> fe80::/10, ff02::/16)	Link Local Only
Router Solicitation (133)	ALL (fe80::/10, ff02::/16 <-> fe80::/10, ff02::/16)	Link Local Only
Router Advertisement (124)	ALL (fe80::/10, ff02::/16 <-> fe80::/10, ff02::/16)	Link Local Only

XDP ACCELERATOR

By combining XDP (eXpress Data Path) and eBPF (extended Berkeley Packet Filter), a program can be written that outsources the filtering of network traffic to the NIC driver (Network Interface Card) for lightning fast packet processing. The eBPF program is attached directly to the NIC driver to process network data at a very low level. eBPF is used to implement the network traffic logic.

This allows network data processing to be performed directly in the NIC driver without the data having to traverse the entire Linux kernel, resulting in faster processing and better performance.



TBF XDP is an add-on to nftables and accelerates connections by a **factor of 5** after they have been

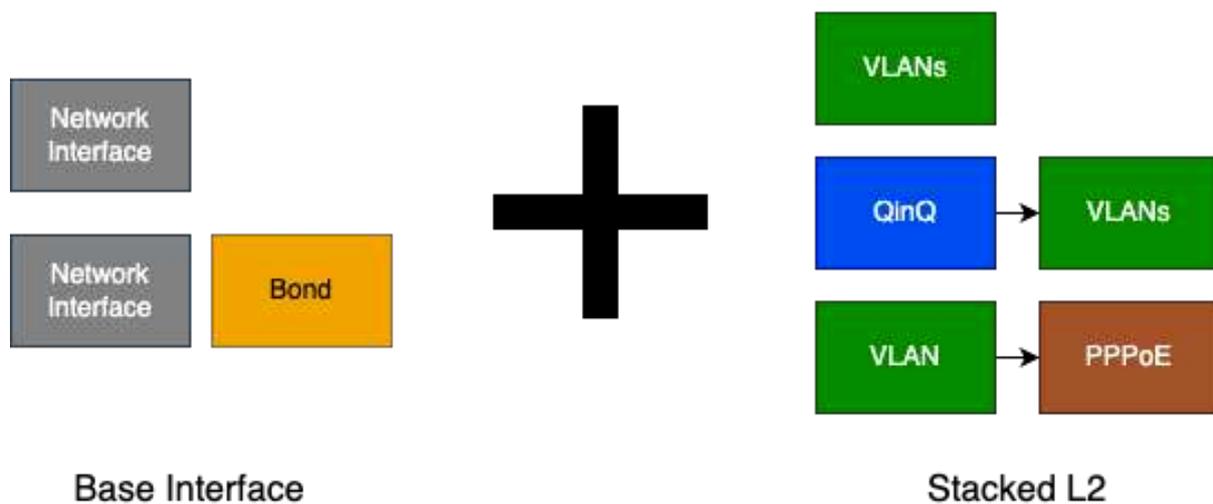
confirmed and allowed by the firewall rules. This allows for the traditional and comprehensive protection of nftables and the speed of XDP, the best of both worlds.

Our TBF XDP/eBPF offloader is a powerful tool that can handle a variety of network traffic scenarios. It supports both TCP and UDP traffic, the two most common protocols on the Internet. This means that the offloader can handle a wide range of applications such as web browsing, file transfers, and video streaming.

In addition, TBF XDP can handle **SNAT** (Source Network Address Translation), **DNAT** (Destination Network Address Translation) and **routing**. SNAT and DNAT are techniques to modify the source and destination addresses of network packets, respectively, while routing is the function that directs the packets between different networks. By supporting these features, our offloader provides flexible and powerful network filtering capabilities.

TBF XDP also supports **VLAN** (Virtual LAN), **QinQ** (Dual Tagged VLAN) and **PPPoE** (Point-to-Point Protocol over Ethernet) connections.

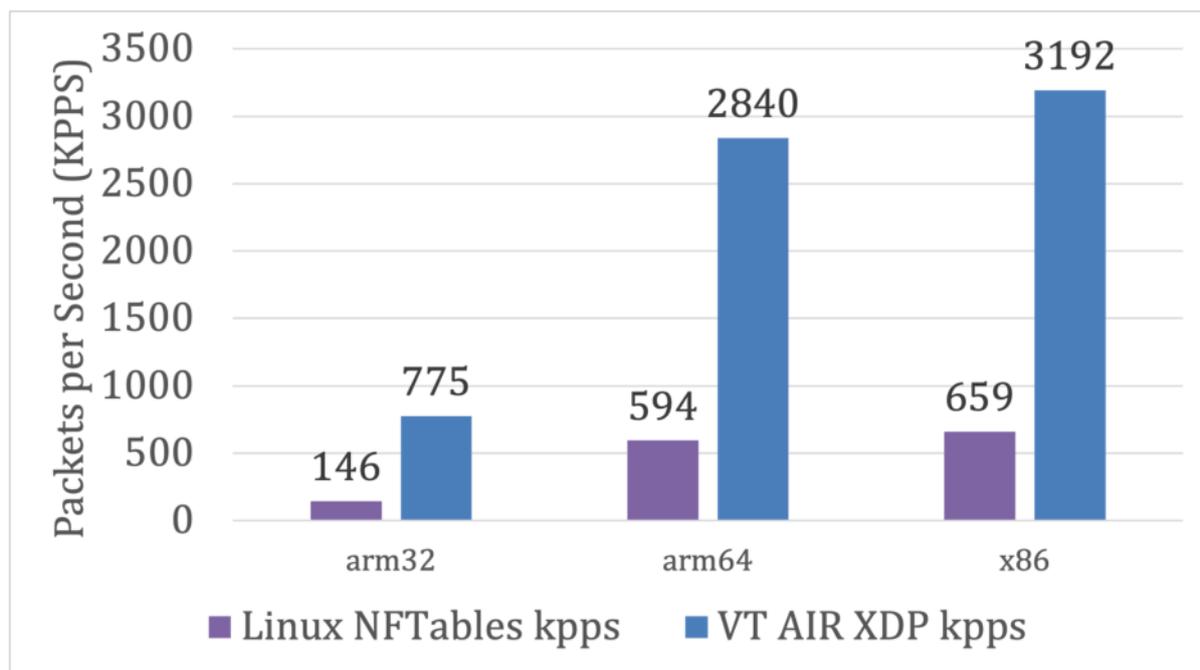
Stacked Interfaces



2.1 XDP Speedups

We tested our TBF XDP against a normal nftables firewall. For the test we used three different devices on three different architectures.

Device	CPUs	NFTables pps	TBF XDP pps	Speedup
TBF 100 (armhf)	2x Cortex v7	146 Kpps	775 Kpps	5,3
TBF 600 (arm64)	4x A72	594 Kpps	2840 Kpps	4,8
TBF 500 (x86)	4x Intel Atom C3558	659 Kpps	3192 Kpps	4,8



2.2 XDP DDoS Protection

TBF XDP is also capable of blocking DDoS traffic at very high rates. This is an important capability for networks at high risk of DDoS attacks, such as hosting environments or critical infrastructure, popular websites, or other high-value targets. By using our offloader to block DDoS attacks, network operators can help keep their networks running smoothly and avoid costly downtime.

APPLIANCES USER MANUALS

3.1 VT AIR 100

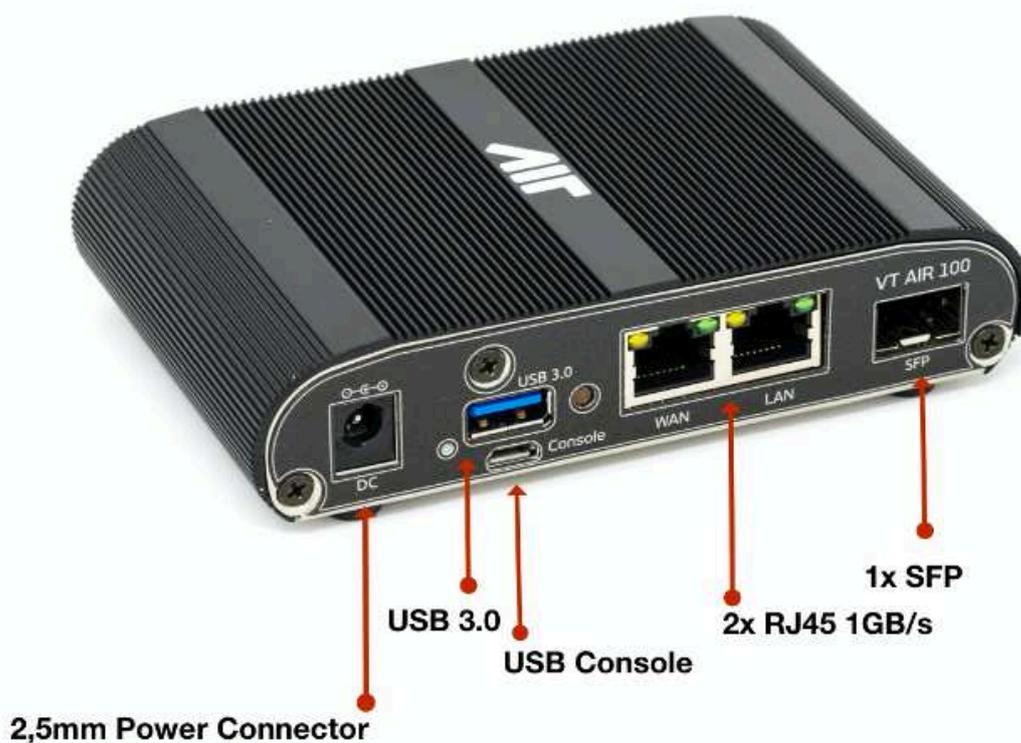


3.1.1 Overview

Summary of Features

CPU	armhf (Marvell ARMADA 388)
CPU Cores	2 Cores
NIC	1x 1GbE SFP Port 2x 1Gbps RJ45
SSD	8 GB eMMC
RAM	2 GB DDR3
Expansion	None
Console-Port	USB
USB Ports	1x USB 3.0 ports
Form factor	Desktop
Power	9 - 32V via 1x 2.5mm DC plug
Environment	0°C to 35°C Operating Temp
Dimensions	125 mm x 80 mm x 30 mm
Certificates	CE, FCC, RoHS, UL, IEC-60950
Software	VT AIR Linux

3.1.2 External Connectors



Certified Cables

The following is a list of industry-standard cables, sorted by type, with the necessary compliance requirements that have been proven to work well with the VT AIR product family.

These examples are the cables which Voleatech uses for testing and should provide enough information to source products from your preferred cable vendor.

- Ethernet cable: Monoprice 24AWG Cat6A 500MHz STP (max. 30m)
- USB Cable: SuperSpeed USB 3.0 Type A Male to Male Cable
- USB Console Cable: USB 2.0 Micro Type A Male to USB 2.0 Type A Male Cable

USB Connector

The front USB connector supports USB 3.0, connector type A. It can deliver up to 500 mA of power.

3.1.3 Packaging

The following items will be in the packaging of your VT AIR 100. Please make sure to check all items upon arrival of the device:

- VT AIR 100 Device in the enclosure
- Power adapter - 100-120/220-240 Vac 50/60 Hz US or EU plug
- USB Console Cable: USB 2.0 Type A Male to USB 2.0 Micro B Male Cable

3.1.4 Ports

Front Connectors

Network Ports		
eth0 (WAN)	eth1 (LAN)	eth2 (SFP)

Label	Software Name	Features
WAN	eth0	RJ45 1000/100/10 Mbit/s
LAN	eth1	RJ45 1000/100/10 Mbit/s
SFP	eth2	SFP 1000 Mbit/s

The RJ45 ports support Autonegotiation and Full Duplex or Half Duplex on all speeds.

The SFP Port supports the following Modules:

- 1Gb BaseT/SR/LR/CR

There is no vendor lock for SFP modules. You can use any Module that conforms to the standard.

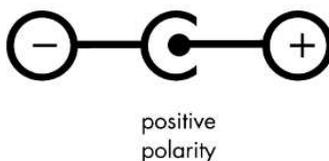
3.1.5 Power

The VT AIR 100 has 1 power connector:

- 9 - 32VDC 5.5mm x 2.5 mm cylindrical barrel connector

9 - 32VDC barrel connector

A suitable external power supply must be connected to the DC power socket, which has the dimensions 5.5 mm x 2.1 mm cylindrical barrel connector. The power supply must be between 9 and 32VDC. Recommended values are: 12VDC/2A (no more than 5A). Please note that the DC jack must have positive polarity in the center pin:



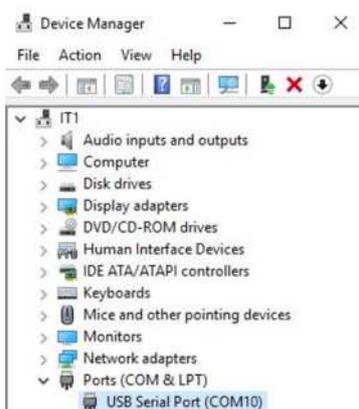
Warning: Please be aware that the maximum temperature for the barrel connector is 40°C.

3.1.6 USB Console

The appliance has a UART to USB bridge allowing convenient connection to the device console. Such serial console connection is of USB-to-UART type. The connection speed should be set to 115200 bps. All modern Operating Systems have a driver for the UART.

Windows

First you have to locate the COM Port number. Open the Device Manager and expand the section for Ports (COM & LPT). Look for an entry with a title such as USB Serial Port. A label is next to the name (COMX) where X is a number.



MacOSX

In OSX the device shows up at /dev/tty.usbserial-XXXXXX where X is a series of numbers and letters.

Linux

In Linux the device shows up at /dev/ttyUSBX where X is a number. You can also have a look at the output of dmesg to locate the newly connected device.

Terminal Program

A terminal program is required to open the connected serial port. We recommend:

OS	Program
Windows	Putty
MacOSX	Screen, Serial
Linux	Screen

First Connection to TBF Appliance

All TBF Appliances have a default LAN IP Address of *192.168.1.1* and the DHCP Server is active on LAN. Please make sure to locate the *LAN* interface of your appliance in the manual.

Connect your computer to the LAN Interface and receive an IP Address from the DHCP Server. It will be in the 192.168.1.X range.

After receiving the IP Address open a supported browser and navigate to **https://192.168.1.1** A certificate warning will appear, since the TBF is using a self signed certificate. Please accept the certificate and continue to the page.

You will now be presented with the TBF login screen and you can use the default User and Password to login.

Note: User: admin Password: vtair

Please change the password after the first login.

3.1.7 VT AIR Reinstallation

Your VT AIR device comes pre-installed with its operating system. Should you ever need to reinstall the VT AIR operating system follow this guide.

Download the Installer File

You can download the installer file from your Portal (see [Downloads](#) for details). Make sure to download the file for your specific model/architecture.

USB Flash Drive Preparation

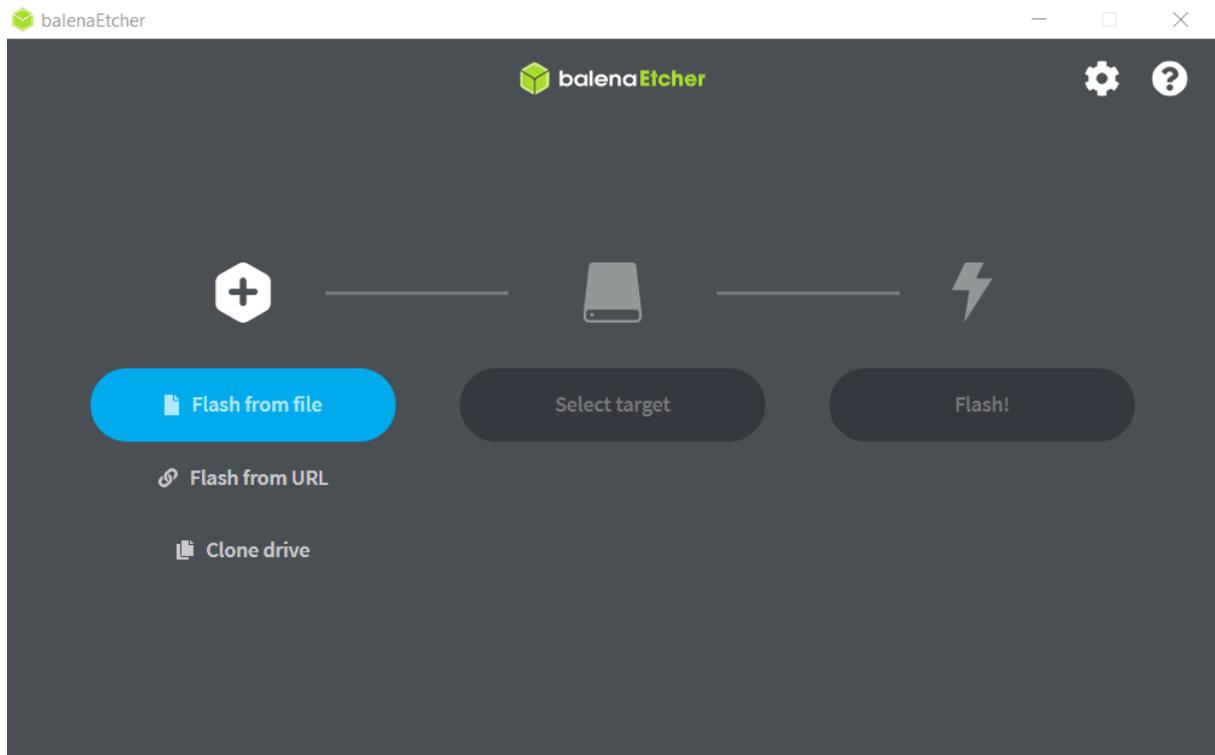
Once you downloaded the file make sure your USB flash drive is at least 2 GB in size. Also backup all your files from the USB flash drive since it will be formatted in the process and all files on it will be deleted.

Download the Software

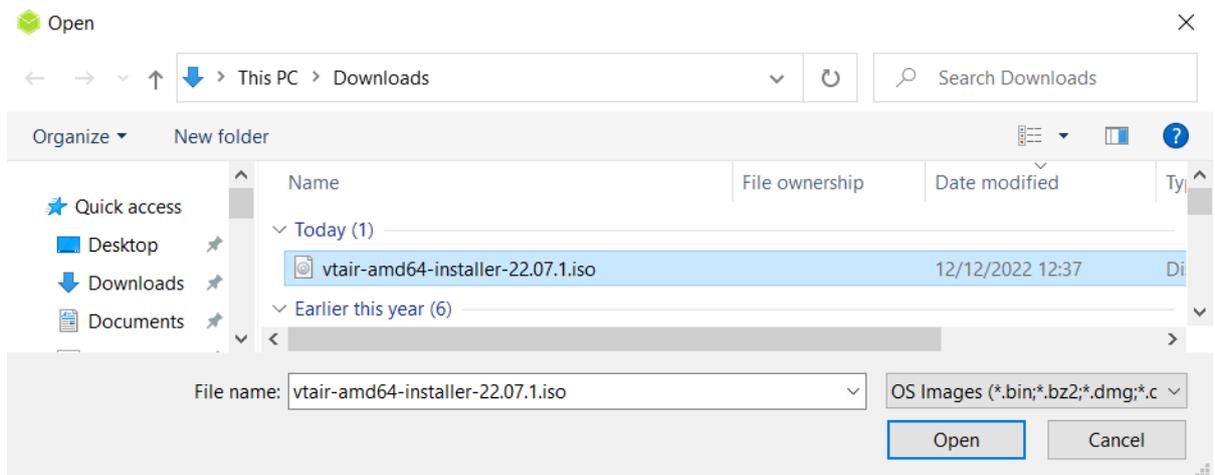
Download and install the software *balenaEtcher* from www.balena.io/etcher. It is available for Windows, macOS and Linux. Select the software for your specific operating system.

Use the Software

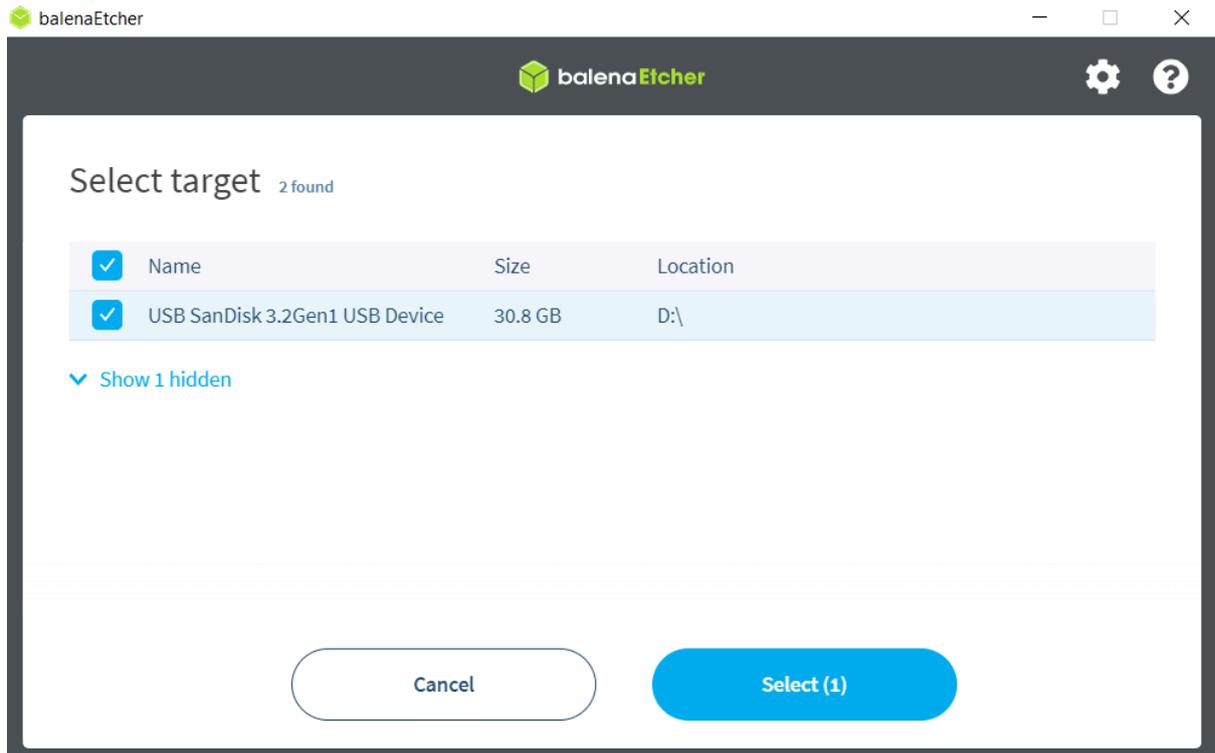
Insert your USB flash drive into the computer. Start the *balenaEtcher* software.



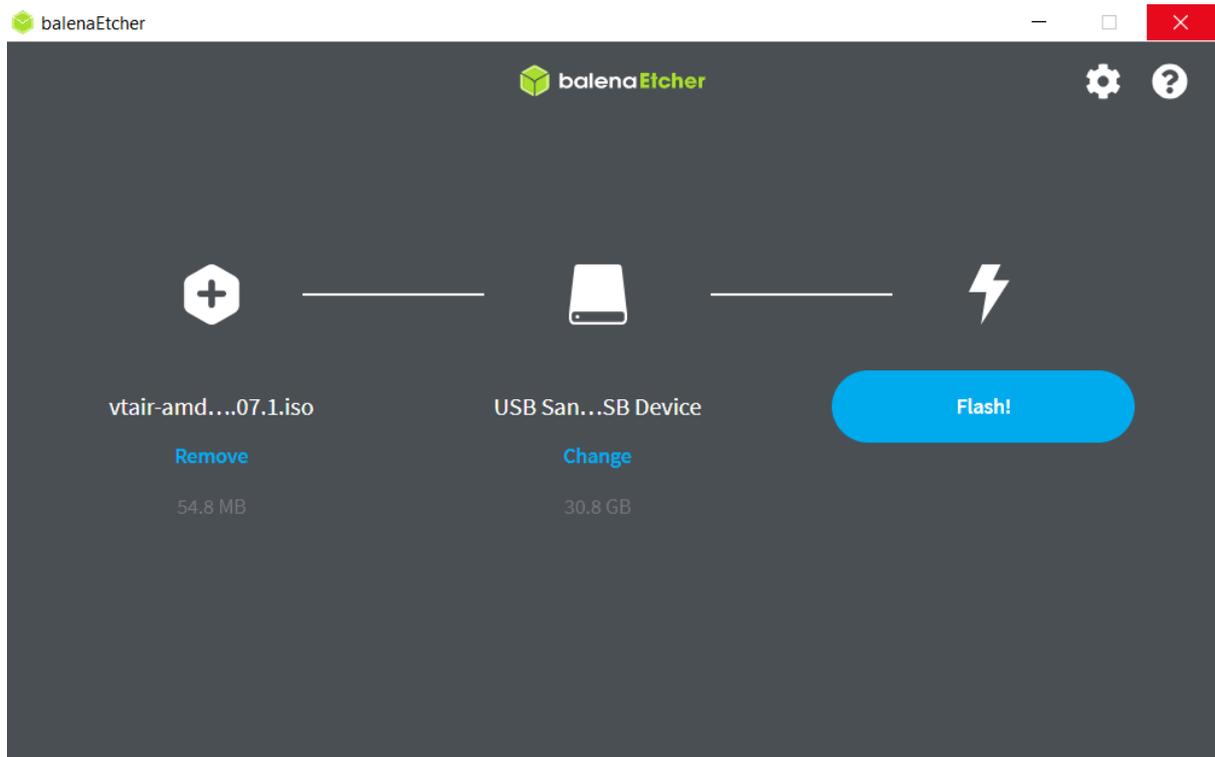
Press *Flash from file*



Select the downloaded installer file with the ending .iso



Select your USB flash drive as target



Press *Flash!* to complete and wait until the process is finished. Close the software and remove the USB flash drive from your computer.

Install the Software

Insert the USB flash drive with the new VT AIR operating system in your VT AIR's USB port.

Serial Console Installation

Connect the USB cable to the Console USB port of your VT AIR device and your computer. On your computer connect to your VT AIR's Console (see [Console Access](#)).

Type **"reboot"** to reboot the system. In the boot process you'll see a timer that you can interrupt by pressing any key. This gives you a shell from where you can reinstall your OS.

```
[ OK ] Reached target Unmount All Filesystems.
[ OK ] Stopped target Local File Systems (Pre).
[ OK ] Stopped Create Static Device Nodes in /dev.
[ OK ] Stopped Create System Users.
[ OK ] Stopped Remount Root and Kernel File Systems.
[ OK ] Reached target Shutdown.
[ OK ] Reached target Final Step.
[ OK ] Started Reboot.
[ OK ] Reached target Reboot.
[ 68.092735] reboot: Restarting system

U-Boot SPL 2020.01-dirty (Mar 15 2020 - 09:59:33 +0000)
High speed PHY - Version: 2.0
Detected Device ID 6828
board SerDes lanes topology details:
| Lane # | Speed | Type |
|-----|-----|-----|
| 0      | 3     | SATA0 |
| 1      | 0     | SGMII1 |
| 2      | 5     | PCIe1 |
| 3      | 5     | USB3 HOST1 |
| 4      | 5     | USB3 HOST0 |
| 5      | 0     | SGMII2 |
|-----|-----|-----|

PCIe, Idx 1: detected no link
High speed PHY - Ended Successfully
mv_ddr: mv_ddr-armada-18.09.2
DDR3 Training Sequence - Switching XBAR Window to FastPath Window
mv_ddr: completed successfully
Trying to boot from SPI

U-Boot 2020.01-dirty (Mar 15 2020 - 09:59:33 +0000)

SoC: MV88F6828-B0 at 1600 MHz
DRAM: 2 GiB (800 MHz, 32-bit, ECC not enabled)
MMC: mv_sdh: 0
Loading Environment from SPI Flash... SF: Detected w25q32 with page size 256 Bytes, erase size 4 KiB, total 4 MiB
*** Warning - bad CRC, using default environment

Model: VT AIR 100
Board: Voleatech VT AIR 100
Invalid EEPROM Header
SCSI: MVEBU SATA INIT
SATA link 0 timeout.
AHCI 0001.0000 32 slots 2 ports 6 Gbps 0x3 impl SATA mode
flags: 64bit ncq led only pmp fbss pio slum part sxs

Net:
Warning: ethernet@70000 using MAC address from ROM
eth1: ethernet@70000
Error: ethernet@30000 address not set.

Error: ethernet@34000 address not set.

Hit any key to stop autoboot: 0
=>
```

Type **"run install"** to run the OS installer from your USB stick. The installer runs without any user inputs.

3.1.8 LEDs

The VT AIR 100 has multiple LEDs. They are indicating for example power on, connection and port activity. Ethernet port related LEDs are embedded in the RJ45 connectors, while the power indicator LED is located next the serial port.

The RJ45 NIC LEDs are configured the following way:

LED Activity	Explanation
Off	No connection
Green Light Only	100Mbit/s Speed
Green and Yellow Light	1000Mbit/s Speed

3.1.9 Operational Data

Operational Voltage

Item	Voltage	Current	Ambient Temperature
Front barrel connector	9 - 32 VDC	2.0 A	Max. 35°C

Environmental Data

The environmental temperature data are based upon the component with the lowest available temperature. Please make sure to check which addons you ordered and make sure not to exceed the allowed ambient temperature.

Warning: Failure to comply with the allowed ambient temperature may void the warranty of your device.

Ambient Temperature	Minimum	Maximum
Base Device/LTE	0°C	35°C
Humidity (non-condensing)	10 %	90 %

Warning: Leave a minimum of 2cm of space on both sides of the device.

For ambient temperatures above 30°C, leave 5cm space on both sides of the device for air cooling to work properly.

3.1.10 Warranty Terms and Conditions

Voleatech GmbH guarantees its hardware products against defects in workmanship and material for a period of one (1) year from the date of shipment. Under warranty, the customer's sole remedy and Voleatech's sole liability shall be, at Voleatech's sole discretion, to either repair or replace the defective hardware product at no charge. This warranty is void if the hardware product has been altered or damaged by an accident, misuse or abuse or is not operated according to this manual. For additional information on warranty and related topics like RMA, please visit www.voleatech.de.

Disclaimer of Warranty THIS WARRANTY IS MADE IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESSED, OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR A SPECIFIC PURPOSE, NONINFRINGEMENT OR THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION, EXCEPT THE WARRANTY EXPRESSLY STATED HEREIN. THE REMEDIES SET FORTH

HEREIN SHALL BE THE SOLE AND EXCLUSIVE REMEDIES OF ANY CUSTOMER OR PURCHASER WITH RESPECT TO ANY DEFECTIVE PRODUCT.

Limitation on Liability UNDER NO CIRCUMSTANCES SHALL VOLEATECH GmbH BE LIABLE FOR ANY LOSS, DAMAGE OR EXPENSES INCURRED OR WITH RESPECT TO ANY DEFECTIVE PRODUCT. IN NO EVENT SHALL Voleatech GmbH BE LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES THAT CUSTOMER MAY SUFFER DIRECTLY OR INDIRECTLY FROM THE USAGE OF ANY PRODUCT. BY ORDERING THE VT AIR 100, THE CUSTOMER APPROVES THAT THE VT AIR 100, HARDWARE AND SOFTWARE, WAS THOROUGHLY TESTED AND HAS MET THE CUSTOMER'S REQUIREMENTS AND SPECIFICATIONS.

3.1.11 LEGAL NOTICE

Voleatech GmbH (hereinafter "Voleatech") products and services are sold subject to Voleatech terms and conditions of sale, delivery and payment supplied at the time of purchase order acknowledgement. Voleatech warrants the performance of its products according to actual specifications at the date of shipment. Voleatech reserves the right to make changes to its products and specifications or to discontinue any product, product line or service without prior notice. Customers should make sure to obtain in each case the latest version of relevant product information from Voleatech and to always verify for themselves that their requirements are met and reference is up to date. Product testing and all additional quality control techniques are utilized to the extent that Voleatech deems necessary to support their warranty and warranty terms. Therefore detailed testing of all parameters in any product is not necessarily performed in full unless required by law or regulation. In order to minimize risks that may be associated with customer products, applications or services, the customer must use adequate design and operating safeguards to minimize any possible hazards. Voleatech is not liable for any applications assistance or customer product design and thus it is the customer's sole responsibility to make the selection and usage of Voleatech products. Voleatech is not liable for any such selection or usage thereafter and neither is liable for the usage of any circuitry or components other than completely and entirely embodied in a Voleatech product. Furthermore Voleatech is not liable for its products commercial fit for any market segment envisioned by the customer. Voleatech products are not intended for use in life support systems, appliances, nuclear systems or systems where malfunction can reasonably be expected to result in personal injury, death or severe property or environmental damage. Any use of Voleatech's products by the customer for such purposes is completely at the customer's own risk. Voleatech does not grant any license -expressed or implied- on any patent right, copyright, mask work right, type or model protection or any other intellectual property right (IPR) of Voleatech covering or relating to any product combination, hardware, machine, software or process in which its products or services might be or are used. Any provision or publication of any third party's products or services does not constitute Voleatech's approval, license, warranty or endorsement thereof. Any third party trademarks contained in this document belong to the respective third party owner. Reproduction of content and information from Voleatech documents and manuals is permissible only if reproduction is without alteration and is accompanied by all associated copyright, proprietary and other notices (including this notice) and related conditions. Voleatech is not liable for any un-authorized alteration of such content and information or for any reliance related to alterations thereon. Any representations made, warranties given, and/or liabilities accepted by any person which differ from those contained in this manual or in Voleatech's standard terms and conditions of sale, delivery and payment are made, given and/or accepted at customer's own risk. Voleatech is not liable for any such representations, warranties or liabilities or for any reliance thereon by any person.

3.1.12 Regulatory

This chapter provides regulatory and compliance information about Voleatech's VT AIR 100 -related information. Product name: VT AIR 100

Safety Notice

Before you begin using this product, please read the following safety information. Attention to these warnings will help prevent personal injuries and damage to the products. It is your responsibility to use the product in an appropriate manner. This product is designed for use solely indoor environments or, if expressly permitted, also in the field and must not be used in any way that may cause personal injury or property damage.

You are responsible if the product is used for any intention other than its designated purpose or in disregard of Voleatech's instructions. Voleatech shall assume no responsibility for such use of the product. The product is used for its designated purpose if it is used in accordance with its product documentation and within its performance limits.

Safety Information and Notices

Never turn on or connect to power any equipment when there is evidence of mechanical damage, fire, exposure to water, or structural damage.

When not in use, avoid placing or storing the product in the following places or under the following conditions:

- Ambient temperature above 40°C
- Exposed to direct sunlight
- Humid or exposed to dust

Warning: This product does not contain any user replicable or serviceable parts. Do not take apart or attempt to service the product yourself.

Never remove the cover or any part of the housing of the product. The internal battery is not user replicable.

In the event of an equipment malfunction, all repairs must be performed either by Voleatech GmbH or by an authorized agent. It is the customer responsibility to report the need for service to Voleatech GmbH or to one of the authorized agents. For service information, contact Voleatech GmbH customer support.

Be careful not subject the product to strong impact.

If the product was subjected to a strong impact and/or falling over check carefully for any damage to the product. If such damage is observed the use of the product must be stopped immediately.

Operation

The product may be operated only under the operating conditions as specified by Voleatech GmbH. When the product is used for an extended period of time, and/or at high ambient temperature and/or exposed to direct sunlight it is normal for the product body to feel warm.

Avoid overheating the product. The product's ventilation should not be obstructed or blocked. If proper ventilation is not provided it can result in battery overheating or explosion of the battery resulting fire, burns or other injuries.

Stop using the product immediately if it emits smoke or a strange smell, or otherwise behaves abnormally.

Following are the required operating position and conditions:

- Do not place the product on unstable surfaces
- Do not place the product on elevated surface and secure it from falling from high places on passerby

- Do not place the product on heat-generating surface or near heat emitting devices or direct flame. Verify that there is sufficient clearance between the product and any other device exhaust warm air
- The product operating ambient range can be found at Environmental Data. Voleatech GmbH recommends that an ambient temperature of 0 to 40 °C (32 to 104 °F) and relative humidity of 30-50% is maintained during normal operation as this will result in better performance and longer life of the equipment. Temperature must not exceed the maximum temperature specified in Environmental Data.
- Do not expose the product to moisture or dust.
- The product is not liquid proof; therefore, the equipment must be protected against penetration by liquids. If the necessary precautions are not taken, the user may suffer electric shock or the product itself may be damaged, which can also lead to personal injury.
- Never use the product under conditions in which condensation has formed or can form in or on the product, e.g. if the product has been moved from a cold to a warm environment. Penetration by water increases the risk of electric shock.

AC/DC Adapter or Power Supply - Electrical Safety

The following information on electrical safety must be observed, failing to follow these instructions may result in electric shock, fire and/or serious personal injury or death.

Use only the adapter or power supply supplied with the product or adapter or power supply with the following specifications:

- Output voltage of 9V - 32V and current of at least 2A and not more than 3A

Prior to powering the product and plugging the adapter or power supply to the mains supply, always ensure that the nominal voltage setting on the adapter or power supply matches the nominal voltage of the AC supply network.

If extension cords or connector strips are implemented, they must be checked on a regular basis to ensure that they are safe to use.

Never use the adapter or power supply if the power cable is damaged. Check the power cable on a regular basis to ensure that it is in proper operating condition. By taking appropriate safety measures and carefully laying the power cable, you can ensure that the cable will not be damaged and that no one can be hurt by, for example, tripping over the cable or suffering an electric shock.

Do not insert the plug into sockets that are dusty or dirty. Insert the plug firmly and all the way into the socket. Otherwise, sparks that result in fire and/or injuries may occur.

Do not overload any sockets, extension cords or connector strips; doing so can cause fire or electric shocks.

Do not insert or remove the plug with wet hands.

Never remove the cover or any part of the housing of the adapter or power supply, doing so will expose circuits and components and can lead to electric shock, injuries, fire or damage to the product.

The adapter or power supply operating ambient temperature range is of 0 to 40°C / 32 to 104 °F (storage temp range: -20 to 60 °C / -04 to 140 °F) maximum operating altitude is 2000 m ASL.

Use suitable overvoltage protection to ensure that no overvoltage (such as that caused by a bolt of lightning) can reach the product. Otherwise, the person operating the product will be exposed to the danger of an electric shock.

The product is not liquid proof; therefore, the equipment must be protected against penetration by liquids. If the necessary precautions are not taken, the user may suffer electric shock or the product itself may be damaged, which can also lead to personal injury.

Never use the product under conditions in which condensation has formed or can form in or on the product, e.g. if the product has been moved from a cold to a warm environment. Penetration by water increases the risk of electric shock.

Prior to cleaning the product, disconnect it completely from the power supply. Use a soft, non-linting cloth to clean the product. Never use chemical cleaning agents such as alcohol, acetone or diluents for cellulose lacquers.

Electronic Emission Notices (EMC)

Federal Communications Commission Declaration of Conformity The following information refers to VT AIR 100. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Responsible Party: Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany

European Union - Compliance to the Electromagnetic Compatibility

(EMC) Directive or Radio Equipment Directive

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU (from 20 April, 2016) on the approximation of the laws of the Member States relating to electromagnetic compatibility.

Voleatech GmbH is not responsible for any radio or television interference caused by using other than specified or recommended cables and connectors or by unauthorized changes or modifications to this equipment.

Unauthorized changes or modifications could void the user's authority to operate the equipment.

WEEE and recycling statements

The WEEE marking on Voleatech GmbH products applies to countries with WEEE and e-waste regulations (for example, the European WEEE Directive). Appliances are labeled in accordance with local regulations concerning waste electrical and electronic equipment (WEEE).

These regulations determine the framework for the return and recycling of used appliances as applicable within each geography. This label is applied to various products to indicate that the product is not to be thrown away, but rather put in the established collection systems for reclaiming these end of life products.

Users of electrical and electronic equipment (EEE) with the WEEE marking must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to them for the return, recycle and recovery of WEEE and to minimize any potential effects of EEE on the environment and human health due to the presence of hazardous substances. Voleatech GmbH electrical and electronic equipment (EEE) may contain parts and components, which at end-of-life might qualify as hazardous waste.

EEE and waste electrical and electronic equipment (WEEE) can be delivered free of charge to the place of sale or any distributor that sells electrical and electronic equipment of the same nature and function as the used EEE or WEEE.



Restriction of Hazardous Substances (RoHS) European Union RoHS

This product, with included parts (cables, cords, and so on) meets the requirements of Directive 2011/65/EU and directive 2015/863/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment ("RoHS recast" or "RoHS 2").

3.1.13 Contact Information and Resources

Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany

www.voleatech.de info@voleatech.de +49 7121 539 550

3.2 VT AIR 300



3.2.1 Overview

Summary of Features

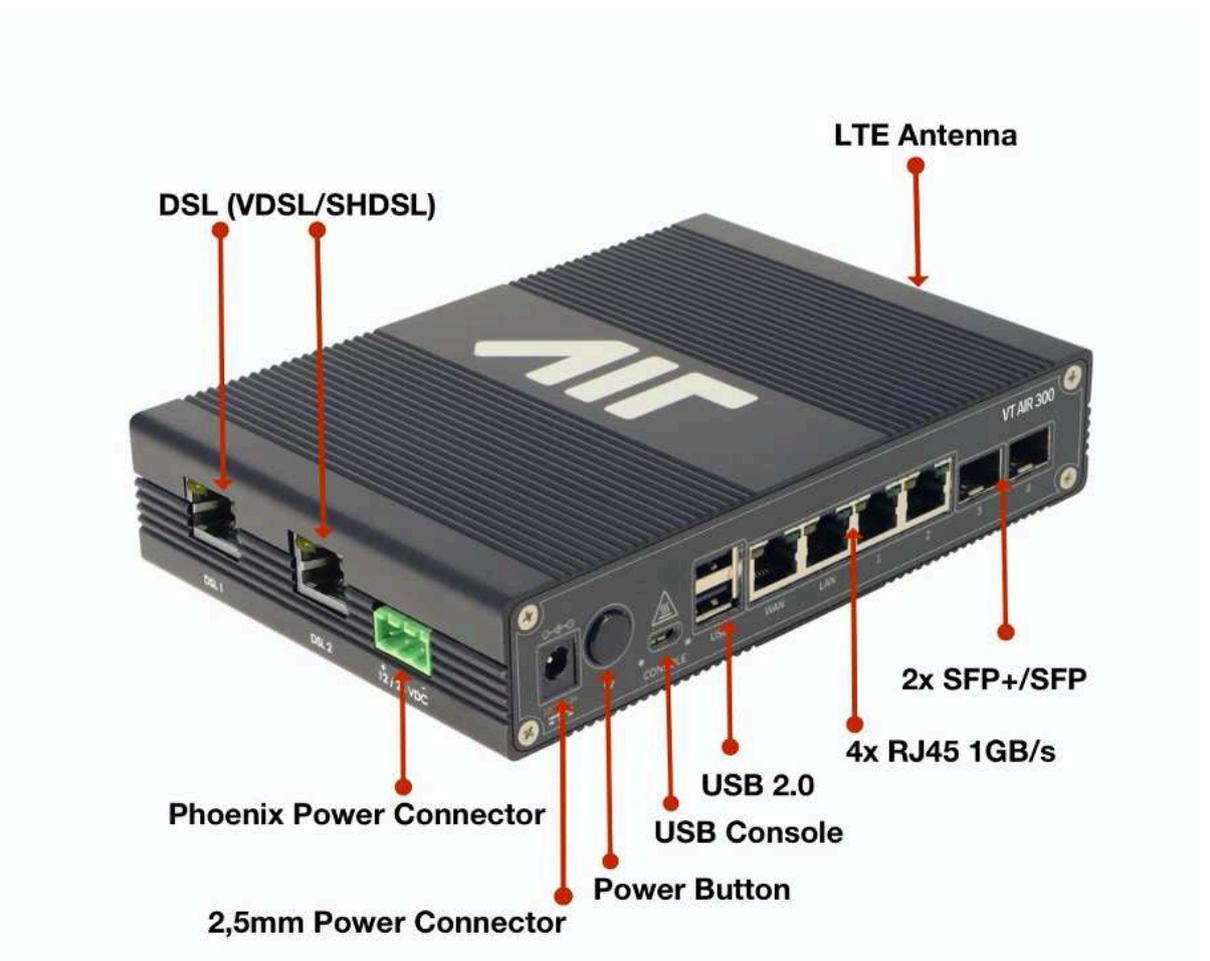
CPU	ARM64 (Marvell ARMADA 8040)
CPU Cores	4 Cores
NIC	2x 10GbE/1GbE SFP+/SFP Ports 4x 1Gbps RJ45
SSD	16 GB eMMC
RAM	4 GB DDR4
Ex-pansion	2x DSL (VDSL/SHDSL) 1x LTE 1x mSATA
VDSL	ADSL ITU-T G.992.1/3/5, VDSL2 ITU-T G.993.2, TR-048/067, TR-100, TR-114, ITU-T G.inp, ITU-T G.vector ADSL2+ bis 24 Mbps, VDSL2 bis 200 Mbps
SHDSL	SICO/CPE 1 Channel Mode EFM annex A/B TCPAM Auto/4/8/16/32/64/128 Bitrate Auto/32/64/128/256/512/1024/2048/4096/8192/16384 kbit/s ETSI SDSL, ETSI SDSL.bis, IEEE EFM, ITU G.shdsl, ITU G.shdsl.bis, ITU G.hs, ITU G.bond Emergency Freeze Modes: Point-to-Point, Point-to-Multipoint (Star), Line and Ring operation (with 2 modems)
LTE	LTE: B1 (2100), B2 (1900), B3 (1800), B4 (AWS), B7 (2600), B12 (700ac), B13 (700c), B20 (800DD), B5 (850), B25 (1900), B26 (US 850 Ext), B29 (US 700de Lower), B41 (TDD 2500), B30 (2300 WCS) 3G/UMTS: B1 (2100), B2 (1900), B8 (900), B4 (AWS), B3 (1800), B5 (850) 300Mbit/s Download, 50Mbit/s Upload
Console Port	1x RS-485
USB Ports	2x USB 2.0 ports
Mounting	DIN rail mount
Power	12/24V via 1x 2.5mm DC plug or 1x Phoenix/Euroblock connector
Environment	-20°C to 60°C Operating Temp -20°C to 50°C (SHDSL) -20°C to 50°C (VDSL)
Certificates	CE, FCC, RoHS
Software	VT AIR Linux

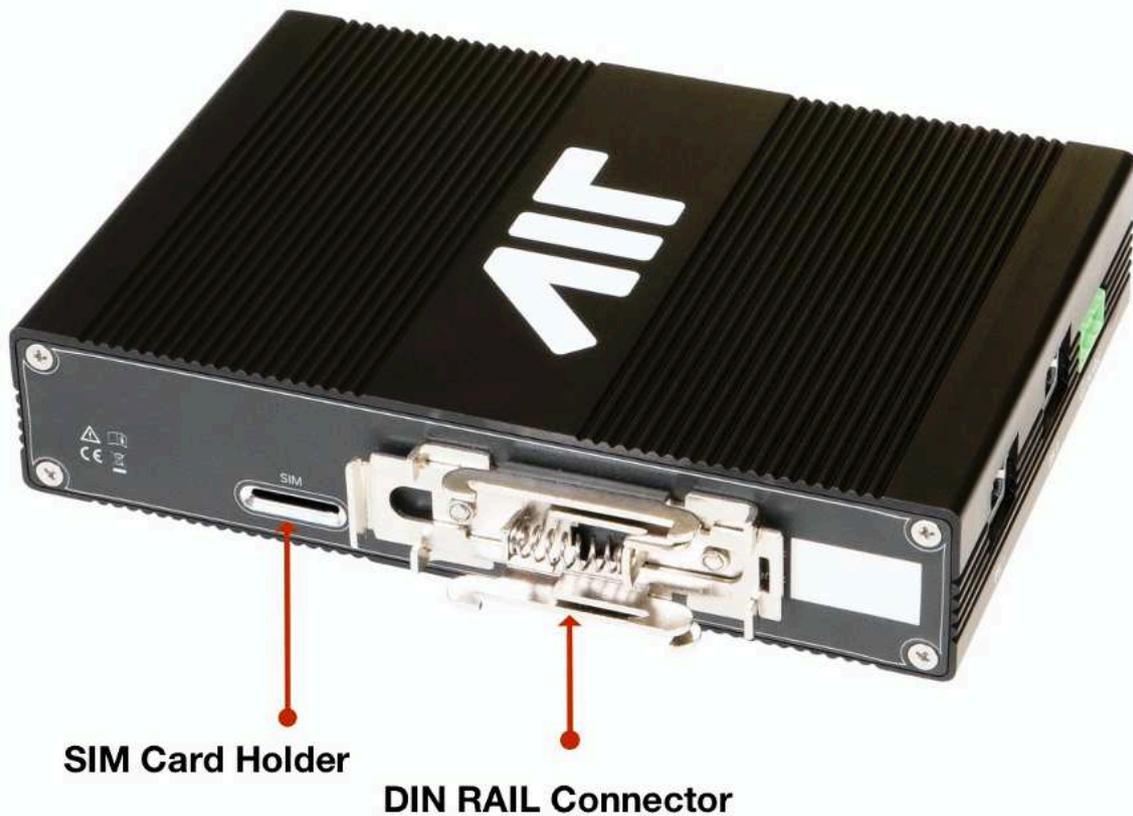
3.2.2 Industrial Usage

The product can be used in the industrial sector.

Electromagnetic Immunity: EN 55024, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11, EN 61000-6-2, EN 61326-1, IEC 61131-2
 Electromagnetic Emission: FCC Class B, EN 55032, EN 61000-3-2, EN 61000-3-3, EN 61000-6-4
 Safety: EN 60950-1

3.2.3 External Connectors





Certified Cables

The following is a list of industry-standard cables, sorted by type, with the necessary compliance requirements that have been proven to work well with the VT AIR product family.

These examples are the cables which Voleatech uses for testing and should provide enough information to source products from your preferred cable vendor.

- Ethernet cable: Monoprice 24AWG Cat6A 500MHz STP (max. 30m)
- USB Cable: USB 2.0 Type A Male to Male Cable
- USB Console Cable: USB 2.0 Micro Type A Male to USB 2.0 Type A Male Cable

USB Connector

The front USB connector supports USB 2.0 (Data rate of maximum 480 Mbit/s), connector type A. It can deliver up to 500 mA of power on each port.

LTE

If you bought the optional LTE configuration the Antenna can be mounted directly at the top of the unit. If you choose to use an Antenna cable, the device is certified for a cable length of up to 1m.

The main Antenna is in the back towards the DIN RAIL connector, the auxiliary Antenna is at the front of the device.

3.2.4 Packaging

The following items will be in the packaging of your VT AIR 300. Please make sure to check all items upon arrival of the device:

- VT AIR 300 Device in the enclosure
- Power adapter - 110V/220V US or EU plug
- USB Console Cable: USB 2.0 Type A Male to USB 2.0 Micro B Male Cable
- LTE Antennas (Only with LTE Kit)
- RJ45 to 2 Pin connector (Only with SHDSL)
- Phoenix Power Connector Adapter

Additionally, your device comes with different ports depending on your order:

- 1x or 2x SHDSL
- 1x or 2x VDSL
- 1x SHDSL, 1x VDSL
- LTE Kit
- mSATA

3.2.5 Ports

Front Connectors

Network Ports				
eno0 (WAN)	eno1 (LAN)	eno2	eno3	eno4 (SFP) eno5 (SFP)

Label	Software Name	Features
WAN	eno0	RJ45 1000/100/10 Mbit/s
LAN	eno1	RJ45 1000/100/10 Mbit/s
1	eno2	RJ45 1000/100/10 Mbit/s
2	eno3	RJ45 1000/100/10 Mbit/s
3	eno4	SFP+/SFP (10000/1000 Mbit/s)
4	eno5	SFP+/SFP (10000/1000 Mbit/s)

The RJ45 ports support Autonegotiation and Full Duplex or Half Duplex on all speeds.

The SFP/SFP+ Ports support the following Modules:

- 10Gb BaseT/SR/LR/LRM/ER/CR
- 1Gb BaseT/SR/LR/CR

There is no vendor lock for SFP modules. You can use any Module that conforms to the standard.

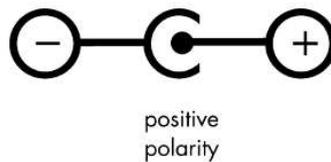
3.2.6 Power

The VT AIR 300 has 2 power connectors:

- 12/24VDC barrel connector
- 12/24VDC Phoenix/Euroblock connector

12/24VDC barrel connector

A suitable external power supply must be connected to the DC power socket, which has the dimensions 5.5mm x 2.5 mm cylindrical barrel connector. The power supply must be 12 or 24VDC. Recommended values are: 12VDC/2A (no more than 5A). Please note that the DC jack must have positive polarity in the center pin:



Warning: Please be aware that the maximum temperature for the barrel connector is 40°C.

12/24VDC Phoenix/Euroblock connector

A suitable external power supply must be connected to the DC Phoenix power connector. The power supply must be 12 or 24VDC. Recommended values are: 24VDC/1A (no more than 3A). Please note that the polarity is printed below the Phoenix power connector. Never connect the wrong polarity as the device will break.

The middle pin can be used as grounding.

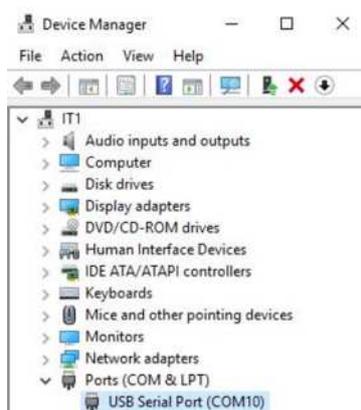
Warning: Only one power connector is allowed to be connected at any time!

3.2.7 USB Console

The appliance has a UART to USB bridge allowing convenient connection to the device console. Such serial console connection is of USB-to-UART type. The connection speed should be set to 115200 bps. All modern Operating Systems have a driver for the UART.

Windows

First you have to locate the COM Port number. Open the Device Manager and expand the section for Ports (COM & LPT). Look for an entry with a title such as USB Serial Port. A label is next to the name (COMX) where X is a number.



MacOSX

In OSX the device shows up at `/dev/tty.usbserial-XXXXXX` where X is a series of numbers and letters.

Linux

In Linux the device shows up at `/dev/ttyUSBX` where X is a number. You can also have a look at the output of `dmesg` to locate the newly connected device.

Terminal Program

A terminal program is required to open the connected serial port. We recommend:

OS	Program
Windows	Putty
MacOSX	Screen, Serial
Linux	Screen

First Connection to TBF Appliance

All TBF Appliances have a default LAN IP Address of `192.168.1.1` and the DHCP Server is active on LAN. Please make sure to locate the *LAN* interface of your appliance in the manual.

Connect your computer to the LAN Interface and receive an IP Address from the DHCP Server. It will be in the `192.168.1.X` range.

After receiving the IP Address open a supported browser and navigate to **`https://192.168.1.1`** A certificate warning will appear, since the TBF is using a self signed certificate. Please accept the certificate and continue to the page.

You will now be presented with the TBF login screen and you can use the default User and Password to login.

Note: User: admin Password: vtair

Please change the password after the first login.

3.2.8 VT AIR Reinstallation

Your VT AIR device comes pre-installed with its operating system. Should you ever need to reinstall the VT AIR operating system follow this guide.

Download the Installer File

You can download the installer file from your Portal (see [Downloads](#) for details). Make sure to download the file for your specific model/architecture.

USB Flash Drive Preparation

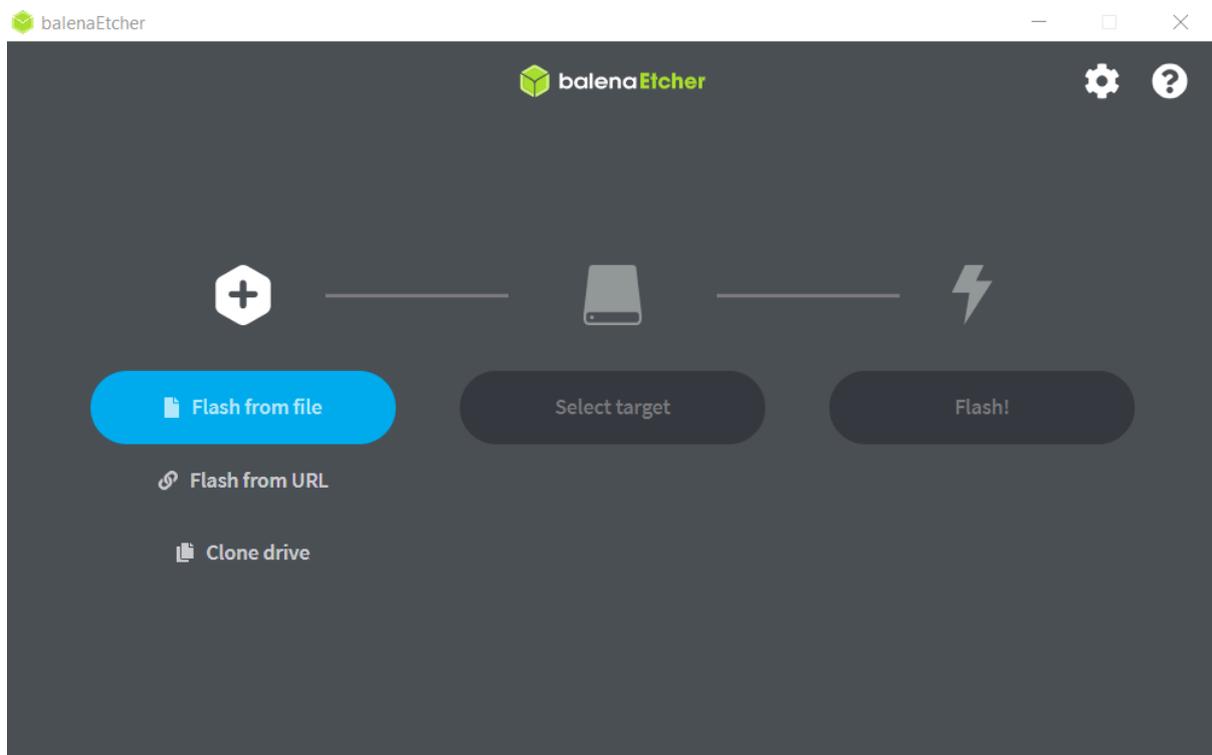
Once you downloaded the file make sure your USB flash drive is at least 2 GB in size. Also backup all your files from the USB flash drive since it will be formatted in the process and all files on it will be deleted.

Download the Software

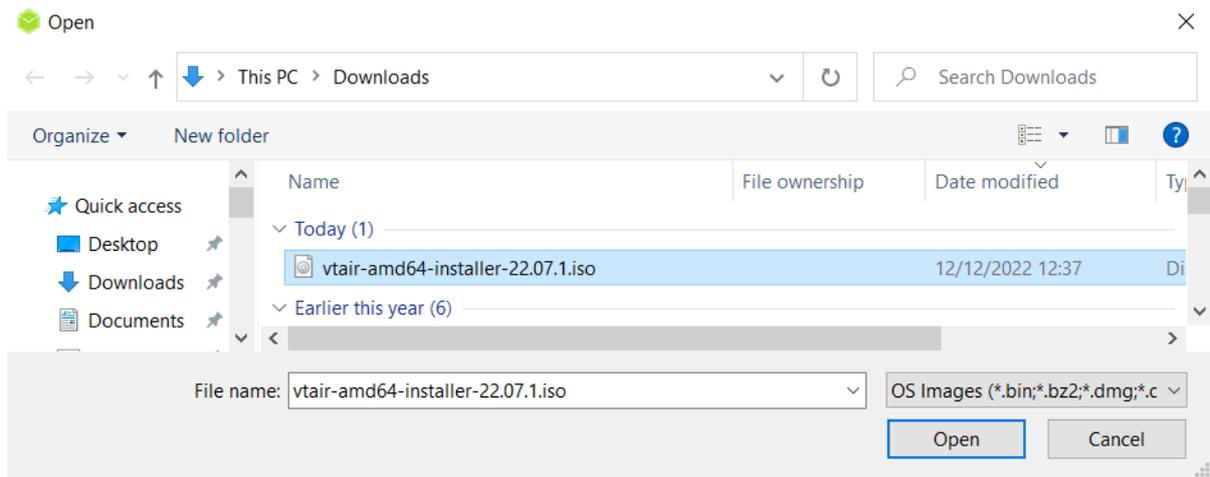
Download and install the software *balenaEtcher* from www.balena.io/etcher. It is available for Windows, macOS and Linux. Select the software for your specific operating system.

Use the Software

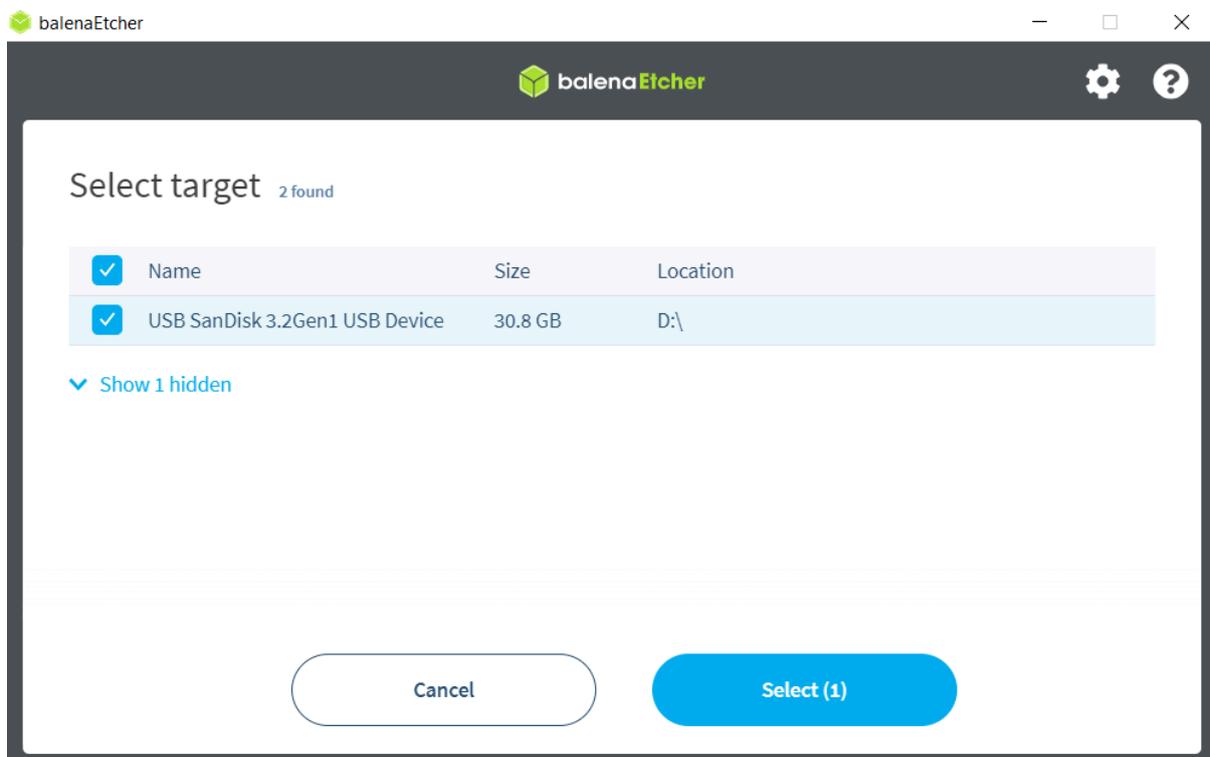
Insert your USB flash drive into the computer. Start the *balenaEtcher* software.



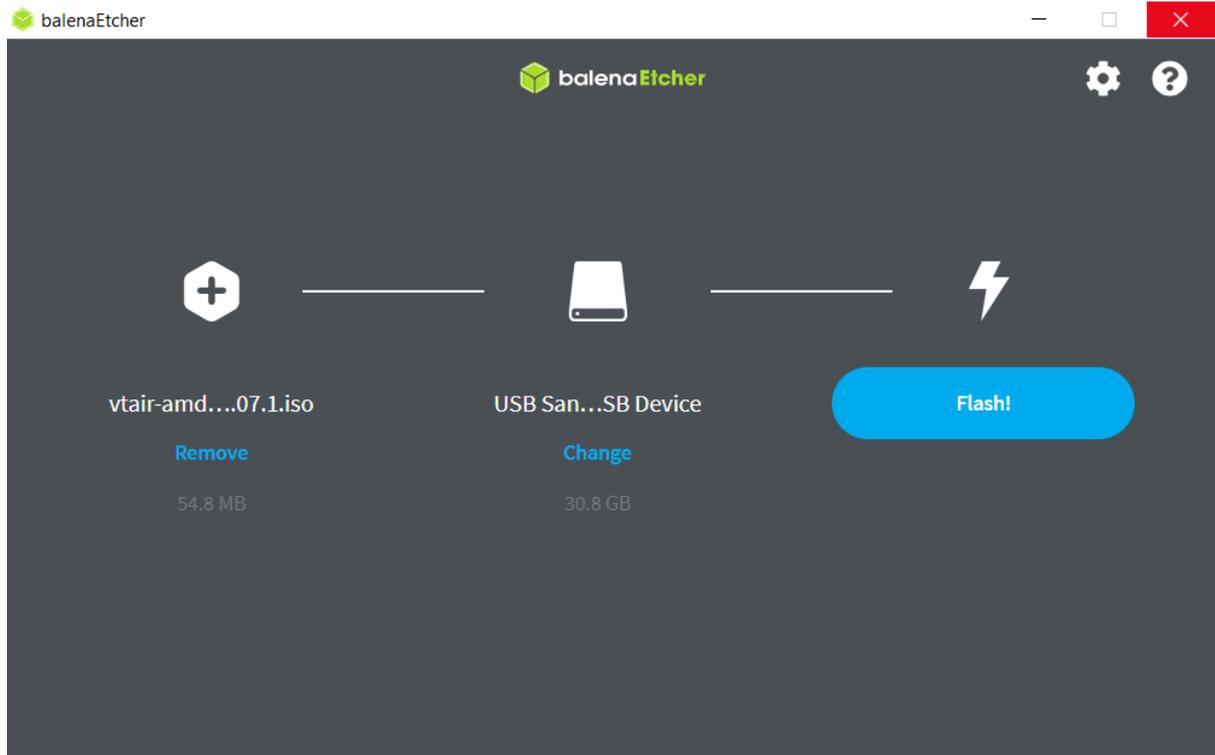
Press *Flash from file*



Select the downloaded installer file with the ending .iso



Select your USB flash drive as target



Press *Flash!* to complete and wait until the process is finished. Close the software and remove the USB flash drive from your computer.

Install the Software

Insert the USB flash drive with the new VT AIR operating system in your VT AIR's USB port.

Serial Console Installation

Connect the USB cable to the Console USB port of your VT AIR device and your computer. On your computer connect to your VT AIR's Console (see [Console Access](#)).

Type **"reboot"** to reboot the system. In the boot process you'll see a timer that you can interrupt by pressing any key. This gives you a shell from where you can reinstall your OS.

```
[ OK ] Reached target Unmount All Filesystems.
[ OK ] Stopped target Local File Systems (Pre).
[ OK ] Stopped Create Static Device Nodes in /dev.
[ OK ] Stopped Create System Users.
[ OK ] Stopped Remount Root and Kernel File Systems.
[ OK ] Reached target Shutdown.
[ OK ] Reached target Final Step.
[ OK ] Started Reboot.
[ OK ] Reached target Reboot.
[ 68.092735] reboot: Restarting system

U-Boot SPL 2020.01-dirty (Mar 15 2020 - 09:59:33 +0000)
High speed PHY - Version: 2.0
Detected Device ID 6828
board SerDes lanes topology details:
| Lane # | Speed | Type |
|-----|-----|-----|
| 0      | 3     | SATA0 |
| 1      | 0     | SGMII1 |
| 2      | 5     | PCIe1 |
| 3      | 5     | USB3 HOST1 |
| 4      | 5     | USB3 HOST0 |
| 5      | 0     | SGMII2 |
|-----|-----|-----|
PCIe, Idx 1: detected no link
High speed PHY - Ended Successfully
mv_ddr: mv_ddr-armada-18.09.2
DDR3 Training Sequence - Switching XBAR Window to FastPath Window
mv_ddr: completed successfully
Trying to boot from SPI

U-Boot 2020.01-dirty (Mar 15 2020 - 09:59:33 +0000)

SoC: MV88F6028-B0 at 1600 MHz
DRAM: 2 GiB (800 MHz, 32-bit, ECC not enabled)
MMC: mv_sdh: 0
Loading Environment from SPI Flash... SF: Detected w25q32 with page size 256 Bytes, erase size 4 KiB, total 4 MiB
*** Warning - bad CRC, using default environment

Model: VT AIR 100
Board: Voleatech VT AIR 100
Invalid EEPROM Header
SCSI: MVEBU SATA INIT
SATA link 0 timeout.
AHCI 0001.0000 32 slots 2 ports 6 Gbps 0x3 impl SATA mode
flags: 64bit ncq led only pmp fbss pio slum part sxs

Net:
Warning: ethernet@70000 using MAC address from ROM
eth1: ethernet@70000
Error: ethernet@30000 address not set.

Error: ethernet@34000 address not set.

Hit any key to stop autoboot: 0
=>
```

Type “**run install**” to run the OS installer from your USB stick. The installer runs without any user inputs.

3.2.9 LEDs

The VT AIR 300 has multiple LEDs. They are indicating for example power on, connection and port activity. Ethernet port related LEDs are embedded in the RJ45 connectors, while the power indicator LED is located below the serial port.

The RJ45 NIC LEDs are configured the following way:

LED Activity	Explanation
Off	No connection
Green Light Only	100Mbit/s Speed
Green and Yellow Light	1000Mbit/s Speed

SHDSL LEDs

If your order includes a SHDSL card you will also have 2 LEDs on each SHDSL RJ45 connector. The left LED is for power on and will be on when the SHDSL port is ready to do a connection. The right LED has three different modes:

LED Activity	Explanation
Slow Blinking	Searching for remote modem
Fast Blinking	Connection parameters are being negotiated
Steady Light	Connection established

VDSL LEDS

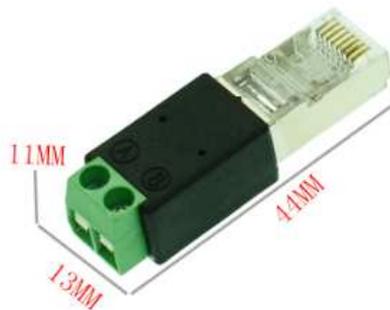
If your order includes a VDSL card you will also have 2 LEDs on each SHDSL RJ45 connector. The left LED is for power on and will be on when the VDSL port is ready to do a connection. The right LED has three different modes:

LED Activity	Explanation
Slow Blinking	Searching for remote modem
Fast Blinking	Connection parameters are being negotiated
Steady Light	Connection established

3.2.10 SHDSL

The optional SHDSL modems only use 2 PINs of the RJ45 connector, PIN4 and PIN5. It does not matter in which order two SHDSL modems are connected to each other the PINs can be swapped.

We add a RJ45 to 2 PIN connector for each SHDSL modem.



3.2.11 Operational Data

Operational Voltage

Item	Voltage	Current	Ambient Temperature
Front barrel connector	12 or 24 VDC	2.0 A	Max. 40°C
Phoenix/Euroblock connector	12 or 24 VDC	2.0 A	Max. 60°C

Environmental Data

The environmental temperature data are based upon the component with the lowest available temperature. Please make sure to check which addons you ordered and make sure not to exceed the allowed ambient temperature.

Warning: Failure to comply with the allowed ambient temperature may void the warranty of your device.

Ambient Temperature	Minimum	Maximum
Base Device/LTE	-20°C	60°C
VDSL	-20°C	50°C
SHDSL	-20°C	50°C
Humidity (non-condensing)	10 %	90 %

Leave a minimum of 2cm of space on both sides of the device when installed on a DIN Rail.

For ambient temperatures above 30°C, leave 5cm space on both sides of the device for air cooling to work properly.

Grounding

The device can be grounded through the DIN RAIL connector. The case dissipates high currents across the DIN RAIL connector.

The middle pin of the Phoenix plug can also be used as grounding. Please note that this can dissipate only a low current, in comparison to the DIN rail.

3.2.12 Warranty Terms and Conditions

Voleatech GmbH guarantees its hardware products against defects in workmanship and material for a period of one (1) year from the date of shipment. Under warranty, the customer's sole remedy and Voleatech's sole liability shall be, at Voleatech's sole discretion, to either repair or replace the defective hardware product at no charge. This warranty is void if the hardware product has been altered or damaged by an accident, misuse or abuse or is not operated according to this manual. For additional information on warranty and related topics like RMA, please visit www.voleatech.de.

Disclaimer of Warranty THIS WARRANTY IS MADE IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESSED, OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR A SPECIFIC PURPOSE, NONINFRINGEMENT OR THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION, EXCEPT THE WARRANTY EXPRESSLY STATED HEREIN. THE REMEDIES SET FORTH HEREIN SHALL BE THE SOLE AND EXCLUSIVE REMEDIES OF ANY CUSTOMER OR PURCHASER WITH RESPECT TO ANY DEFECTIVE PRODUCT.

Limitation on Liability UNDER NO CIRCUMSTANCES SHALL VOLEATECH GmbH BE LIABLE FOR ANY LOSS, DAMAGE OR EXPENSES INCURRED OR WITH RESPECT TO ANY DEFECTIVE PRODUCT. IN NO EVENT SHALL Voleatech GmbH BE LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES THAT CUSTOMER MAY SUFFER DIRECTLY OR INDIRECTLY FROM THE USAGE OF ANY PRODUCT. BY ORDERING THE VT AIR 300, THE CUSTOMER APPROVES THAT THE VT AIR 300, HARDWARE AND SOFTWARE, WAS THOROUGHLY TESTED AND HAS MET THE CUSTOMER'S REQUIREMENTS AND SPECIFICATIONS.

3.2.13 LEGAL NOTICE

Voleatech GmbH (hereinafter "Voleatech") products and services are sold subject to Voleatech terms and conditions of sale, delivery and payment supplied at the time of purchase order acknowledgement. Voleatech warrants the performance of its products according to actual specifications at the date of shipment. Voleatech reserves the right to make changes to its products and specifications or to discontinue any product, product line or service without prior notice. Customers should make sure to obtain in each case the latest version of relevant product information from Voleatech and to always verify for themselves that their requirements are met and reference is up to date. Product testing and all additional

quality control techniques are utilized to the extent that Voleatech deems necessary to support their warranty and warranty terms. Therefore detailed testing of all parameters in any product is not necessarily performed in full unless required by law or regulation. In order to minimize risks that may be associated with customer products, applications or services, the customer must use adequate design and operating safeguards to minimize any possible hazards. Voleatech is not liable for any applications assistance or customer product design and thus it is the customer's sole responsibility to make the selection and usage of Voleatech products. Voleatech is not liable for any such selection or usage thereafter and neither is liable for the usage of any circuitry or components other than completely and entirely embodied in a Voleatech product. Furthermore Voleatech is not liable for its products commercial fit for any market segment envisioned by the customer. Voleatech products are not intended for use in life support systems, appliances, nuclear systems or systems where malfunction can reasonably be expected to result in personal injury, death or severe property or environmental damage. Any use of Voleatech's products by the customer for such purposes is completely at the customer's own risk. Voleatech does not grant any license -expressed or implied- on any patent right, copyright, mask work right, type or model protection or any other intellectual property right (IPR) of Voleatech covering or relating to any product combination, hardware, machine, software or process in which its products or services might be or are used. Any provision or publication of any third party's products or services does not constitute Voleatech's approval, license, warranty or endorsement thereof. Any third party trademarks contained in this document belong to the respective third party owner. Reproduction of content and information from Voleatech documents and manuals is permissible only if reproduction is without alteration and is accompanied by all associated copyright, proprietary and other notices (including this notice) and related conditions. Voleatech is not liable for any un-authorized alteration of such content and information or for any reliance related to alterations thereon. Any representations made, warranties given, and/or liabilities accepted by any person which differ from those contained in this manual or in Voleatech's standard terms and conditions of sale, delivery and payment are made, given and/or accepted at customer's own risk. Voleatech is not liable for any such representations, warranties or liabilities or for any reliance thereon by any person.

3.2.14 Regulatory

This chapter provides regulatory and compliance information about Voleatech's VT AIR 300 -related information. Product name: VT AIR 300

Safety Notice

Before you begin using this product, please read the following safety information. Attention to these warnings will help prevent personal injuries and damage to the products. It is your responsibility to use the product in an appropriate manner. This product is designed for use solely indoor environments or, if expressly permitted, also in the field and must not be used in any way that may cause personal injury or property damage.

You are responsible if the product is used for any intention other than its designated purpose or in disregard of Voleatech's instructions. Voleatech shall assume no responsibility for such use of the product. The product is used for its designated purpose if it is used in accordance with its product documentation and within its performance limits.

Safety Information and Notices

Never turn on or connect to power any equipment when there is evidence of mechanical damage, fire, exposure to water, or structural damage.

When not in use, avoid placing or storing the product in the following places or under the following conditions:

- Ambient temperature above 40°C
- Exposed to direct sunlight
- Humid or exposed to dust

Warning: This product does not contain any user replicable or serviceable parts. Do not take apart or attempt to service the product yourself.

Never remove the cover or any part of the housing of the product. The internal battery is not user replicable.

In the event of an equipment malfunction, all repairs must be performed either by Voleatech GmbH or by an authorized agent. It is the customer responsibility to report the need for service to Voleatech GmbH or to one of the authorized agents. For service information, contact Voleatech GmbH customer support.

Be careful not subject the product to strong impact.

If the product was subjected to a strong impact and/or falling over check carefully for any damage to the product. If such damage is observed the use of the product must be stopped immediately.

Operation

The product may be operated only under the operating conditions as specified by Voleatech GmbH. When the product is used for an extended period of time, and/or at high ambient temperature and/or exposed to direct sunlight it is normal for the product body to feel warm.

Avoid overheating the product. The product's ventilation should not be obstructed or blocked. If proper ventilation is not provided it can result in battery overheating or explosion of the battery resulting fire, burns or other injuries.

Stop using the product immediately if it emits smoke or a strange smell, or otherwise behaves abnormally.

Following are the required operating position and conditions:

- Do not place the product on unstable surfaces
- Do not place the product on elevated surface and secure it from falling from high places on passerby
- Do not place the product on heat-generating surface or near heat emitting devices or direct flame. Verify that there is sufficient clearance between the product and any other device exhaust warm air
- The product operating ambient range can be found at Environmental Data. Voleatech GmbH recommends that an ambient temperature of 0 to 40 °C (32 to 104 °F) and relative humidity of 30-50% is maintained during normal operation as this will result in better performance and longer life of the equipment. Temperature must not exceed the maximum temperature specified in Environmental Data.
- Do not expose the product to moisture or dust.
- The product is not liquid-proof; therefore, the equipment must be protected against penetration by liquids. If the necessary precautions are not taken, the user may suffer electric shock or the product itself may be damaged, which can also lead to personal injury.
- Never use the product under conditions in which condensation has formed or can form in or on the product, e.g. if the product has been moved from a cold to a warm environment. Penetration by water increases the risk of electric shock.

AC/DC Adapter or Power Supply - Electrical Safety

The following information on electrical safety must be observed, failing to follow these instruction may result in electric shock, fire and/or serious personal injury or death.

Use only the adapter or power supply supplied with the product or adapter or power supply with the following specifications:

Output voltage of 12V or 24V and current of at least 2A and not more than 3A.

Prior to powering the product and plugging the adapter or power supply to the mains supply, always ensure that the nominal voltage setting on the adapter or power supply matches the nominal voltage of the AC supply network.

If extension cords or connector strips are implemented, they must be checked on a regular basis to ensure that they are safe to use.

Never use the adapter or power supply if the power cable is damaged. Check the power cable on a regular basis to ensure that it is in proper operating condition. By taking appropriate safety measures and carefully laying the power cable, you can ensure that the cable will not be damaged and that no one can be hurt by, for example, tripping over the cable or suffering an electric shock.

Do not insert the plug into sockets that are dusty or dirty. Insert the plug firmly and all the way into the socket. Otherwise, sparks that result in fire and/or injuries may occur.

Do not overload any sockets, extension cords or connector strips; doing so can cause fire or electric shocks.

Do not insert or remove the plug with wet hands.

Never remove the cover or any part of the housing of the adapter or power supply, doing so will expose circuits and components and can lead to electric shock, injuries, fire or damage to the product.

The adapter or power supply operating ambient temperature range is of 0 to 40°C / 32 to 104 °F (storage temp range: -20 to 60 °C / -04 to 140 °F) maximum operating altitude is 2000 m ASL.

Use suitable overvoltage protection to ensure that no overvoltage (such as that caused by a bolt of lightning) can reach the product. Otherwise, the person operating the product will be exposed to the danger of an electric shock.

The product is not liquid-proof; therefore, the equipment must be protected against penetration by liquids. If the necessary precautions are not taken, the user may suffer electric shock or the product itself may be damaged, which can also lead to personal injury.

Never use the product under conditions in which condensation has formed or can form in or on the product, e.g. if the product has been moved from a cold to a warm environment. Penetration by water increases the risk of electric shock.

Prior to cleaning the product, disconnect it completely from the power supply. Use a soft, non-linting cloth to clean the product. Never use chemical cleaning agents such as alcohol, acetone or diluents for cellulose lacquers.

Electronic Emission Notices (EMC)

Federal Communications Commission Declaration of Conformity The following information refers to VT AIR 300. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Responsible Party: Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany

European Union - Compliance to the Electromagnetic Compatibility

(EMC) Directive or Radio Equipment Directive

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU (from 20 April, 2016) on the approximation of the laws of the Member States relating to electromagnetic compatibility.

Voleatech GmbH is not responsible for any radio or television interference caused by using other than specified or recommended cables and connectors or by unauthorized changes or modifications to this equipment.

Unauthorized changes or modifications could void the user's authority to operate the equipment.

WEEE and recycling statements

The WEEE marking on Voleatech GmbH products applies to countries with WEEE and e-waste regulations (for example, the European WEEE Directive). Appliances are labeled in accordance with local regulations concerning waste electrical and electronic equipment (WEEE).

These regulations determine the framework for the return and recycling of used appliances as applicable within each geography. This label is applied to various products to indicate that the product is not to be thrown away, but rather put in the established collection systems for reclaiming these end of life products.

Users of electrical and electronic equipment (EEE) with the WEEE marking must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to them for the return, recycle and recovery of WEEE and to minimize any potential effects of EEE on the environment and human health due to the presence of hazardous substances. Voleatech GmbH electrical and electronic equipment (EEE) may contain parts and components, which at end-of-life might qualify as hazardous waste.

EEE and waste electrical and electronic equipment (WEEE) can be delivered free of charge to the place of sale or any distributor that sells electrical and electronic equipment of the same nature and function as the used EEE or WEEE.



Restriction of Hazardous Substances (RoHS) European Union RoHS

This product, with included parts (cables, cords, and so on) meets the requirements of Directive 2011/65/EU and directive 2015/863/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment ("RoHS recast" or "RoHS 2").

EU Radio Directive Equipment (RED)

Declaration of Conformity (DoC)

Voleatech declares that the radio equipment for the VT AIR 300 is in compliance with Radio Equipment Directive 2014/53/EU.

LTE Modem

<p>Warning: A safety distance of at least 20 cm must be kept between the product antenna and the operator or and other persons.</p>
--

3.2.15 Contact Information and Resources

Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany

www.voleatech.de info@voleatech.de +49 7121 539 550

3.3 VT AIR 310



3.3.1 Overview

Summary of Features

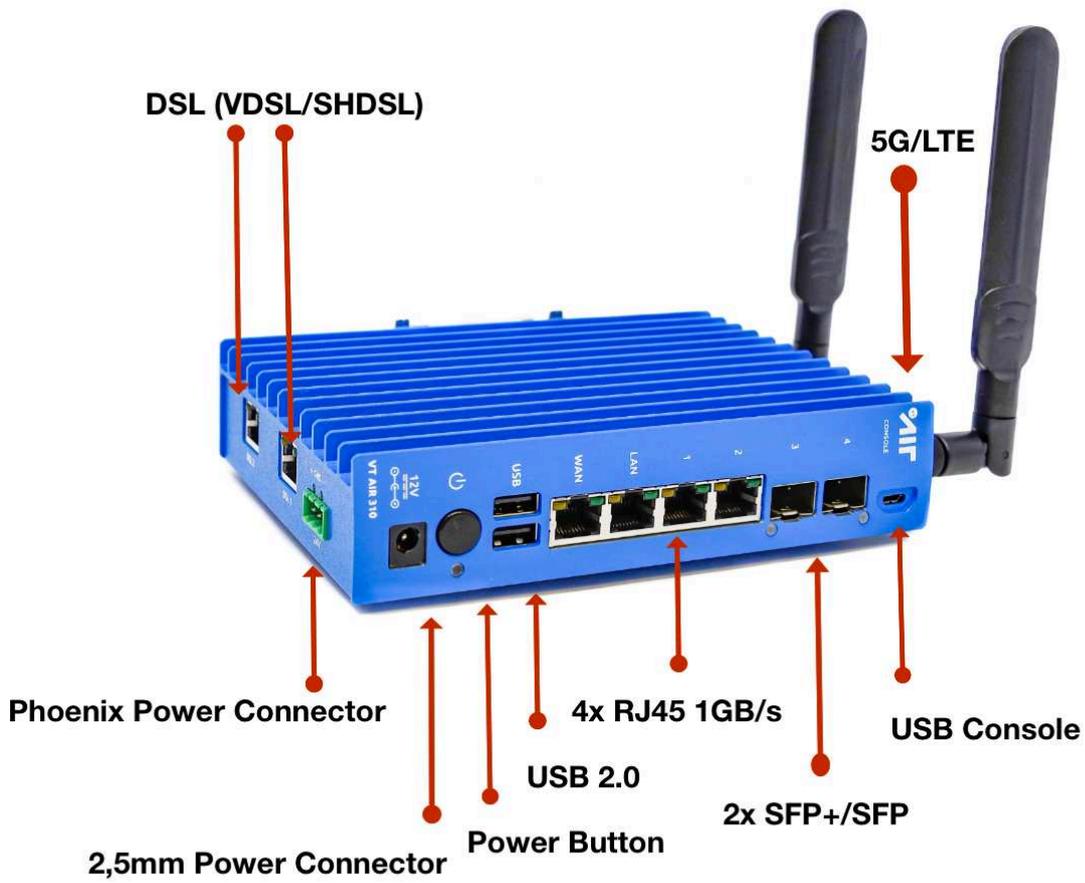
CPU	ARM64
CPU Cores	4 Cores
NIC	2x 10GbE/1GbE SFP+/SFP Ports 4x 1Gbps RJ45
SSD	16 GB eMMC
RAM	4 GB DDR4
Ex-pansion	2x DSL (VDSL/SHDSL) 1x LTE 1x mSATA
VDSL	ADSL ITU-T G.992.1/3/5, VDSL2 ITU-T G.993.2, TR-048/067, TR-100, TR-114, ITU-T G.inp, ITU-T G.vector ADSL2+ bis 24 Mbps, VDSL2 bis 200 Mbps
SHDSL	CO/CPE 1 Channel Mode EFM annex A/B TCPAM Auto/4/8/16/32/64/128 Bitrate Auto/32/64/128/256/512/1024/2048/4096/8192/16384 kbit/s ETSI SDSL, ETSI SDSL.bis, IEEE EFM, ITU G.shdsl, ITU G.shdsl.bis, ITU G.hs, ITU G.bond Emergency Freeze Modes: Point-to-Point, Point-to-Multipoint (Star), Line and Ring operation (with 2 modems)
LTE	LTE: B1 (2100), B2 (1900), B3 (1800), B4 (AWS), B7 (2600), B12 (700ac), B13 (700c), B20 (800DD), B5 (850), B25 (1900), B26 (US 850 Ext), B29 (US 700de Lower), B41 (TDD 2500), B30 (2300 WCS) 3G/UMTS: B1 (2100), B2 (1900), B8 (900), B4 (AWS), B3 (1800), B5 (850) 300Mbit/s Download, 50Mbit/s Upload
Console Port	1x RS485
USB Ports	2x USB 2.0 ports
Mounting	DIN rail mount
Power	12/24V via 1x 2.5mm DC plug or 1x Phoenix/Euroblock connector
Environment	-20°C to 60°C Operating Temp -20°C to 50°C (SHDSL) -20°C to 50°C (VDSL)
Certificates	CE, FCC, RoHS
Software	VT AIR Linux

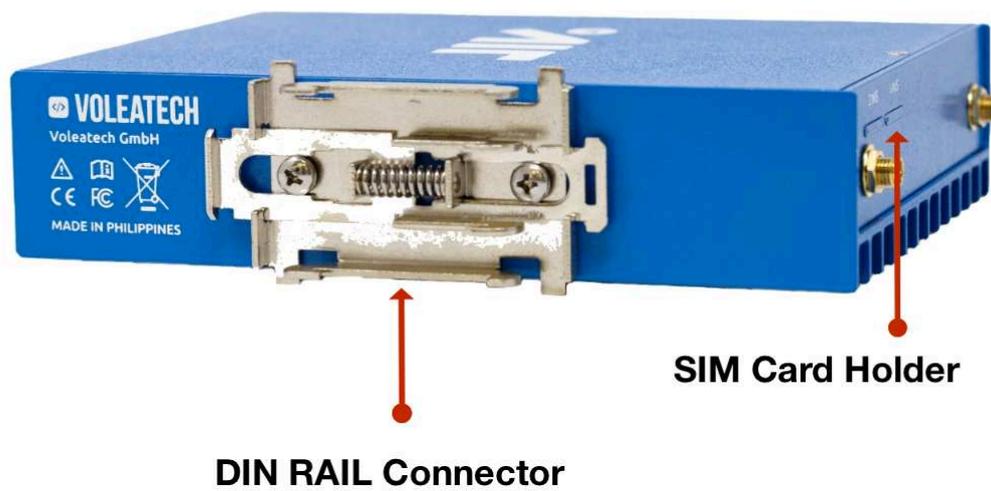
3.3.2 Industrial Usage

The product can be used in the industrial sector.

Electromagnetic Immunity: EN 55024, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11, EN 61000-6-2, EN 61326-1, IEC 61131-2
 Electromagnetic Emission: FCC Class B, EN 55032, EN 61000-3-2, EN 61000-3-3, EN 61000-6-4
 Safety: EN 60950-1

3.3.3 External Connectors





Certified Cables

The following is a list of industry-standard cables, sorted by type, with the necessary compliance requirements that have been proven to work well with the VT AIR product family.

These examples are the cables which Voleatech uses for testing and should provide enough information to source products from your preferred cable vendor.

- Ethernet cable: Monoprice 24AWG Cat6A 500MHz STP (max. 30m)
- USB Cable: USB 2.0 Type A Male to Male Cable
- USB Console Cable: USB 2.0 Type A Male to USB 2.0 Micro B Male Cable

USB Connector

The front USB connector supports USB 2.0 (Data rate of maximum 480 Mbit/s), connector type A. It can deliver up to 500 mA of power on each port.

LTE

If you bought the optional LTE configuration the Antenna can be mounted directly at the top of the unit. If you choose to use an Antenna cable, the device is certified for a cable length of up to 1m.

The main Antenna is in the back towards the DIN RAIL connector, the auxiliary Antenna is at the front of the device.

3.3.4 Packaging

The following items will be in the packaging of your VT AIR 310. Please make sure to check all items upon arrival of the device:

- VT AIR 310 Device in the enclosure
- Power adapter - 110V/220V US or EU plug
- USB Console Cable: USB 2.0 Type A Male to USB 2.0 Micro B Male Cable
- LTE Antennas (Only with LTE Kit)
- RJ45 to 2 Pin connector (Only with SHDSL)
- Phoenix Power Connector Adapter

Additionally, your device comes with different ports depending on your order:

- 1x or 2x SHDSL
- 1x or 2x VDSL
- 1x SHDSL, 1x VDSL
- LTE Kit
- mSATA

3.3.5 Ports

Front Conenctors

Network Ports				
eno0 (WAN)	eno1 (LAN)	eno2	eno3	eno4 (SFP) eno5 (SFP)

Label	Software Name	Features
WAN	eno0	RJ45 1000/100/10 Mbit/s
LAN	eno1	RJ45 1000/100/10 Mbit/s
1	eno2	RJ45 1000/100/10 Mbit/s
2	eno3	RJ45 1000/100/10 Mbit/s
3	eno4	SFP+/SFP (10000/1000 Mbit/s)
4	eno5	SFP+/SFP (10000/1000 Mbit/s)

The RJ45 ports support Autonegotiation and Full Duplex or Half Duplex on all speeds.

The SFP/SFP+ Ports support the following Modules:

- 10Gb BaseT/SR/LR/LRM/ER/CR
- 1Gb BaseT/SR/LR/CR

There is no vendor lock for SFP modules. You can use any Module that conforms to the standard.

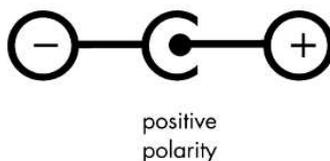
3.3.6 Power

The VT AIR 310 has 2 power connectors:

- 12/24VDC barrel connector
- 12/24VDC Phoenix/Euroblock connector

12/24VDC barrel connector

A suitable external power supply must be connected to the DC power socket, which has the dimensions 5.5mm x 2.5 mm cylindrical barrel connector. The power supply must be 12 or 24VDC. Recommended values are: 12VDC/2A (no more than 5A). Please note that the DC jack must have positive polarity in the center pin:



Warning: Please be aware that the maximum temperature for the barrel connector is 40°C.

12/24VDC Phoenix/Euroblock connector

A suitable external power supply must be connected to the DC Phoenix power connector. The power supply must be 12 or 24VDC. Recommended values are: 24VDC/1A (no more than 3A). Please note that the polarity is printed below the Phoenix power connector. Never connect the wrong polarity as the device will break.

The middle pin can be used as grounding.

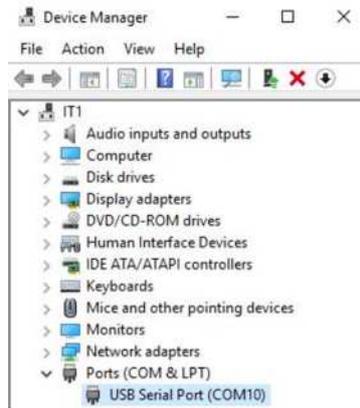
Warning: Only one power connector is allowed to be connected at any time!

3.3.7 USB Console

The appliance has a UART to USB bridge allowing convenient connection to the device console. Such serial console connection is of USB-to-UART type. The connection speed should be set to 115200 bps. All modern Operating Systems have a driver for the UART.

Windows

First you have to locate the COM Port number. Open the Device Manager and expand the section for Ports (COM & LPT). Look for an entry with a title such as USB Serial Port. A label is next to the name (COMX) where X is a number.



MacOSX

In OSX the device shows up at `/dev/tty.usbserial-XXXXXX` where X is a series of numbers and letters.

Linux

In Linux the device shows up at `/dev/ttyUSBX` where X is a number. You can also have a look at the output of `dmesg` to locate the newly connected device.

Terminal Program

A terminal program is required to open the connected serial port. We recommend:

OS	Program
Windows	Putty
MacOSX	Screen, Serial
Linux	Screen

First Connection to TBF Appliance

All TBF Appliances have a default LAN IP Address of `192.168.1.1` and the DHCP Server is active on LAN. Please make sure to locate the *LAN* interface of your appliance in the manual.

Connect your computer to the LAN Interface and receive an IP Address from the DHCP Server. It will be in the `192.168.1.X` range.

After receiving the IP Address open a supported browser and navigate to <https://192.168.1.1> A certificate warning will appear, since the TBF is using a self signed certificate. Please accept the certificate and continue to the page.

You will now be presented with the TBF login screen and you can use the default User and Password to login.

Note: User: admin Password: vtair

Please change the password after the first login.

3.3.8 VT AIR Reinstallation

Your VT AIR device comes pre-installed with its operating system. Should you ever need to reinstall the VT AIR operating system follow this guide.

Download the Installer File

You can download the installer file from your Portal (see [Downloads](#) for details). Make sure to download the file for your specific model/architecture.

USB Flash Drive Preparation

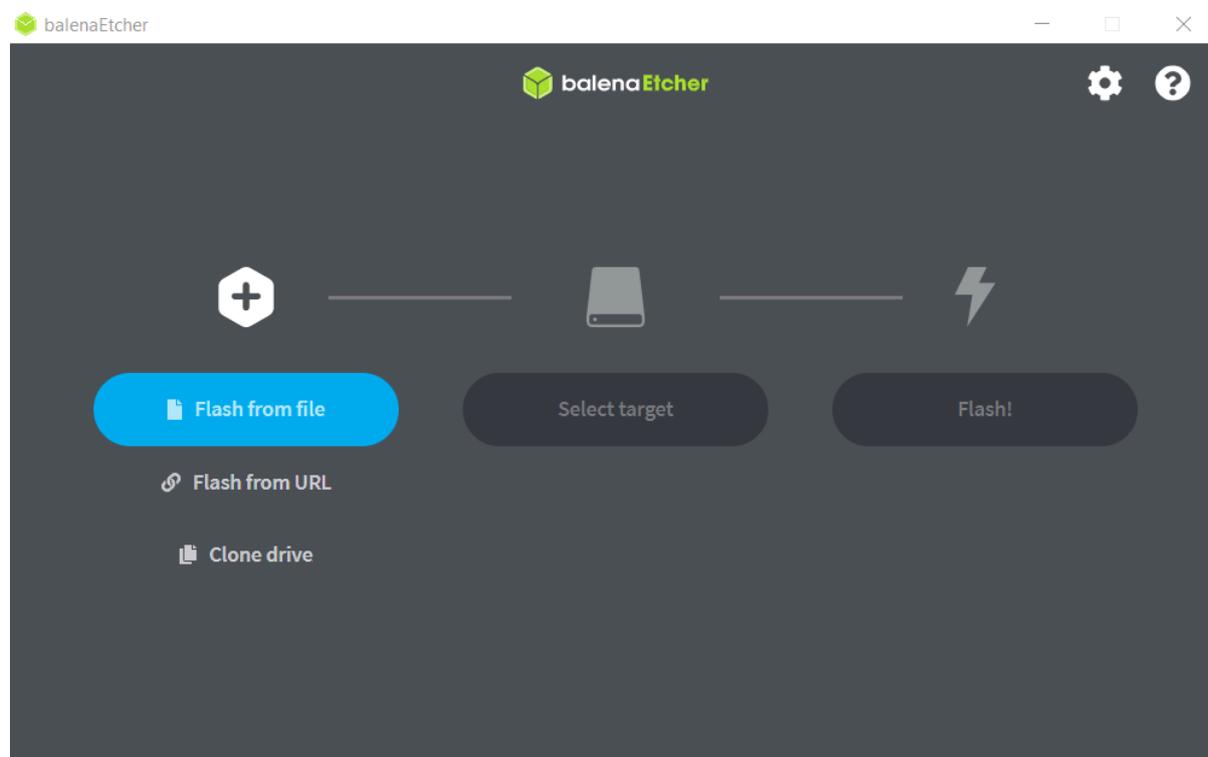
Once you downloaded the file make sure your USB flash drive is at least 2 GB in size. Also backup all your files from the USB flash drive since it will be formatted in the process and all files on it will be deleted.

Download the Software

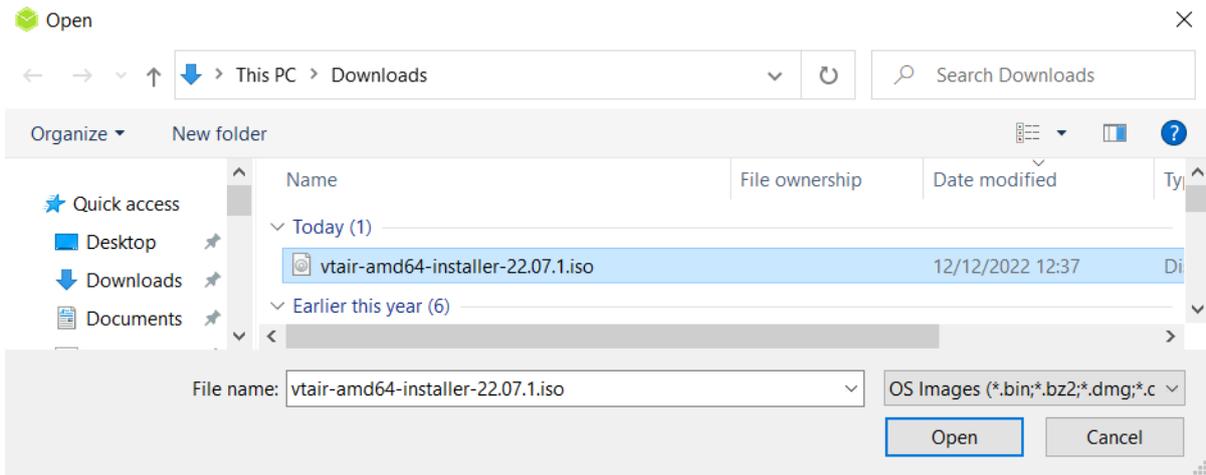
Download and install the software *balenaEtcher* from www.balena.io/etcher. It is available for Windows, macOS and Linux. Select the software for your specific operating system.

Use the Software

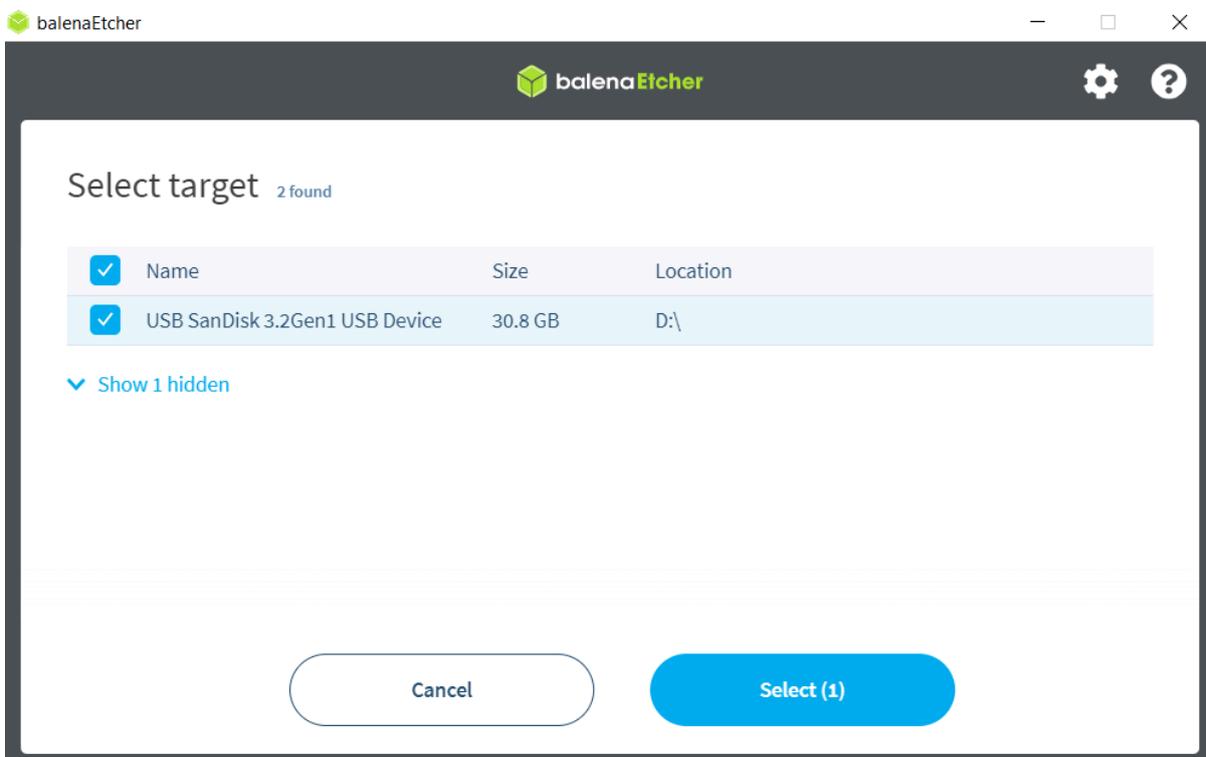
Insert your USB flash drive into the computer. Start the *balenaEtcher* software.



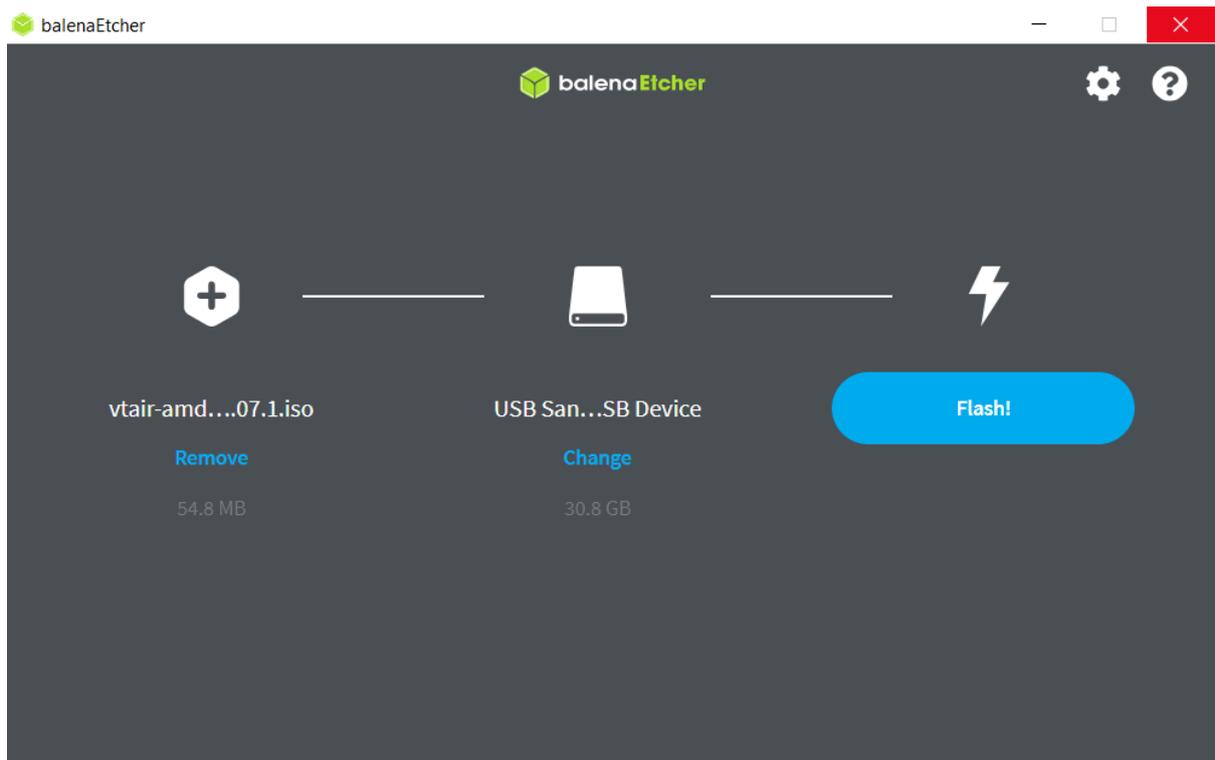
Press *Flash from file*



Select the downloaded installer file with the ending .iso



Select your USB flash drive as target



Press *Flash!* to complete and wait until the process is finished. Close the software and remove the USB flash drive from your computer.

Install the Software

Insert the USB flash drive with the new VT AIR operating system in your VT AIR's USB port.

Serial Console Installation

Connect the USB cable to the Console USB port of your VT AIR device and your computer. On your computer connect to your VT AIR's Console (see [Console Access](#)).

Type **“reboot”** to reboot the system. In the boot process you'll see a timer that you can interrupt by pressing any key. This gives you a shell from where you can reinstall your OS.

```
[ OK ] Reached target Unmount All Filesystems.
[ OK ] Stopped target Local File Systems (Pre).
[ OK ] Stopped Create Static Device Nodes in /dev.
[ OK ] Stopped Create System Users.
[ OK ] Stopped Remount Root and Kernel File Systems.
[ OK ] Reached target Shutdown.
[ OK ] Reached target Final Step.
[ OK ] Started Reboot.
[ OK ] Reached target Reboot.
[ 68.092735] reboot: Restarting system

U-Boot SPL 2020.01-dirty (Mar 15 2020 - 09:59:33 +0000)
High speed PHY - Version: 2.0
Detected Device ID 6828
board SerDes lanes topology details:
| Lane # | Speed | Type |
|-----|-----|-----|
| 0      | 3     | SATA0 |
| 1      | 0     | SGMII1 |
| 2      | 5     | PCIe1 |
| 3      | 5     | USB3 HOST1 |
| 4      | 5     | USB3 HOST0 |
| 5      | 0     | SGMII2 |
|-----|-----|-----|
PCIe, Idx 1: detected no link
High speed PHY - Ended Successfully
mv_ddr: mv_ddr-armada-18.09.2
DDR3 Training Sequence - Switching XBAR Window to FastPath Window
mv_ddr: completed successfully
Trying to boot from SPI

U-Boot 2020.01-dirty (Mar 15 2020 - 09:59:33 +0000)

SoC: MV88F6028-B0 at 1600 MHz
DRAM: 2 GiB (800 MHz, 32-bit, ECC not enabled)
MMC: mv_sdh: 0
Loading Environment from SPI Flash... SF: Detected w25q32 with page size 256 Bytes, erase size 4 KiB, total 4 MiB
*** Warning - bad CRC, using default environment

Model: VT AIR 100
Board: Voleatech VT AIR 100
Invalid EEPROM Header
SCSI: MVEBU SATA INIT
SATA link 0 timeout.
AHCI 0001.0000 32 slots 2 ports 6 Gbps 0x3 impl SATA mode
flags: 64bit ncq led only pmp fbss pio slum part sxs

Net:
Warning: ethernet@70000 using MAC address from ROM
eth1: ethernet@70000
Error: ethernet@30000 address not set.

Error: ethernet@34000 address not set.

Hit any key to stop autoboot: 0
=>
```

Type “**run install**” to run the OS installer from your USB stick. The installer runs without any user inputs.

3.3.9 LEDs

The VT AIR 310 has multiple LEDs. They are indicating for example power on, connection and port activity. Ethernet port related LEDs are embedded in the RJ45 connectors, while the power indicator LED is located below the serial port.

The RJ45 NIC LEDs are configured the following way:

LED Activity	Explanation
Off	No connection
Green Light Only	100Mbit/s Speed
Green and Yellow Light	1000Mbit/s Speed

SFP LED

The SFP LED is software controlled and will be green if the configured and active SFP interface is up and has a physical connection to the other end. The SFP interface has to be configured and enabled for the LED to work otherwise it will stay off.

SHDSL LEDs

If your order includes a SHDSL card you will also have 2 LEDs on each SHDSL RJ45 connector. The left LED is for power on and will be on when the SHDSL port is ready to do a connection. The right LED has three different modes:

LED Activity	Explanation
Slow Blinking	Searching for remote modem
Fast Blinking	Connection parameters are being negotiated
Steady Light	Connection established

VDSL LEDs

If your order includes a VDSL card you will also have 2 LEDs on each RJ45 connector. The left LED is for power on and will be on when the VDSL port is ready to do a connection. The right LED has three different modes:

LED Activity	Explanation
Slow Blinking	Searching for remote modem
Fast Blinking	Connection parameters are being negotiated
Steady Light	Connection established

3.3.10 SHDSL

The optional SHDSL modems only use 2 PINs of the RJ45 connector, PIN4 and PIN5. It does not matter in which order two SHDSL modems are connected to each other the PINs can be swapped.

We add a RJ45 to 2 PIN connector for each SHDSL modem.



3.3.11 Operational Data

Operational Voltage

Item	Voltage	Current	Ambient Temperature
Front barrel connector	12 or 24 VDC	2.0 A	Max. 40°C
Phoenix/Euroblock connector	12 or 24 VDC	2.0 A	Max. 60°C

Environmental Data

The environmental temperature data are based upon the component with the lowest available temperature. Please make sure to check which addons you ordered and make sure not to exceed the allowed ambient temperature.

Warning: Failure to comply with the allowed ambient temperature may void the warranty of your device.

Ambient Temperature	Minimum	Maximum
Base Device/LTE	-20°C	60°C
VDSL	-20°C	50°C
SHDSL	-20°C	50°C
Humidity (non-condensing)	10 %	90 %

Leave a minimum of 2cm of space on both sides of the device when installed on a DIN Rail.

For ambient temperatures above 30°C, leave 5cm space on both sides of the device for air cooling to work properly.

Grounding

The device can be grounded through the DIN RAIL connector. The case dissipates high currents across the DIN RAIL connector.

The middle pin of the Phoenix plug can also be used as grounding. Please note that this can dissipate only a low current, in comparison to the DIN rail.

3.3.12 Warranty Terms and Conditions

Voleatech GmbH guarantees its hardware products against defects in workmanship and material for a period of one (1) year from the date of shipment. Under warranty, the customer's sole remedy and Voleatech's sole liability shall be, at Voleatech's sole discretion, to either repair or replace the defective hardware product at no charge. This warranty is void if the hardware product has been altered or damaged by an accident, misuse or abuse or is not operated according to this manual. For additional information on warranty and related topics like RMA, please visit www.voleatech.de.

Disclaimer of Warranty THIS WARRANTY IS MADE IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESSED, OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR A SPECIFIC PURPOSE, NONINFRINGEMENT OR THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION, EXCEPT THE WARRANTY EXPRESSLY STATED HEREIN. THE REMEDIES SET FORTH HEREIN SHALL BE THE SOLE AND EXCLUSIVE REMEDIES OF ANY CUSTOMER OR PURCHASER WITH RESPECT TO ANY DEFECTIVE PRODUCT.

Limitation on Liability UNDER NO CIRCUMSTANCES SHALL VOLEATECH GmbH BE LIABLE FOR ANY LOSS, DAMAGE OR EXPENSES INCURRED OR WITH RESPECT TO ANY DEFECTIVE PRODUCT. IN NO EVENT SHALL Voleatech GmbH BE LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES THAT CUSTOMER MAY SUFFER DIRECTLY OR INDIRECTLY FROM THE USAGE OF ANY PRODUCT. BY ORDERING THE VT AIR 310, THE CUSTOMER APPROVES THAT THE VT AIR 310, HARDWARE AND SOFTWARE, WAS THOROUGHLY TESTED AND HAS MET THE CUSTOMER'S REQUIREMENTS AND SPECIFICATIONS.

3.3.13 LEGAL NOTICE

Voleatech GmbH (hereinafter “Voleatech”) products and services are sold subject to Voleatech terms and conditions of sale, delivery and payment supplied at the time of purchase order acknowledgement. Voleatech warrants the performance of its products according to actual specifications at the date of shipment. Voleatech reserves the right to make changes to its products and specifications or to discontinue any product, product line or service without prior notice. Customers should make sure to obtain in each case the latest version of relevant product information from Voleatech and to always verify for themselves that their requirements are met and reference is up to date. Product testing and all additional quality control techniques are utilized to the extent that Voleatech deems necessary to support their warranty and warranty terms. Therefore detailed testing of all parameters in any product is not necessarily performed in full unless required by law or regulation. In order to minimize risks that may be associated with customer products, applications or services, the customer must use adequate design and operating safeguards to minimize any possible hazards. Voleatech is not liable for any applications assistance or customer product design and thus it is the customer’s sole responsibility to make the selection and usage of Voleatech products. Voleatech is not liable for any such selection or usage thereafter and neither is liable for the usage of any circuitry or components other than completely and entirely embodied in a Voleatech product. Furthermore Voleatech is not liable for its products commercial fit for any market segment envisioned by the customer. Voleatech products are not intended for use in life support systems, appliances, nuclear systems or systems where malfunction can reasonably be expected to result in personal injury, death or severe property or environmental damage. Any use of Voleatech’s products by the customer for such purposes is completely at the customer’s own risk. Voleatech does not grant any license -expressed or implied- on any patent right, copyright, mask work right, type or model protection or any other intellectual property right (IPR) of Voleatech covering or relating to any product combination, hardware, machine, software or process in which its products or services might be or are used. Any provision or publication of any third party’s products or services does not constitute Voleatech’s approval, license, warranty or endorsement thereof. Any third party trademarks contained in this document belong to the respective third party owner. Reproduction of content and information from Voleatech documents and manuals is permissible only if reproduction is without alteration and is accompanied by all associated copyright, proprietary and other notices (including this notice) and related conditions. Voleatech is not liable for any un-authorized alteration of such content and information or for any reliance related to alterations thereon. Any representations made, warranties given, and/or liabilities accepted by any person which differ from those contained in this manual or in Voleatech’s standard terms and conditions of sale, delivery and payment are made, given and/or accepted at customer’s own risk. Voleatech is not liable for any such representations, warranties or liabilities or for any reliance thereon by any person.

3.3.14 Regulatory

This chapter provides regulatory and compliance information about Voleatech’s VT AIR 310 -related information. Product name: VT AIR 310

Safety Notice

Before you begin using this product, please read the following safety information. Attention to these warnings will help prevent personal injuries and damage to the products. It is your responsibility to use the product in an appropriate manner. This product is designed for use solely indoor environments or, if expressly permitted, also in the field and must not be used in any way that may cause personal injury or property damage.

You are responsible if the product is used for any intention other than its designated purpose or in disregard of Voleatech’s instructions. Voleatech shall assume no responsibility for such use of the product. The product is used for its designated purpose if it is used in accordance with its product documentation and within its performance limits.

Safety Information and Notices

Never turn on or connect to power any equipment when there is evidence of mechanical damage, fire, exposure to water, or structural damage.

When not in use, avoid placing or storing the product in the following places or under the following conditions:

- Ambient temperature above 40°C
- Exposed to direct sunlight
- Humid or exposed to dust

Warning: This product does not contain any user replicable or serviceable parts. Do not take apart or attempt to service the product yourself.

Never remove the cover or any part of the housing of the product. The internal battery is not user replicable.

In the event of an equipment malfunction, all repairs must be performed either by Voleatech GmbH or by an authorized agent. It is the customer responsibility to report the need for service to Voleatech GmbH or to one of the authorized agents. For service information, contact Voleatech GmbH customer support.

Be careful not subject the product to strong impact.

If the product was subjected to a strong impact and/or falling over check carefully for any damage to the product. If such damage is observed the use of the product must be stopped immediately.

Operation

The product may be operated only under the operating conditions as specified by Voleatech GmbH. When the product is used for an extended period of time, and/or at high ambient temperature and/or exposed to direct sunlight it is normal for the product body to feel warm.

Avoid overheating the product. The product's ventilation should not be obstructed or blocked. If proper ventilation is not provided it can result in battery overheating or explosion of the battery resulting fire, burns or other injuries.

Stop using the product immediately if it emits smoke or a strange smell, or otherwise behaves abnormally.

Following are the required operating position and conditions:

- Do not place the product on unstable surfaces
- Do not place the product on elevated surface and secure it from falling from high places on passerby
- Do not place the product on heat-generating surface or near heat emitting devices or direct flame. Verify that there is sufficient clearance between the product and any other device exhaust warm air
- The product operating ambient range can be found at Environmental Data. Voleatech GmbH recommends that an ambient temperature of 0 to 40 °C (32 to 104 °F) and relative humidity of 30-50% is maintained during normal operation as this will result in better performance and longer life of the equipment. Temperature must not exceed the maximum temperature specified in Environmental Data.
- Do not expose the product to moisture or dust.
- The product is not liquid-proof; therefore, the equipment must be protected against penetration by liquids. If the necessary precautions are not taken, the user may suffer electric shock or the product itself may be damaged, which can also lead to personal injury.
- Never use the product under conditions in which condensation has formed or can form in or on the product, e.g. if the product has been moved from a cold to a warm environment. Penetration by water increases the risk of electric shock.

AC/DC Adapter or Power Supply - Electrical Safety

The following information on electrical safety must be observed, failing to follow these instruction may result in electric shock, fire and/or serious personal injury or death.

Use only the adapter or power supply supplied with the product or adapter or power supply with the following specifications:

Output voltage of 12V or 24V and current of at least 2A and not more than 3A.

Prior to powering the product and plugging the adapter or power supply to the mains supply, always ensure that the nominal voltage setting on the adapter or power supply matches the nominal voltage of the AC supply network.

If extension cords or connector strips are implemented, they must be checked on a regular basis to ensure that they are safe to use.

Never use the adapter or power supply if the power cable is damaged. Check the power cable on a regular basis to ensure that it is in proper operating condition. By taking appropriate safety measures and carefully laying the power cable, you can ensure that the cable will not be damaged and that no one can be hurt by, for example, tripping over the cable or suffering an electric shock.

Do not insert the plug into sockets that are dusty or dirty. Insert the plug firmly and all the way into the socket. Otherwise, sparks that result in fire and/or injuries may occur.

Do not overload any sockets, extension cords or connector strips; doing so can cause fire or electric shocks.

Do not insert or remove the plug with wet hands.

Never remove the cover or any part of the housing of the adapter or power supply, doing so will expose circuits and components and can lead to electric shock, injuries, fire or damage to the product.

The adapter or power supply operating ambient temperature range is of 0 to 40°C / 32 to 104 °F (storage temp range: -20 to 60 °C / -04 to 140 °F) maximum operating altitude is 2000 m ASL.

Use suitable overvoltage protection to ensure that no overvoltage (such as that caused by a bolt of lightning) can reach the product. Otherwise, the person operating the product will be exposed to the danger of an electric shock.

The product is not liquid-proof; therefore, the equipment must be protected against penetration by liquids. If the necessary precautions are not taken, the user may suffer electric shock or the product itself may be damaged, which can also lead to personal injury.

Never use the product under conditions in which condensation has formed or can form in or on the product, e.g. if the product has been moved from a cold to a warm environment. Penetration by water increases the risk of electric shock.

Prior to cleaning the product, disconnect it completely from the power supply. Use a soft, non-linting cloth to clean the product. Never use chemical cleaning agents such as alcohol, acetone or diluents for cellulose lacquers.

Electronic Emission Notices (EMC)

Federal Communications Commission Declaration of Conformity The following information refers to VT AIR 310. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Responsible Party: Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany

European Union - Compliance to the Electromagnetic Compatibility

(EMC) Directive or Radio Equipment Directive

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU (from 20 April, 2016) on the approximation of the laws of the Member States relating to electromagnetic compatibility.

Voleatech GmbH is not responsible for any radio or television interference caused by using other than specified or recommended cables and connectors or by unauthorized changes or modifications to this equipment.

Unauthorized changes or modifications could void the user's authority to operate the equipment.

WEEE and recycling statements

The WEEE marking on Voleatech GmbH products applies to countries with WEEE and e-waste regulations (for example, the European WEEE Directive). Appliances are labeled in accordance with local regulations concerning waste electrical and electronic equipment (WEEE).

These regulations determine the framework for the return and recycling of used appliances as applicable within each geography. This label is applied to various products to indicate that the product is not to be thrown away, but rather put in the established collection systems for reclaiming these end of life products.

Users of electrical and electronic equipment (EEE) with the WEEE marking must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to them for the return, recycle and recovery of WEEE and to minimize any potential effects of EEE on the environment and human health due to the presence of hazardous substances. Voleatech GmbH electrical and electronic equipment (EEE) may contain parts and components, which at end-of-life might qualify as hazardous waste.

EEE and waste electrical and electronic equipment (WEEE) can be delivered free of charge to the place of sale or any distributor that sells electrical and electronic equipment of the same nature and function as the used EEE or WEEE.



Restriction of Hazardous Substances (RoHS) European Union RoHS

This product, with included parts (cables, cords, and so on) meets the requirements of Directive 2011/65/EU and directive 2015/863/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment ("RoHS recast" or "RoHS 2").

EU Radio Directive Equipment (RED)

Declaration of Conformity (DoC)

Voleatech declares that the radio equipment for the VT AIR 310 is in compliance with Radio Equipment Directive 2014/53/EU.

LTE Modem

Warning: A safety distance of at least 20 cm must be kept between the product antenna and the operator or and other persons.

3.3.15 Contact Information and Resources

Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany

www.voleatech.de info@voleatech.de +49 7121 539 550

3.4 VT AIR 500

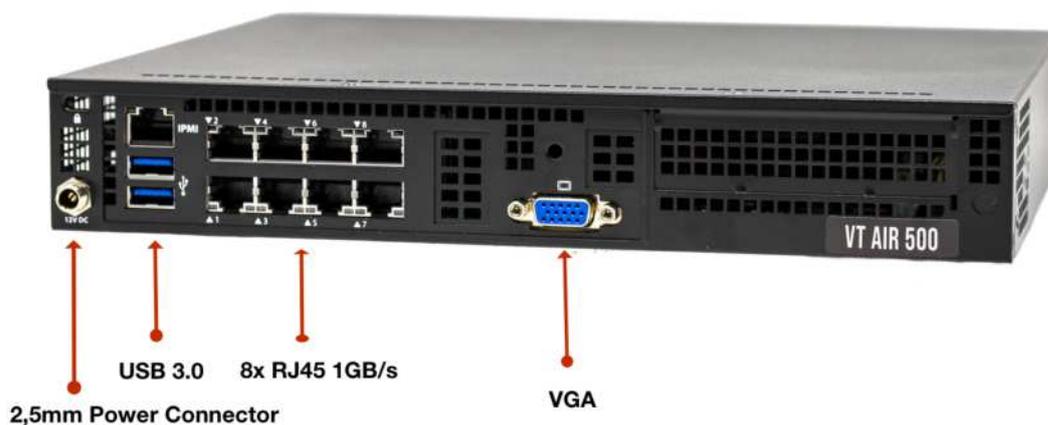


3.4.1 Overview

Summary of Features

CPU	Intel® Atom C3558
CPU Cores	4 Cores
NIC	8x 1Gbps Intel RJ45
Re- mote Man- age- ment	1x 1Gbps RJ45 IPMI
SSD	256 GB M.2 MLC SSD SATA
RAM	8 GB DDR4 ECC Reg. or 16 GB DDR4 ECC Reg.
Ex- pan- sion	None
Console Port	1x VGA
USB Ports	2x USB 2.0 ports
LED	Power/Status/SATA Activity
Size	Desktop
Cool- ing	Active control chassis fan
Power	12V 7A 2,5mm cylindrical barrel connector EU
En- vi- ro- ment	0°C to 35°C Operating Temp 8% to 90% Operating Relative Humidity (non-condensing)
Cer- tifi- cates	Electromagnetic Emissions: FCC Class B, EN 55032 Class B, EN 61000-3-2/3-3, CISPR 32 Class B Electromagnetic Immunity: EN 55024/CISPR 24 (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11) Other: VCCI-CISPR 32 and AS/NZS CISPR 32 Environmental: Directive 2011/65/EU, Directive 2012/19/EU Safety: CSA/EN/IEC/UL 60950-1 Compliant UL or CSA Listed (USA and Canada), CE Marking (Europe)
Soft- ware	VT AIR Linux

3.4.2 External Connectors



Certified Cables

The following is a list of industry-standard cables, sorted by type, with the necessary compliance requirements that have been proven to work well with the VT AIR product family.

These examples are the cables which Voleatech uses for testing and should provide enough information to source products from your preferred cable vendor.

- Ethernet cable: Monoprice 24AWG Cat6A 500MHz STP (max. 30m)
- USB Cable: USB 2.0 Type A Male to Male Cable

USB Connector

The front USB connector supports USB 2.0, connector type A. It can deliver up to 500 mA of power.

3.4.3 Packaging

The following items will be in the packaging of your VT AIR 500. Please make sure to check all items upon arrival of the device:

- VT AIR 500 Device in the enclosure
- Power cable

3.4.4 Ports

Front Connectors

Network Ports				
IPMI	eno2 (WAN)	eno4	eno6	eno8
	eno1 (LAN)	eno3	eno5	eno7

Label	Software Name	Features
LAN1	eno1	RJ45 1000/100/10 Mbit/s
LAN2	eno2	RJ45 1000/100/10 Mbit/s
LAN3	eno3	RJ45 1000/100/10 Mbit/s
LAN4	eno4	RJ45 1000/100/10 Mbit/s
WAN1	eno5	RJ45 1000/100/10 Mbit/s
WAN2	eno6	RJ45 1000/100/10 Mbit/s
WAN3	eno7	RJ45 1000/100/10 Mbit/s
WAN4	eno8	RJ45 1000/100/10 Mbit/s

The RJ45 ports support Autonegotiation and Full Duplex or Half Duplex on all speeds.

3.4.5 IPMI

The model comes equipped with an IPMI controller. The IPMI controller has a separate Network Interface but can also get its IP from a shared Network Port.

Warning: If you see a dhcp address being taken on the LAN port by default than is is the IPMI IP and not the Webgui

Note: Login Data are User: **ADMIN** (capital letters) Password: Provided on a sticker on the bottom or side of the device

3.4.6 Buttons

The **Reset Button** actually reboots the system immediatly. No config reset is performed. The **Power Button** will start or shutdown the system.

3.4.7 Power

The VT AIR 500 has 1 power cable connector.

3.4.8 VGA Console

The VT AIR 500 has a VGA port where you can connect a VGA monitor to see the console.

First Connection to TBF Appliance

All TBF Appliances have a default LAN IP Address of *192.168.1.1* and the DHCP Server is active on LAN. Please make sure to locate the *LAN* interface of your appliance in the manual.

Connect your computer to the LAN Interface and receive an IP Address from the DHCP Server. It will be in the 192.168.1.X range.

After receiving the IP Address open a supported browser and navigate to **https://192.168.1.1** A certificate warning will appear, since the TBF is using a self signed certificate. Please accept the certificate and continue to the page.

You will now be presented with the TBF login screen and you can use the default User and Password to login.

Note: User: admin Password: vtair

Please change the password after the first login.

3.4.9 VT AIR Reinstallation

Your VT AIR device comes pre-installed with its operating system. Should you ever need to reinstall the VT AIR operating system follow this guide.

Download the Installer File

You can download the installer file from your Portal (see [Downloads](#) for details). Make sure to download the file for your specific model/architecture.

USB Flash Drive Preparation

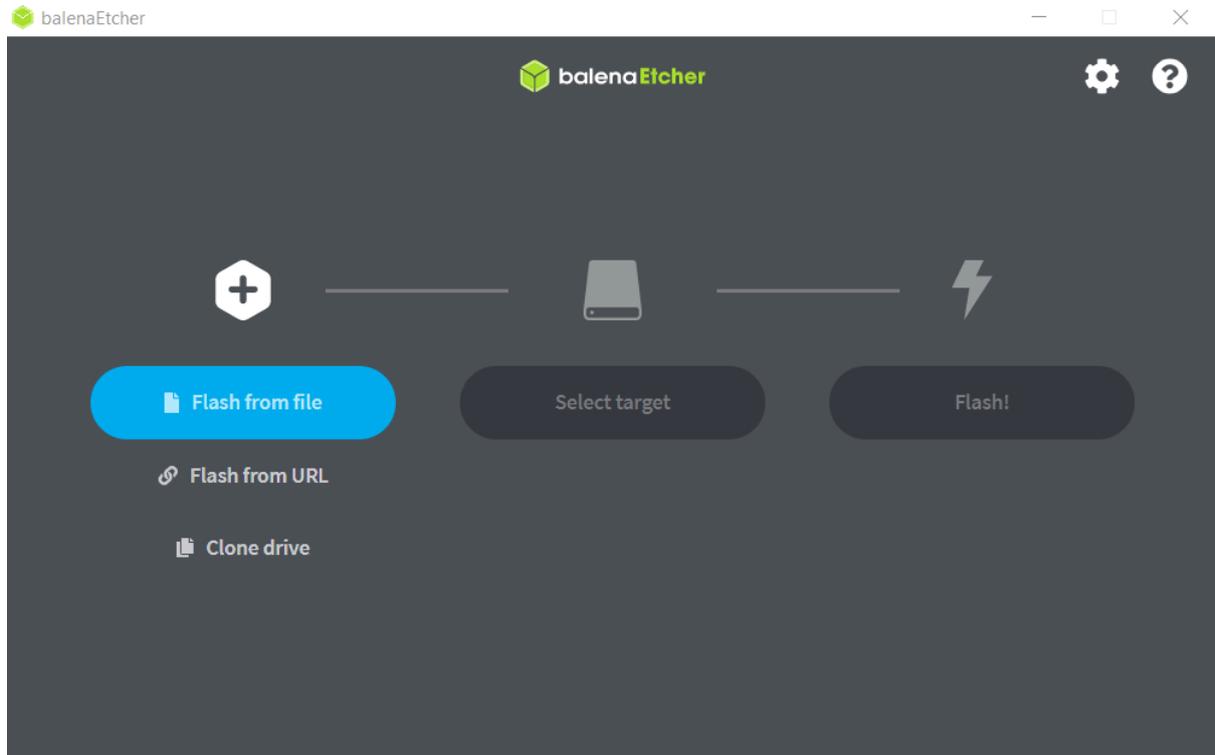
Once you downloaded the file make sure your USB flash drive is at least 2 GB in size. Also backup all your files from the USB flash drive since it will be formatted in the process and all files on it will be deleted.

Download the Software

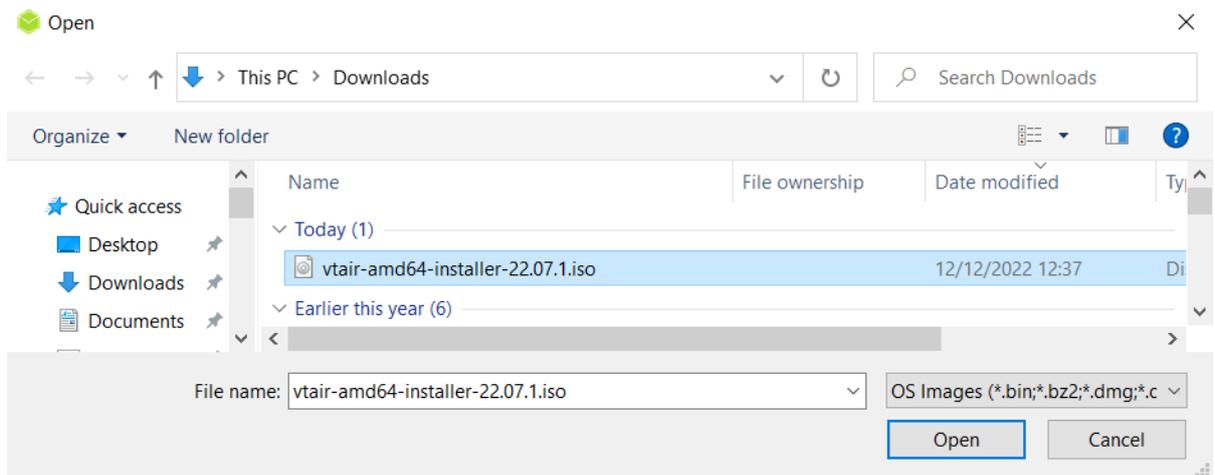
Download and install the software *balenaEtcher* from www.balena.io/etcher. It is available for Windows, macOS and Linux. Select the software for your specific operating system.

Use the Software

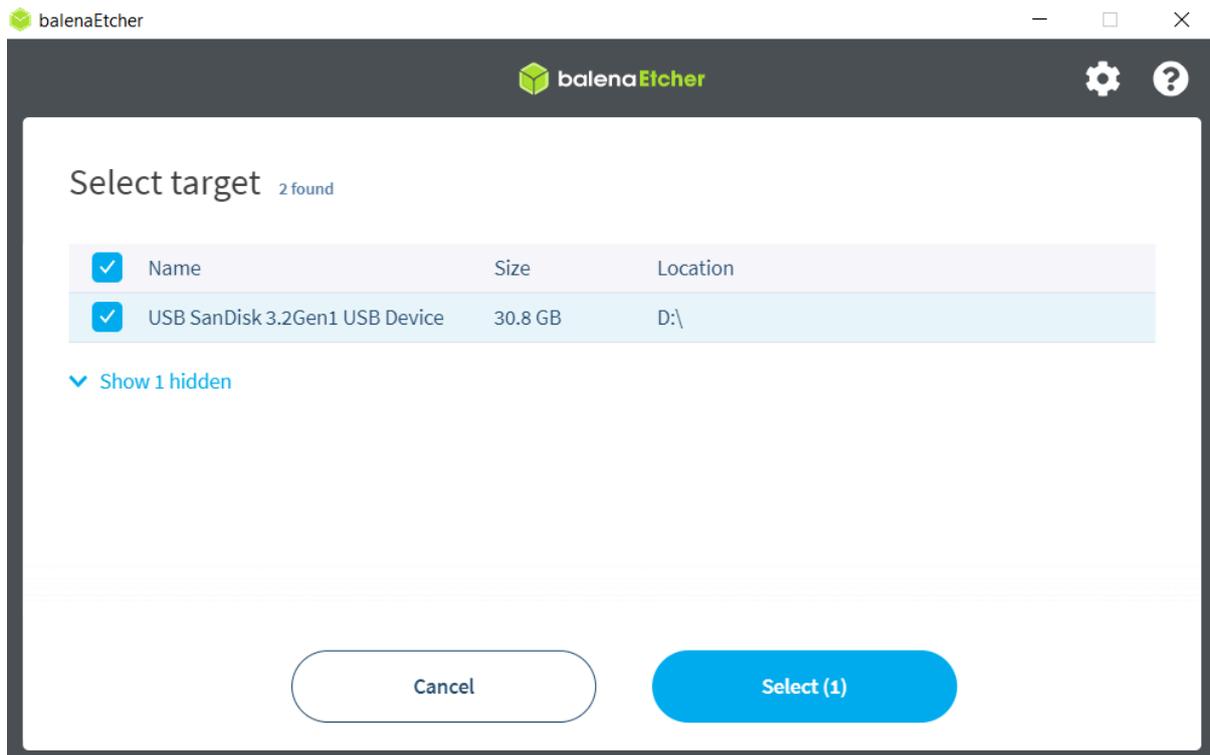
Insert your USB flash drive into the computer. Start the *balenaEtcher* software.



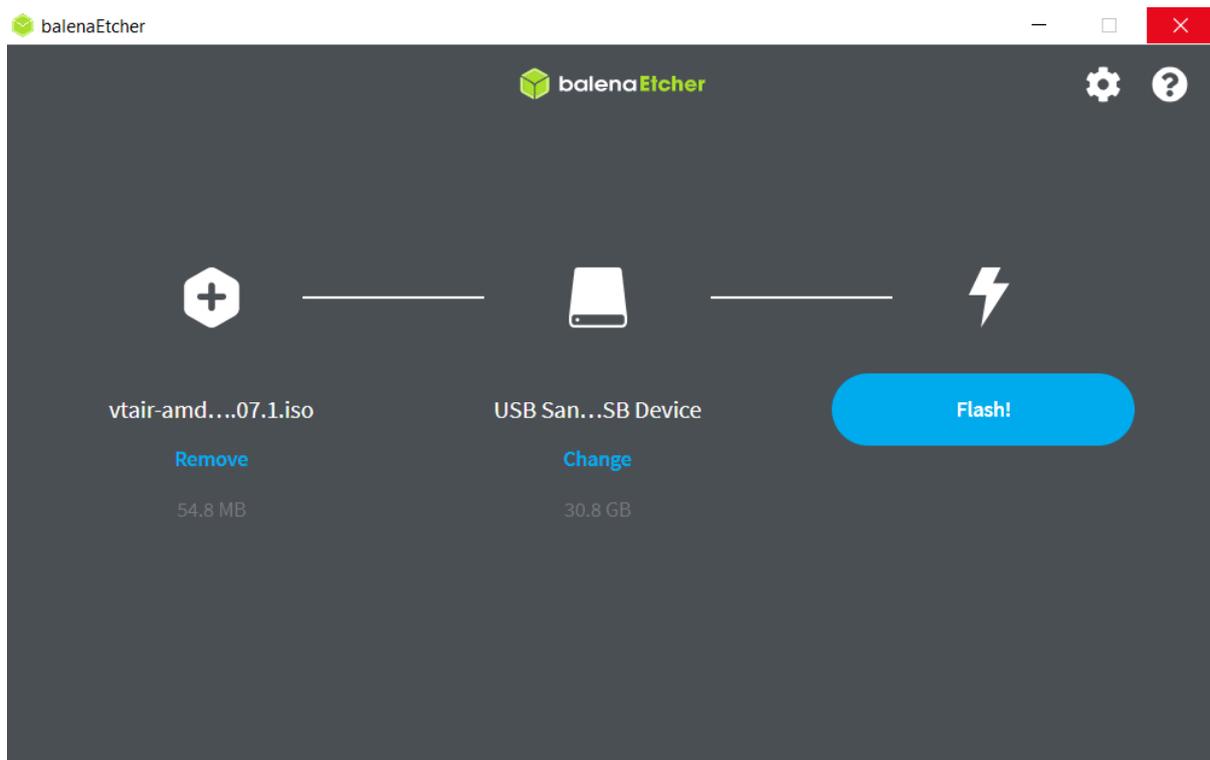
Press *Flash from file*



Select the downloaded installer file with the ending .iso



Select your USB flash drive as target



Press *Flash!* to complete and wait until the process is finished. Close the software and remove the USB flash drive from your computer.

Install the Software

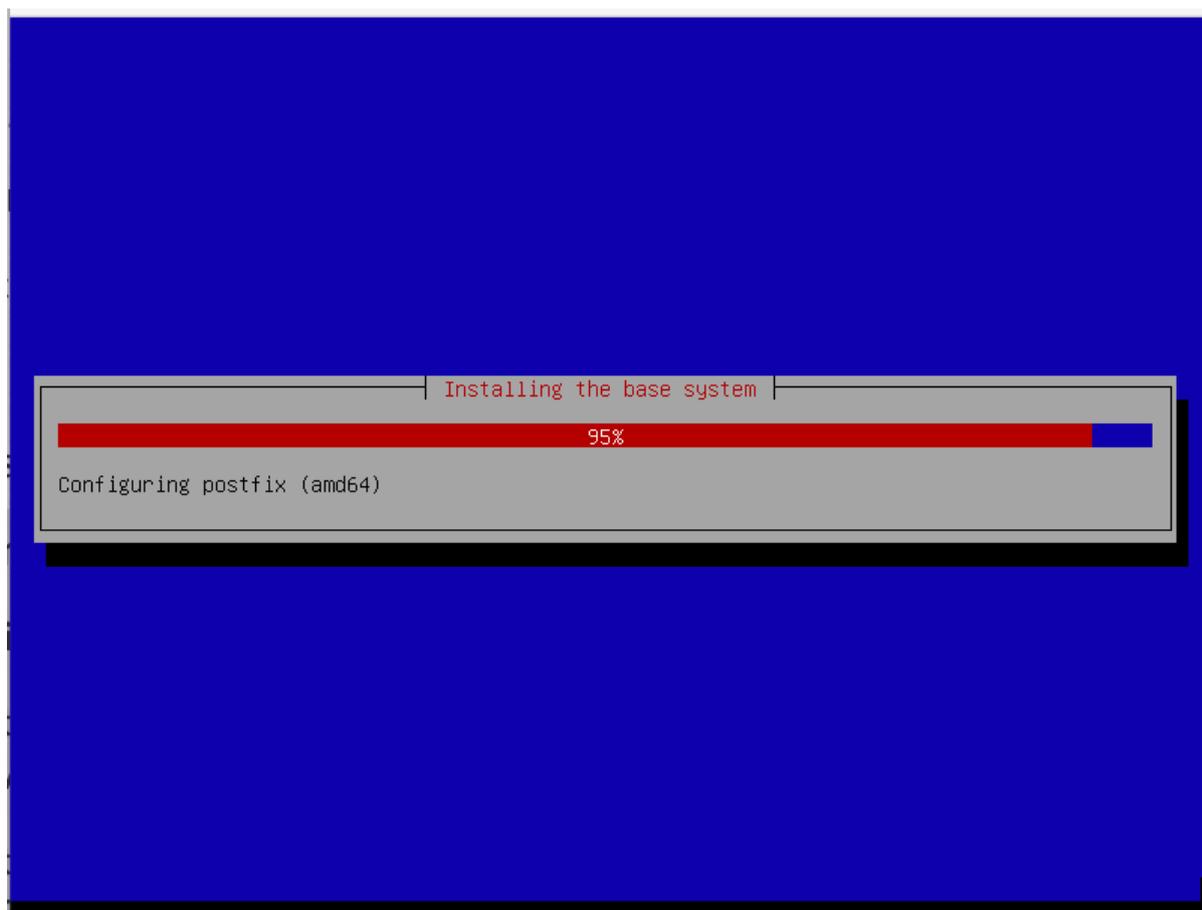
Insert the USB flash drive with the new VT AIR operating system in your VT AIR's USB port.

VGA Monitor Installation

Connect a monitor and keyboard to your VT AIR device. Reboot the device and press *F8* during the boot process to get into the boot menu. Select the USB key and boot from it.

In the installer choose **Install**.





The installer runs without any user inputs.

3.4.10 LEDs

The VT AIR 500 has multiple LEDs. They are indicating for example power on, connection and port activity. Ethernet port related LEDs are embedded in the RJ45 connectors, while the power indicator LED is located next the serial port.

The RJ45 NIC LEDs are configured the following way:

LED Activity	Explanation
Off	No connection
Green Light Only	100Mbit/s Speed
Green and Yellow Light	1000Mbit/s Speed

3.4.11 Operational Data

Operational Voltage

Item	Voltage	Current	Ambient Temperature
AC Voltage	100 - 240 V	0.5 - 2.5 A	Max. 45°C

Environmental Data

The environmental temperature data are based upon the component with the lowest available temperature. Please make sure to check which addons you ordered and make sure not to exceed the allowed

ambient temperature.

Warning: Failure to comply with the allowed ambient temperature may void the warranty of your device.

Ambient Temperature	Minimum	Maximum
Base Device	0°C	35°C
Humidity (non-condensing)	8 %	90 %

3.4.12 Warranty Terms and Conditions

Voleatech GmbH guarantees its hardware products against defects in workmanship and material for a period of one (1) year from the date of shipment. Under warranty, the customer's sole remedy and Voleatech's sole liability shall be, at Voleatech's sole discretion, to either repair or replace the defective hardware product at no charge. This warranty is void if the hardware product has been altered or damaged by an accident, misuse or abuse or is not operated according to this manual. For additional information on warranty and related topics like RMA, please visit voleatech.de.

Disclaimer of Warranty THIS WARRANTY IS MADE IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESSED, OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR A SPECIFIC PURPOSE, NON-INFRINGEMENT OR THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION, EXCEPT THE WARRANTY EXPRESSLY STATED HEREIN. THE REMEDIES SET FORTH HEREIN SHALL BE THE SOLE AND EXCLUSIVE REMEDIES OF ANY CUSTOMER OR PURCHASER WITH RESPECT TO ANY DEFECTIVE PRODUCT.

Limitation on Liability UNDER NO CIRCUMSTANCES SHALL VOLEATECH GmbH BE LIABLE FOR ANY LOSS, DAMAGE OR EXPENSES INCURRED OR WITH RESPECT TO ANY DEFECTIVE PRODUCT. IN NO EVENT SHALL Voleatech GmbH BE LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES THAT CUSTOMER MAY SUFFER DIRECTLY OR INDIRECTLY FROM THE USAGE OF ANY PRODUCT. BY ORDERING THE VT AIR 500, THE CUSTOMER APPROVES THAT THE VT AIR 500, HARDWARE AND SOFTWARE, WAS THOROUGHLY TESTED AND HAS MET THE CUSTOMER'S REQUIREMENTS AND SPECIFICATIONS.

3.4.13 Legal Notice

Voleatech GmbH (hereinafter "Voleatech") products and services are sold subject to Voleatech terms and conditions of sale, delivery and payment supplied at the time of purchase order acknowledgement. Voleatech warrants the performance of its products according to actual specifications at the date of shipment. Voleatech reserves the right to make changes to its products and specifications or to discontinue any product, product line or service without prior notice. Customers should make sure to obtain in each case the latest version of relevant product information from Voleatech and to always verify for themselves that their requirements are met and reference is up to date. Product testing and all additional quality control techniques are utilized to the extent that Voleatech deems necessary to support their warranty and warranty terms. Therefore detailed testing of all parameters in any product is not necessarily performed in full unless required by law or regulation. In order to minimize risks that may be associated with customer products, applications or services, the customer must use adequate design and operating safeguards to minimize any possible hazards. Voleatech is not liable for any applications assistance or customer product design and thus it is the customer's sole responsibility to make the selection and usage of Voleatech products. Voleatech is not liable for any such selection or usage thereafter and neither is liable for the usage of any circuitry or components other than completely and entirely embodied in a Voleatech product. Furthermore Voleatech is not liable for its products commercial fit for any market segment envisioned by the customer. Voleatech products are not intended for use in life support systems, appliances, nuclear systems or systems where malfunction can reasonably be expected to result in personal injury, death or severe property or environmental damage. Any use of Voleatech's

products by the customer for such purposes is completely at the customer's own risk. Voleatech does not grant any license -expressed or implied- on any patent right, copyright, mask work right, type or model protection or any other intellectual property right (IPR) of Voleatech covering or relating to any product combination, hardware, machine, software or process in which its products or services might be or are used. Any provision or publication of any third party's products or services does not constitute Voleatech's approval, license, warranty or endorsement thereof. Any third party trademarks contained in this document belong to the respective third party owner. Reproduction of content and information from Voleatech documents and manuals is permissible only if reproduction is without alteration and is accompanied by all associated copyright, proprietary and other notices (including this notice) and related conditions. Voleatech is not liable for any un-authorized alteration of such content and information or for any reliance related to alterations thereon. Any representations made, warranties given, and/or liabilities accepted by any person which differ from those contained in this manual or in Voleatech's standard terms and conditions of sale, delivery and payment are made, given and/or accepted at customer's own risk. Voleatech is not liable for any such representations, warranties or liabilities or for any reliance thereon by any person.

3.4.14 Regulatory

This chapter provides regulatory and compliance information about Voleatech's VT AIR 500 -related information. Product name: VT AIR 500

Safety Notice

Before you begin using this product, please read the following safety information. Attention to these warnings will help prevent personal injuries and damage to the products. It is your responsibility to use the product in an appropriate manner. This product is designed for use solely indoor environments or, if expressly permitted, also in the field and must not be used in any way that may cause personal injury or property damage.

You are responsible if the product is used for any intention other than its designated purpose or in disregard of Voleatech's instructions. Voleatech shall assume no responsibility for such use of the product. The product is used for its designated purpose if it is used in accordance with its product documentation and within its performance limits.

Safety Information and Notices

Never turn on or connect to power any equipment when there is evidence of mechanical damage, fire, exposure to water, or structural damage.

When not in use, avoid placing or storing the product in the following places or under the following conditions

- Ambient temperature above 45°C
- Exposed to direct sunlight
- Humid or exposed to dust

<p>Warning: This product does not contain any user replicable or serviceable parts. Do not take apart or attempt to service the product yourself.</p>
--

Never remove the cover or any part of the housing of the product. The internal battery is not user replicable.

In the event of an equipment malfunction, all repairs must be performed either by Voleatech GmbH or by an authorized agent. It is the customer responsibility to report the need for service to Voleatech GmbH or to one of the authorized agents. For service information, contact Voleatech GmbH customer support.

Be careful not subject the product to strong impact.

If the product was subjected to a strong impact and/or falling over check carefully for any damage to the product. If such damage is observed the use of the product must be stopped immediately.

Operation

The product may be operated only under the operating conditions as specified by Voleatech GmbH. When the product is used for an extended period of time, and/or at high ambient temperature and/or exposed to direct sunlight it is normal for the product body to feel warm.

Avoid overheating the product. The product's ventilation should not be obstructed or blocked. If proper ventilation is not provided it can result in battery overheating or explosion of the battery resulting fire, burns or other injuries.

Stop using the product immediately if it emits smoke or a strange smell, or otherwise behaves abnormally.

Following are the required operating position and conditions:

- Do not place the product on unstable surfaces
- Do not place the product on elevated surface and secure it from falling from high places on passerby
- Do not place the product on heat-generating surface or near heat emitting devices or direct flame. Verify that there is sufficient clearance between the product and any other device exhaust warm air.
- The product operating ambient range can be found at Environmental Data. Voleatech GmbH recommends that an ambient temperature of 0 to 40 °C (32 to 104 °F) and relative humidity of 30-50% is maintained during normal operation as this will result in better performance and longer life of the equipment. Temperature must not exceed the maximum temperature specified in Environmental Data.
- Do not expose the product to moisture or dust.
- The product is not liquid proof; therefore, the equipment must be protected against penetration by liquids. If the necessary precautions are not taken, the user may suffer electric shock or the product itself may be damaged, which can also lead to personal injury.
- Never use the product under conditions in which condensation has formed or can form in or on the product, e.g. if the product has been moved from a cold to a warm environment. Penetration by water increases the risk of electric shock.

Electronic Emission Notices (EMC)

Federal Communications Commission Declaration of Conformity The following information refers to VT AIR 500. This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

Responsible Party: Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany

WEEE and recycling statements

The WEEE marking on Voleatech GmbH products applies to countries with WEEE and e-waste regulations (for example, the European WEEE Directive). Appliances are labeled in accordance with local regulations concerning waste electrical and electronic equipment (WEEE).

These regulations determine the framework for the return and recycling of used appliances as applicable within each geography. This label is applied to various products to indicate that the product is not to be thrown away, but rather put in the established collection systems for reclaiming these end of life products.

Users of electrical and electronic equipment (EEE) with the WEEE marking must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to them for the return, recycle and recovery of WEEE and to minimize any potential effects of EEE on the environment and human health due to the presence of hazardous substances. Voleatech GmbH electrical and electronic

equipment (EEE) may contain parts and components, which at end-of-life might qualify as hazardous waste.

EEE and waste electrical and electronic equipment (WEEE) can be delivered free of charge to the place of sale or any distributor that sells electrical and electronic equipment of the same nature and function as the used EEE or WEEE.



Restriction of Hazardous Substances (RoHS) European Union RoHS

This product, with included parts (cables, cords, and so on) meets the requirements of Directive 2011/65/EU and directive 2015/863/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment ("RoHS recast" or "RoHS 2").

3.4.15 Contact Information and Resources

Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany

www.voleatech.de info@voleatech.de +49 7121 539 550

3.5 VT AIR 600



3.5.1 Overview

Summary of Features

CPU	ARM64
CPU Cores	4 Cores
NIC	2x 10GbE/1GbE SFP+/SFP Ports 4x 1Gbps RJ45
SSD	16 GB eMMC
RAM	4 GB DDR4
Ex-pan-sion	2x VDSL 1x LTE 1x mSATA
VDSL	ADSL ITU-T G.992.1/3/5, VDSL2 ITU-T G.993.2, TR-048/067, TR-100, TR-114, ITU-T G.inp, ITU-T G.vector ADSL2+ bis 24 Mbps, VDSL2 bis 200 Mbps
LTE	LTE: B1 (2100), B2 (1900), B3 (1800), B4 (AWS), B7 (2600), B12 (700ac), B13 (700c), B20 (800DD), B5 (850), B25 (1900), B26 (US 850 Ext), B29 (US 700de Lower), B41 (TDD 2500), B30 (2300 WCS) 3G/UMTS: B1 (2100), B2 (1900), B8 (900), B4 (AWS), B3 (1800), B5 (850) 300Mbit/s Download, 50Mbit/s Upload
Console Port	1x USB
USB Ports	2x USB 2.0 ports
Mounting	DIN rail mount
Power	12V via 1x 2.5mm DC plug
En-vi-ro-ment	0°C to 35°C Operating Temp
Cer-tifi-cates	CE, FCC, RoHS
Soft-ware	VT AIR Linux

3.5.2 Industrial Usage

The product can be used in an office environment.

Electromagnetic Immunity: EN 55024, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11, EN 61000-6-2, EN 61326-1, IEC 61131-2
 Electromagnetic Emission: FCC Class B, EN 55032, EN 61000-3-2, EN 61000-3-3, EN 61000-6-4
 Safety: EN 60950-1

3.5.3 External Connectors

Certified Cables

The following is a list of industry-standard cables, sorted by type, with the necessary compliance requirements that have been proven to work well with the VT AIR product family.

These examples are the cables which Voleatech uses for testing and should provide enough information to source products from your preferred cable vendor.

- Ethernet cable: Monoprice 24AWG Cat6A 500MHz STP (max. 30m)
- USB Cable: USB 2.0 Type A Male to Male Cable
- USB Console Cable: USB 2.0 Type A Male to USB 2.0 Micro B Male Cable

USB Connector

The front USB connector supports USB 2.0 (Data rate of maximum 480 Mbit/s), connector type A. It can deliver up to 500 mA of power on each port.

LTE

If you bought the optional LTE configuration the Antenna can be mounted directly at the top of the unit. If you choose to use an Antenna cable, the device is certified for a cable length of up to 1m.

The main Antenna is in the back towards the DIN RAIL connector, the auxiliary Antenna is at the front of the device.

3.5.4 Packaging

The following items will be in the packaging of your VT AIR 600. Please make sure to check all items upon arrival of the device:

- VT AIR 600 Device in the enclosure
- Power adapter - 110V/220V US or EU plug
- USB Console Cable: USB 2.0 Type A Male to USB 2.0 Micro B Male Cable
- LTE Antennas (Only with LTE Kit)

Additionally, your device comes with different ports depending on your order:

- 1x or 2x VDSL
- LTE Kit
- mSATA

3.5.5 Ports

Front Conenctors

Network Ports					
eno0 (WAN)	eno1 (LAN)	eno2	eno3	eno4 (SFP)	eno5 (SFP)

Label	Software Name	Features
WAN	eno0	RJ45 1000/100/10 Mbit/s
LAN	eno1	RJ45 1000/100/10 Mbit/s
1	eno2	RJ45 1000/100/10 Mbit/s
2	eno3	RJ45 1000/100/10 Mbit/s
3	eno4	SFP+/SFP (10000/1000 Mbit/s)
4	eno5	SFP+/SFP (10000/1000 Mbit/s)

The RJ45 ports support Autonegotiation and Full Duplex or Half Duplex on all speeds.

The SFP/SFP+ Ports support the following Modules:

- 10Gb BaseT/SR/LR/LRM/ER/CR
- 1Gb BaseT/SR/LR/CR

There is no vendor lock for SFP modules. You can use any Module that conforms to the standard.

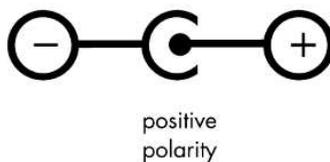
3.5.6 Power

The VT AIR 600 has 1 power connector:

- 12VDC barrel connector

12VDC barrel connector

A suitable external power supply must be connected to the DC power socket, which has the dimensions 5.5mm x 2.5 mm cylindrical barrel connector. The power supply must be 12VDC. Recommended values are: 12VDC/2A (no more than 5A). Please note that the DC jack must have positive polarity in the center pin:



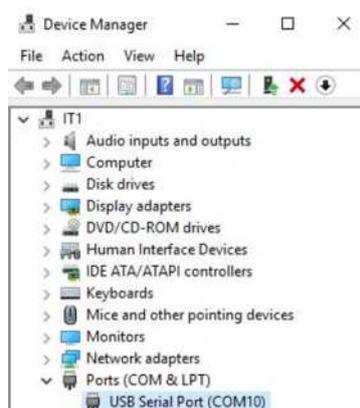
Warning: Please be aware that the maximum temperature for the barrel connector is 40°C.

3.5.7 USB Console

The appliance has a UART to USB bridge allowing convenient connection to the device console. Such serial console connection is of USB-to-UART type. The connection speed should be set to 115200 bps. All modern Operating Systems have a driver for the UART.

Windows

First you have to locate the COM Port number. Open the Device Manager and expand the section for Ports (COM & LPT). Look for an entry with a title such as USB Serial Port. A label is next to the name (COMX) where X is a number.



MacOSX

In OSX the device shows up at `/dev/tty.usbserial-XXXXXX` where X is a series of numbers and letters.

Linux

In Linux the device shows up at `/dev/ttyUSBX` where X is a number. You can also have a look at the output of `dmesg` to locate the newly connected device.

Terminal Program

A terminal program is required to open the connected serial port. We recommend:

OS	Program
Windows	Putty
MacOSX	Screen, Serial
Linux	Screen

First Connection to TBF Appliance

All TBF Appliances have a default LAN IP Address of `192.168.1.1` and the DHCP Server is active on LAN. Please make sure to locate the *LAN* interface of your appliance in the manual.

Connect your computer to the LAN Interface and receive an IP Address from the DHCP Server. It will be in the `192.168.1.X` range.

After receiving the IP Address open a supported browser and navigate to <https://192.168.1.1> A certificate warning will appear, since the TBF is using a self signed certificate. Please accept the certificate and continue to the page.

You will now be presented with the TBF login screen and you can use the default User and Password to login.

Note: User: admin Password: vtair

Please change the password after the first login.

3.5.8 VT AIR Reinstallation

Your VT AIR device comes pre-installed with its operating system. Should you ever need to reinstall the VT AIR operating system follow this guide.

Download the Installer File

You can download the installer file from your Portal (see [Downloads](#) for details). Make sure to download the file for your specific model/architecture.

USB Flash Drive Preparation

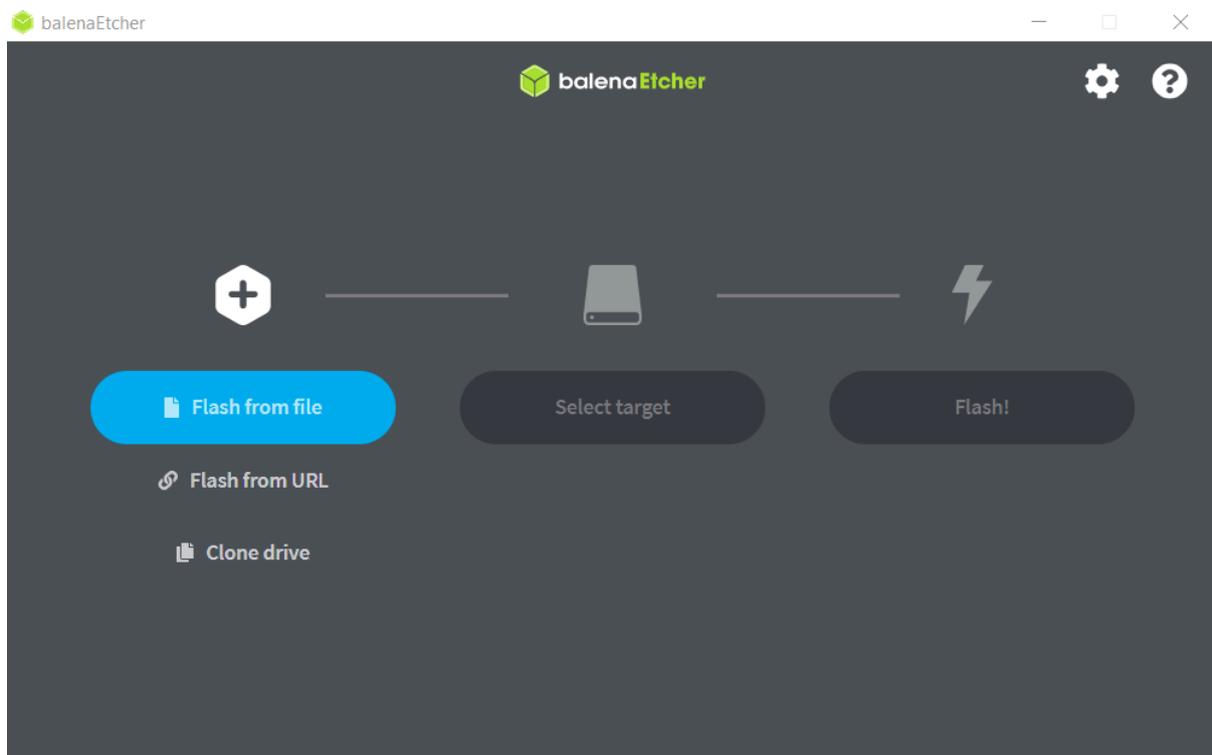
Once you downloaded the file make sure your USB flash drive is at least 2 GB in size. Also backup all your files from the USB flash drive since it will be formatted in the process and all files on it will be deleted.

Download the Software

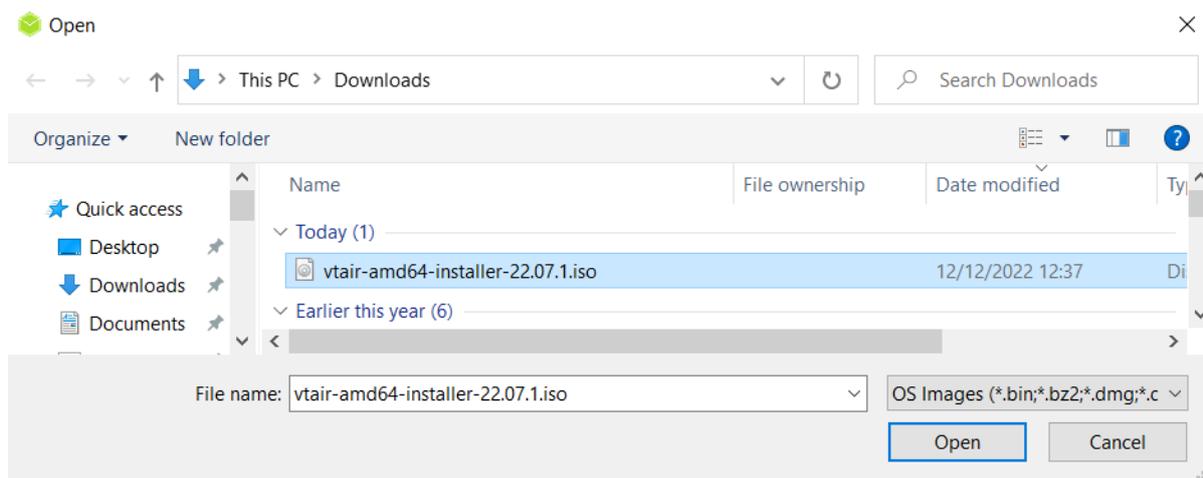
Download and install the software *balenaEtcher* from www.balena.io/etcher. It is available for Windows, macOS and Linux. Select the software for your specific operating system.

Use the Software

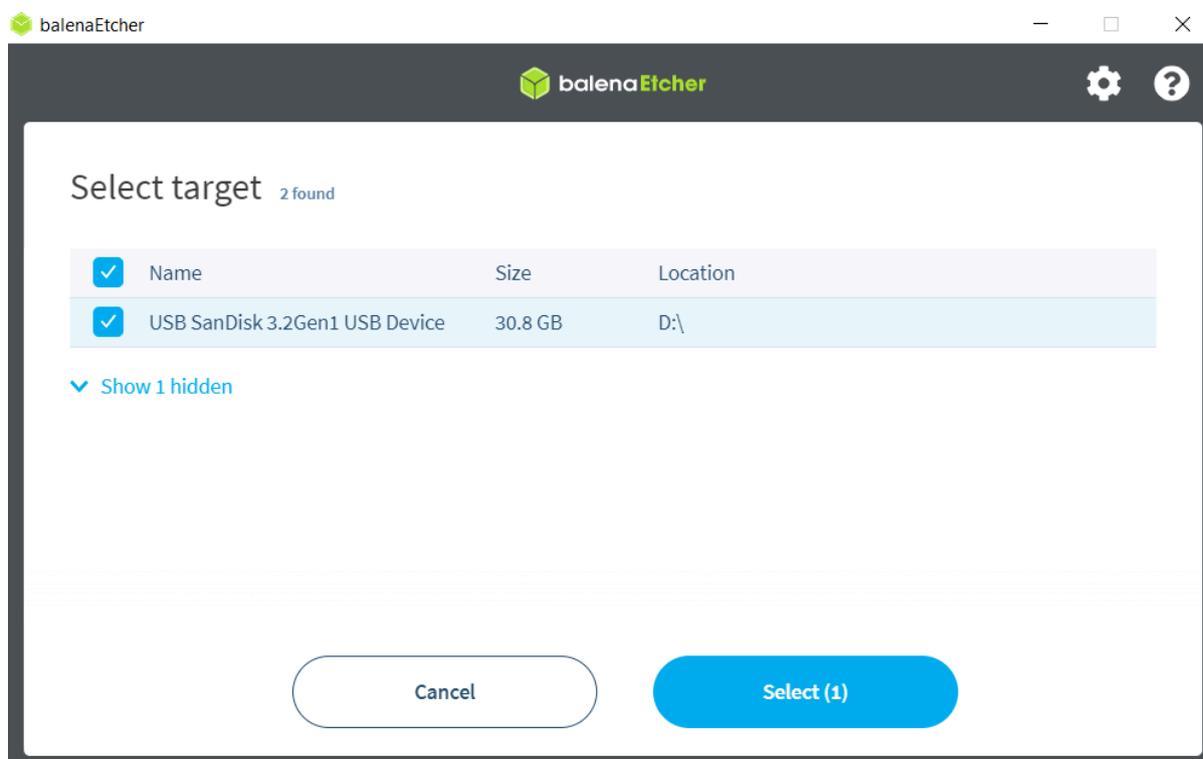
Insert your USB flash drive into the computer. Start the *balenaEtcher* software.



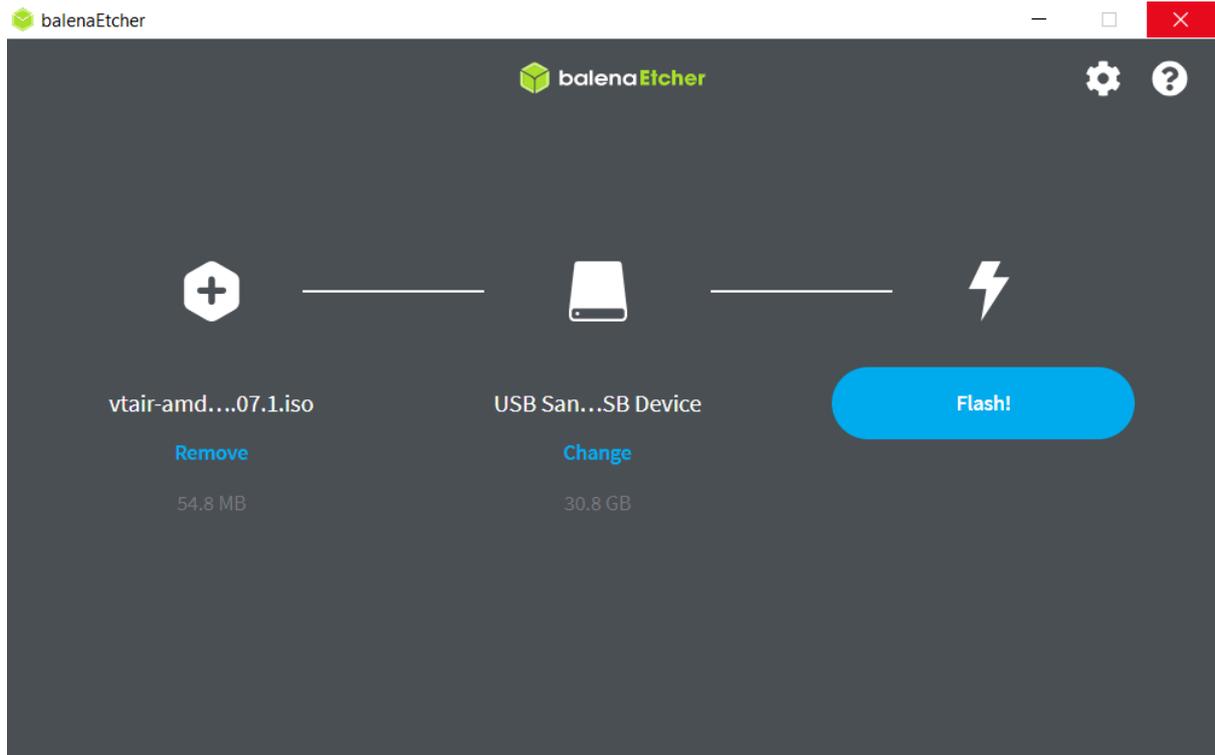
Press *Flash from file*



Select the downloaded installer file with the ending .iso



Select your USB flash drive as target



Press *Flash!* to complete and wait until the process is finished. Close the software and remove the USB flash drive from your computer.

Install the Software

Insert the USB flash drive with the new VT AIR operating system in your VT AIR's USB port.

Serial Console Installation

Connect the USB cable to the Console USB port of your VT AIR device and your computer. On your computer connect to your VT AIR's Console (see [Console Access](#)).

Type **"reboot"** to reboot the system. In the boot process you'll see a timer that you can interrupt by pressing any key. This gives you a shell from where you can reinstall your OS.

```
[ OK ] Reached target Unmount All Filesystems.
[ OK ] Stopped target Local File Systems (Pre).
[ OK ] Stopped Create Static Device Nodes in /dev.
[ OK ] Stopped Create System Users.
[ OK ] Stopped Remount Root and Kernel File Systems.
[ OK ] Reached target Shutdown.
[ OK ] Reached target Final Step.
[ OK ] Started Reboot.
[ OK ] Reached target Reboot.
[ 68.092735] reboot: Restarting system

U-Boot SPL 2020.01-dirty (Mar 15 2020 - 09:59:33 +0000)
High speed PHY - Version: 2.0
Detected Device ID 6828
board SerDes lanes topology details:
| Lane # | Speed | Type |
|-----|-----|-----|
| 0      | 3     | SATA0 |
| 1      | 0     | SGMII1 |
| 2      | 5     | PCIe1 |
| 3      | 5     | USB3 HOST1 |
| 4      | 5     | USB3 HOST0 |
| 5      | 0     | SGMII2 |
|-----|-----|-----|
PCIe, Idx 1: detected no link
High speed PHY - Ended Successfully
mv_ddr: mv_ddr-armada-18.09.2
DDR3 Training Sequence - Switching XBAR Window to FastPath Window
mv_ddr: completed successfully
Trying to boot from SPI

U-Boot 2020.01-dirty (Mar 15 2020 - 09:59:33 +0000)

SoC: MV88F6028-B0 at 1600 MHz
DRAM: 2 GiB (800 MHz, 32-bit, ECC not enabled)
MMC: mv_sdh: 0
Loading Environment from SPI Flash... SF: Detected w25q32 with page size 256 Bytes, erase size 4 KiB, total 4 MiB
*** Warning - bad CRC, using default environment

Model: VT AIR 100
Board: Voleatech VT AIR 100
Invalid EEPROM Header
SCSI: MVEBU SATA INIT
SATA link 0 timeout.
AHCI 0001.0000 32 slots 2 ports 6 Gbps 0x3 impl SATA mode
flags: 64bit ncq led only pmp fbss pio slum part sxs

Net:
Warning: ethernet@70000 using MAC address from ROM
eth1: ethernet@70000
Error: ethernet@30000 address not set.

Error: ethernet@34000 address not set.

Hit any key to stop autoboot: 0
=>
```

Type “**run install**” to run the OS installer from your USB stick. The installer runs without any user inputs.

3.5.9 LEDs

The VT AIR 600 has multiple LEDs. They are indicating for example power on, connection and port activity. Ethernet port related LEDs are embedded in the RJ45 connectors, while the power indicator LED is located below the serial port.

The RJ45 NIC LEDs are configured the following way:

LED Activity	Explanation
Off	No connection
Green Light Only	100Mbit/s Speed
Green and Yellow Light	1000Mbit/s Speed

SFP LED

The SFP LED is software controlled and will be green if the configured and active SFP interface is up and has a physical connection to the other end. The SFP interface has to be configured and enabled for the LED to work otherwise it will stay off.

VDSL LEDS

If your order includes a VDSL card you will also have 2 LEDs on each RJ45 connector. The left LED is for power on and will be on when the VDSL port is ready to do a connection. The right LED has three different modes:

LED Activity	Explanation
Slow Blinking	Searching for remote modem
Fast Blinking	Connection parameters are being negotiated
Steady Light	Connection established

3.5.10 Operational Data

Operational Voltage

Item	Voltage	Current	Ambient Temperature
Front barrel connector	12 VDC	2.0 A	Max. 35°C

3.5.11 Warranty Terms and Conditions

Voleatech GmbH guarantees its hardware products against defects in workmanship and material for a period of one (1) year from the date of shipment. Under warranty, the customer's sole remedy and Voleatech's sole liability shall be, at Voleatech's sole discretion, to either repair or replace the defective hardware product at no charge. This warranty is void if the hardware product has been altered or damaged by an accident, misuse or abuse or is not operated according to this manual. For additional information on warranty and related topics like RMA, please visit www.voleatech.de.

Disclaimer of Warranty THIS WARRANTY IS MADE IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESSED, OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR A SPECIFIC PURPOSE, NONINFRINGEMENT OR THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION, EXCEPT THE WARRANTY EXPRESSLY STATED HEREIN. THE REMEDIES SET FORTH HEREIN SHALL BE THE SOLE AND EXCLUSIVE REMEDIES OF ANY CUSTOMER OR PURCHASER WITH RESPECT TO ANY DEFECTIVE PRODUCT.

Limitation on Liability UNDER NO CIRCUMSTANCES SHALL VOLEATECH GmbH BE LIABLE FOR ANY LOSS, DAMAGE OR EXPENSES INCURRED OR WITH RESPECT TO ANY DEFECTIVE PRODUCT. IN NO EVENT SHALL Voleatech GmbH BE LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES THAT CUSTOMER MAY SUFFER DIRECTLY OR INDIRECTLY FROM THE USAGE OF ANY PRODUCT. BY ORDERING THE VT AIR 600, THE CUSTOMER APPROVES THAT THE VT AIR 600, HARDWARE AND SOFTWARE, WAS THOROUGHLY TESTED AND HAS MET THE CUSTOMER'S REQUIREMENTS AND SPECIFICATIONS.

3.5.12 LEGAL NOTICE

Voleatech GmbH (hereinafter "Voleatech") products and services are sold subject to Voleatech terms and conditions of sale, delivery and payment supplied at the time of purchase order acknowledgement. Voleatech warrants the performance of its products according to actual specifications at the date of shipment. Voleatech reserves the right to make changes to its products and specifications or to discontinue any product, product line or service without prior notice. Customers should make sure to obtain in each case the latest version of relevant product information from Voleatech and to always verify for themselves that their requirements are met and reference is up to date. Product testing and all additional quality control techniques are utilized to the extent that Voleatech deems necessary to support their warranty and warranty terms. Therefore detailed testing of all parameters in any product is not necessarily performed in full unless required by law or regulation. In order to minimize risks that may be associated

with customer products, applications or services, the customer must use adequate design and operating safeguards to minimize any possible hazards. Voleatech is not liable for any applications assistance or customer product design and thus it is the customer's sole responsibility to make the selection and usage of Voleatech products. Voleatech is not liable for any such selection or usage thereafter and neither is liable for the usage of any circuitry or components other than completely and entirely embodied in a Voleatech product. Furthermore Voleatech is not liable for its products commercial fit for any market segment envisioned by the customer. Voleatech products are not intended for use in life support systems, appliances, nuclear systems or systems where malfunction can reasonably be expected to result in personal injury, death or severe property or environmental damage. Any use of Voleatech's products by the customer for such purposes is completely at the customer's own risk. Voleatech does not grant any license -expressed or implied- on any patent right, copyright, mask work right, type or model protection or any other intellectual property right (IPR) of Voleatech covering or relating to any product combination, hardware, machine, software or process in which its products or services might be or are used. Any provision or publication of any third party's products or services does not constitute Voleatech's approval, license, warranty or endorsement thereof. Any third party trademarks contained in this document belong to the respective third party owner. Reproduction of content and information from Voleatech documents and manuals is permissible only if reproduction is without alteration and is accompanied by all associated copyright, proprietary and other notices (including this notice) and related conditions. Voleatech is not liable for any un-authorized alteration of such content and information or for any reliance related to alterations thereon. Any representations made, warranties given, and/or liabilities accepted by any person which differ from those contained in this manual or in Voleatech's standard terms and conditions of sale, delivery and payment are made, given and/or accepted at customer's own risk. Voleatech is not liable for any such representations, warranties or liabilities or for any reliance thereon by any person.

3.5.13 Regulatory

This chapter provides regulatory and compliance information about Voleatech's VT AIR 600 -related information. Product name: VT AIR 600

Safety Notice

Before you begin using this product, please read the following safety information. Attention to these warnings will help prevent personal injuries and damage to the products. It is your responsibility to use the product in an appropriate manner. This product is designed for use solely indoor environments or, if expressly permitted, also in the field and must not be used in any way that may cause personal injury or property damage.

You are responsible if the product is used for any intention other than its designated purpose or in disregard of Voleatech's instructions. Voleatech shall assume no responsibility for such use of the product. The product is used for its designated purpose if it is used in accordance with its product documentation and within its performance limits.

Safety Information and Notices

Never turn on or connect to power any equipment when there is evidence of mechanical damage, fire, exposure to water, or structural damage.

When not in use, avoid placing or storing the product in the following places or under the following conditions:

- Ambient temperature above 40°C
- Exposed to direct sunlight
- Humid or exposed to dust

<p>Warning: This product does not contain any user replicable or serviceable parts. Do not take apart or attempt to service the product yourself.</p>
--

Never remove the cover or any part of the housing of the product. The internal battery is not user replicable.

In the event of an equipment malfunction, all repairs must be performed either by Voleatech GmbH or by an authorized agent. It is the customer responsibility to report the need for service to Voleatech GmbH or to one of the authorized agents. For service information, contact Voleatech GmbH customer support.

Be careful not subject the product to strong impact.

If the product was subjected to a strong impact and/or falling over check carefully for any damage to the product. If such damage is observed the use of the product must be stopped immediately.

Operation

The product may be operated only under the operating conditions as specified by Voleatech GmbH. When the product is used for an extended period of time, and/or at high ambient temperature and/or exposed to direct sunlight it is normal for the product body to feel warm.

Avoid overheating the product. The product's ventilation should not be obstructed or blocked. If proper ventilation is not provided it can result in battery overheating or explosion of the battery resulting fire, burns or other injuries.

Stop using the product immediately if it emits smoke or a strange smell, or otherwise behaves abnormally.

Following are the required operating position and conditions:

- Do not place the product on unstable surfaces
- Do not place the product on elevated surface and secure it from falling from high places on passerby
- Do not place the product on heat-generating surface or near heat emitting devices or direct flame. Verify that there is sufficient clearance between the product and any other device exhaust warm air
- The product operating ambient range can be found at Environmental Data. Voleatech GmbH recommends that an ambient temperature of 0 to 40 °C (32 to 104 °F) and relative humidity of 30-50% is maintained during normal operation as this will result in better performance and longer life of the equipment. Temperature must not exceed the maximum temperature specified in Environmental Data.
- Do not expose the product to moisture or dust.
- The product is not liquid-proof; therefore, the equipment must be protected against penetration by liquids. If the necessary precautions are not taken, the user may suffer electric shock or the product itself may be damaged, which can also lead to personal injury.
- Never use the product under conditions in which condensation has formed or can form in or on the product, e.g. if the product has been moved from a cold to a warm environment. Penetration by water increases the risk of electric shock.

AC/DC Adapter or Power Supply - Electrical Safety

The following information on electrical safety must be observed, failing to follow these instruction may result in electric shock, fire and/or serious personal injury or death.

Use only the adapter or power supply supplied with the product or adapter or power supply with the following specifications:

Output voltage of 12V or 24V and current of at least 2A and not more than 3A.

Prior to powering the product and plugging the adapter or power supply to the mains supply, always ensure that the nominal voltage setting on the adapter or power supply matches the nominal voltage of the AC supply network.

If extension cords or connector strips are implemented, they must be checked on a regular basis to ensure that they are safe to use.

Never use the adapter or power supply if the power cable is damaged. Check the power cable on a regular basis to ensure that it is in proper operating condition. By taking appropriate safety measures and carefully laying the power cable, you can ensure that the cable will not be damaged and that no one can be hurt by, for example, tripping over the cable or suffering an electric shock.

Do not insert the plug into sockets that are dusty or dirty. Insert the plug firmly and all the way into the socket. Otherwise, sparks that result in fire and/or injuries may occur.

Do not overload any sockets, extension cords or connector strips; doing so can cause fire or electric shocks.

Do not insert or remove the plug with wet hands.

Never remove the cover or any part of the housing of the adapter or power supply, doing so will expose circuits and components and can lead to electric shock, injuries, fire or damage to the product.

The adapter or power supply operating ambient temperature range is of 0 to 40°C / 32 to 104 °F (storage temp range: -20 to 60 °C / -04 to 140 °F) maximum operating altitude is 2000 m ASL.

Use suitable overvoltage protection to ensure that no overvoltage (such as that caused by a bolt of lightning) can reach the product. Otherwise, the person operating the product will be exposed to the danger of an electric shock.

The product is not liquid-proof; therefore, the equipment must be protected against penetration by liquids. If the necessary precautions are not taken, the user may suffer electric shock or the product itself may be damaged, which can also lead to personal injury.

Never use the product under conditions in which condensation has formed or can form in or on the product, e.g. if the product has been moved from a cold to a warm environment. Penetration by water increases the risk of electric shock.

Prior to cleaning the product, disconnect it completely from the power supply. Use a soft, non-linting cloth to clean the product. Never use chemical cleaning agents such as alcohol, acetone or diluents for cellulose lacquers.

Electronic Emission Notices (EMC)

Federal Communications Commission Declaration of Conformity The following information refers to VT AIR 600. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Responsible Party: Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany

European Union - Compliance to the Electromagnetic Compatibility

(EMC) Directive or Radio Equipment Directive

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU (from 20 April, 2016) on the approximation of the laws of the Member States relating to electromagnetic compatibility.

Voleatech GmbH is not responsible for any radio or television interference caused by using other than specified or recommended cables and connectors or by unauthorized changes or modifications to this equipment.

Unauthorized changes or modifications could void the user's authority to operate the equipment.

WEEE and recycling statements

The WEEE marking on Voleatech GmbH products applies to countries with WEEE and e-waste regulations (for example, the European WEEE Directive). Appliances are labeled in accordance with local regulations concerning waste electrical and electronic equipment (WEEE).

These regulations determine the framework for the return and recycling of used appliances as applicable within each geography. This label is applied to various products to indicate that the product is not to be thrown away, but rather put in the established collection systems for reclaiming these end of life products.

Users of electrical and electronic equipment (EEE) with the WEEE marking must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to them for the return, recycle and recovery of WEEE and to minimize any potential effects of EEE on the environment and human health due to the presence of hazardous substances. Voleatech GmbH electrical and electronic equipment (EEE) may contain parts and components, which at end-of-life might qualify as hazardous waste.

EEE and waste electrical and electronic equipment (WEEE) can be delivered free of charge to the place of sale or any distributor that sells electrical and electronic equipment of the same nature and function as the used EEE or WEEE.



Restriction of Hazardous Substances (RoHS) European Union RoHS

This product, with included parts (cables, cords, and so on) meets the requirements of Directive 2011/65/EU and directive 2015/863/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment (“RoHS recast” or “RoHS 2”).

EU Radio Directive Equipment (RED)

Declaration of Conformity (DoC)

Voleatech declares that the radio equipment for the VT AIR 600 is in compliance with Radio Equipment Directive 2014/53/EU.

LTE Modem

Warning: A safety distance of at least 20 cm must be kept between the product antenna and the operator or and other persons.

3.5.14 Contact Information and Resources

Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany

www.voleatech.de info@voleatech.de +49 7121 539 550

3.6 VT AIR 1200

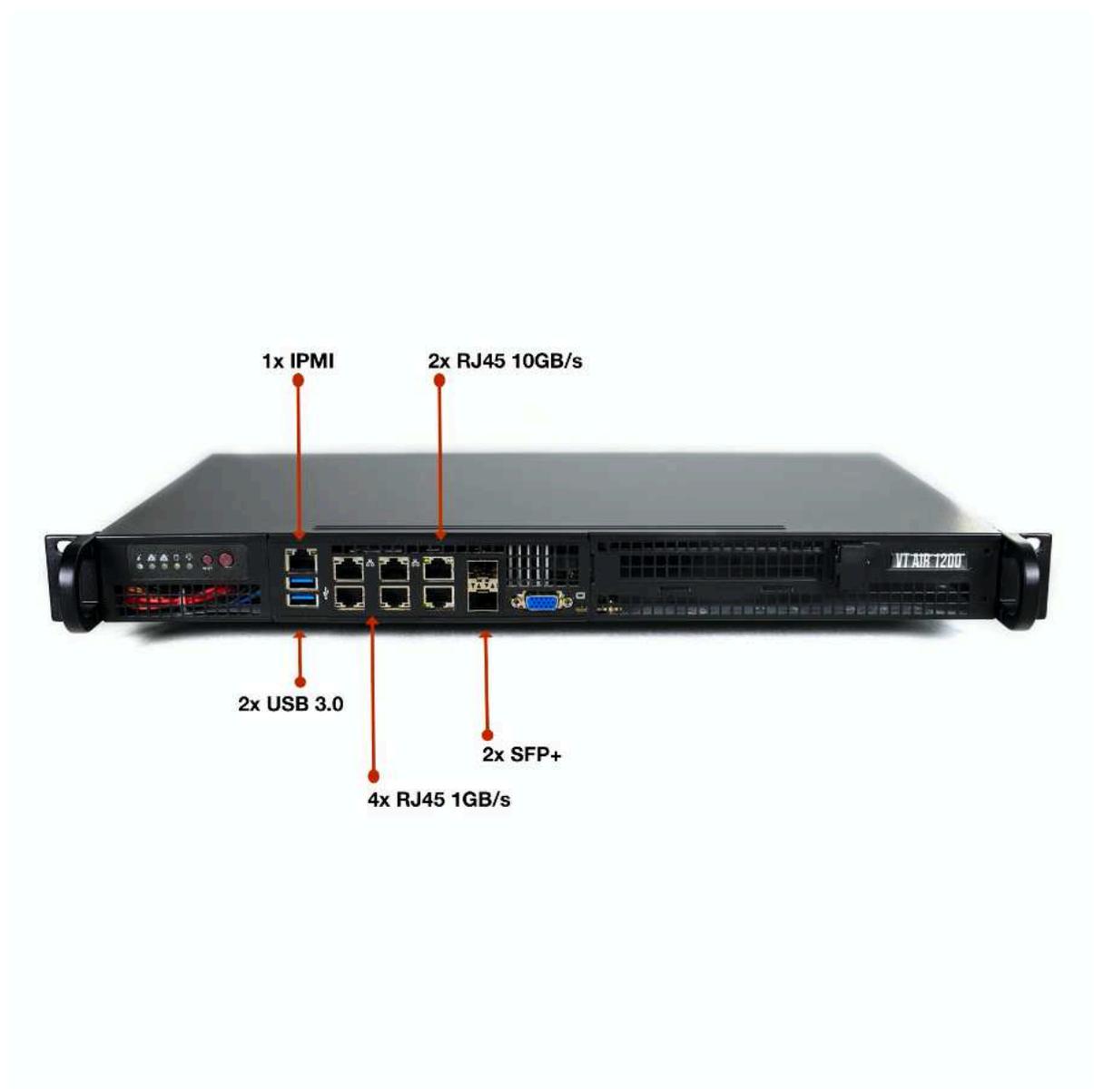


3.6.1 Overview

Summary of Features

CPU	Intel Xeon D 2123IT, 2.2 GHz
CPU Cores	4 Cores
NIC	2x 10GbE Intel SFP+ Ports 2x 10GbE Intel RJ45 Ports 4x 1Gbps Intel RJ45
Remote Management	1x 1Gbps RJ45 IPMI
SSD	256 GB M.2 MLC SSD SATA
RAM	16 GB DDR4 ECC Reg.
Expansion	None
Console Port	eVGA
USB Ports	2x USB 3.0 ports
LED	Power/Status/SATA Activity
Size	Standard 19" 1U rack mount
Cooling	Active control chassis fans
Power	100-240V, Internal Power Supply German Powercord IEC320-C13
Environment	0°C to 45°C Operating Temp 8% to 90% Operating Relative Humidity (non-condensing)
Certificates	Electromagnetic Emissions: FCC Class B, EN 55032 Class B, EN 61000-3-2/3-3, CISPR 32 Electromagnetic Immunity: EN 55024 (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11) Environmental: Directive 2011/65/EU, Deligated Directive (EU) 2015/863, and Directive 2012/19/EU Safety: CE Marking (Europe)
Software	VT AIR Linux

3.6.2 External Connectors



Certified Cables

The following is a list of industry-standard cables, sorted by type, with the necessary compliance requirements that have been proven to work well with the VT AIR product family.

These examples are the cables which Voleatech uses for testing and should provide enough information to source products from your preferred cable vendor.

- Ethernet cable: Monoprice 24AWG Cat6A 500MHz STP (max. 30m)
- USB Cable: SuperSpeed USB 3.0 Type A Male to Male Cable

USB Connector

The front USB connector supports USB 3.0, connector type A. It can deliver up to 500 mA of power.

3.6.3 Packaging

The following items will be in the packaging of your VT AIR 1200. Please make sure to check all items upon arrival of the device:

- VT AIR 1200 Device in the enclosure
- Power cable
- Rack mount

3.6.4 Ports

Front Connectors

Network Ports				
IPMI	eno2 (WAN)	eno4	eno6	eno8
	eno1 (LAN)	eno3	eno5	eno7

Label	Software Name	Features
WAN	eno2	RJ45 1000/100/10 Mbit/s
LAN	eno1	RJ45 1000/100/10 Mbit/s
	eno3	RJ45 1000/100/10 Mbit/s
	eno4	RJ45 1000/100/10 Mbit/s
	eno5	RJ45 10000/1000 Mbit/s
	eno6	RJ45 10000/1000 Mbit/s
	eno7	SFP+ 10000/1000 Mbit/s
	eno8	SFP+ 10000/1000 Mbit/s

The RJ45 ports support Autonegotiation and Full Duplex or Half Duplex on all speeds.

The SFP Port supports the following Modules:

- 10Gb SR/LR
- 1Gb NOT SUPPORTED

SFP modules must be Intel coded. The Speed of the 10Gb modules can be set to 1Gb in VT AIR to connect to a 1Gb SFP.

3.6.5 IPMI

The model comes equipped with an IPMI controller. The IPMI controller has a separate Network Interface but can also get its IP from a shared Network Port.

Warning: If you see a dhcp address being taken on the LAN port by default than is is the IPMI IP and not the Webgui

Note: Login Data are User: **ADMIN** (capital letters) Password: Provided on a sticker on the bottom or side of the device

3.6.6 Power

The VT AIR 1200 has 1 power cable connector.

3.6.7 VGA Console

The VT AIR 1200 has a VGA port where you can connect a VGA monitor to see the console.

First Connection to TBF Appliance

All TBF Appliances have a default LAN IP Address of *192.168.1.1* and the DHCP Server is active on LAN. Please make sure to locate the *LAN* interface of your appliance in the manual.

Connect your computer to the LAN Interface and receive an IP Address from the DHCP Server. It will be in the 192.168.1.X range.

After receiving the IP Address open a supported browser and navigate to **https://192.168.1.1** A certificate warning will appear, since the TBF is using a self signed certificate. Please accept the certificate and continue to the page.

You will now be presented with the TBF login screen and you can use the default User and Password to login.

Note: User: admin Password: vtair

Please change the password after the first login.

3.6.8 VT AIR Reinstallation

Your VT AIR device comes pre-installed with its operating system. Should you ever need to reinstall the VT AIR operating system follow this guide.

Download the Installer File

You can download the installer file from your Portal (see [Downloads](#) for details). Make sure to download the file for your specific model/architecture.

USB Flash Drive Preparation

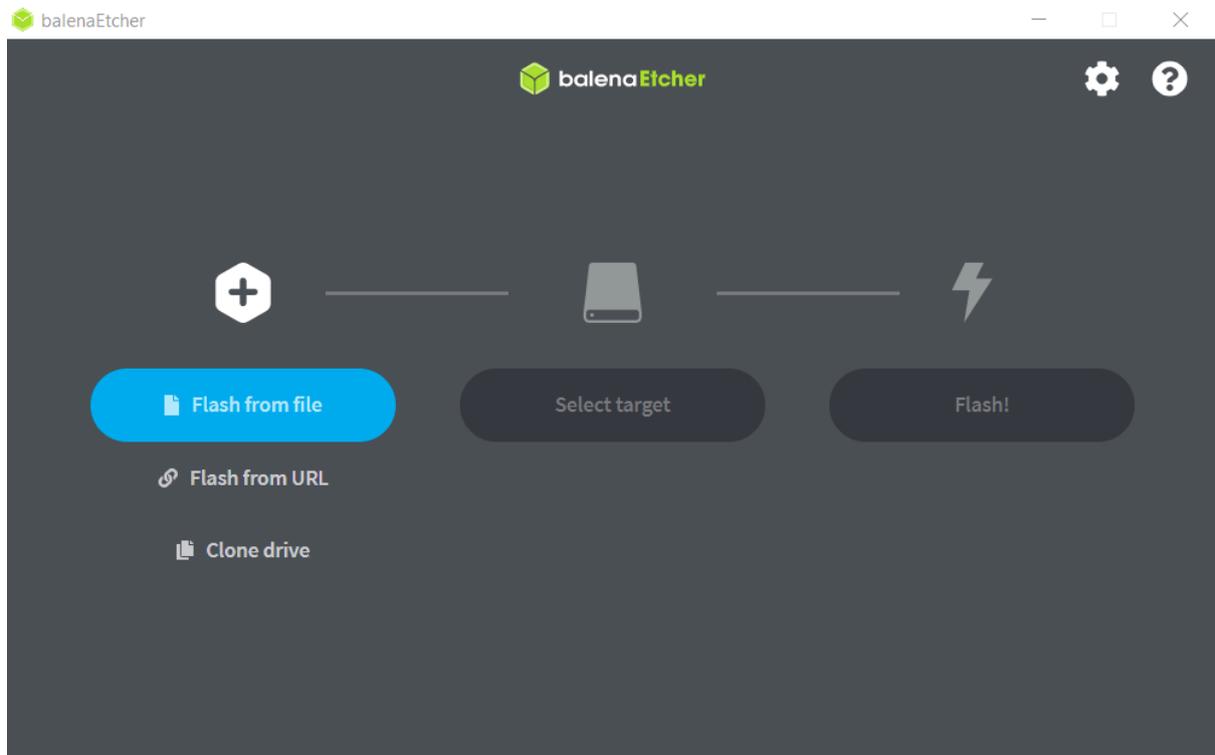
Once you downloaded the file make sure your USB flash drive is at least 2 GB in size. Also backup all your files from the USB flash drive since it will be formatted in the process and all files on it will be deleted.

Download the Software

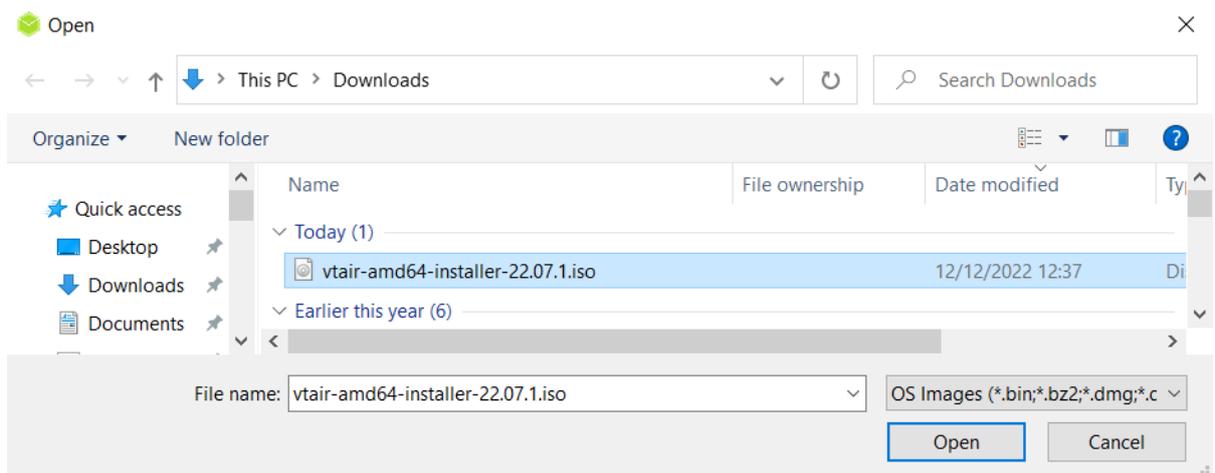
Download and install the software *balenaEtcher* from www.balena.io/etcher. It is available for Windows, macOS and Linux. Select the software for your specific operating system.

Use the Software

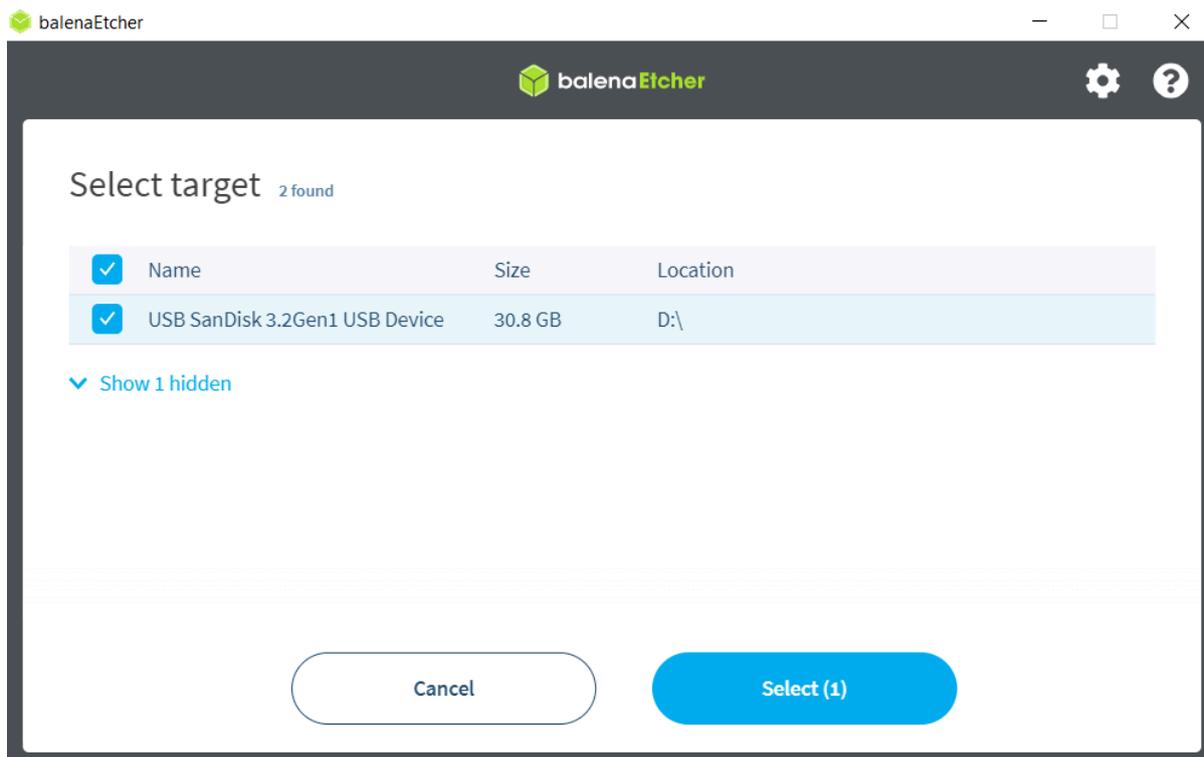
Insert your USB flash drive into the computer. Start the *balenaEtcher* software.



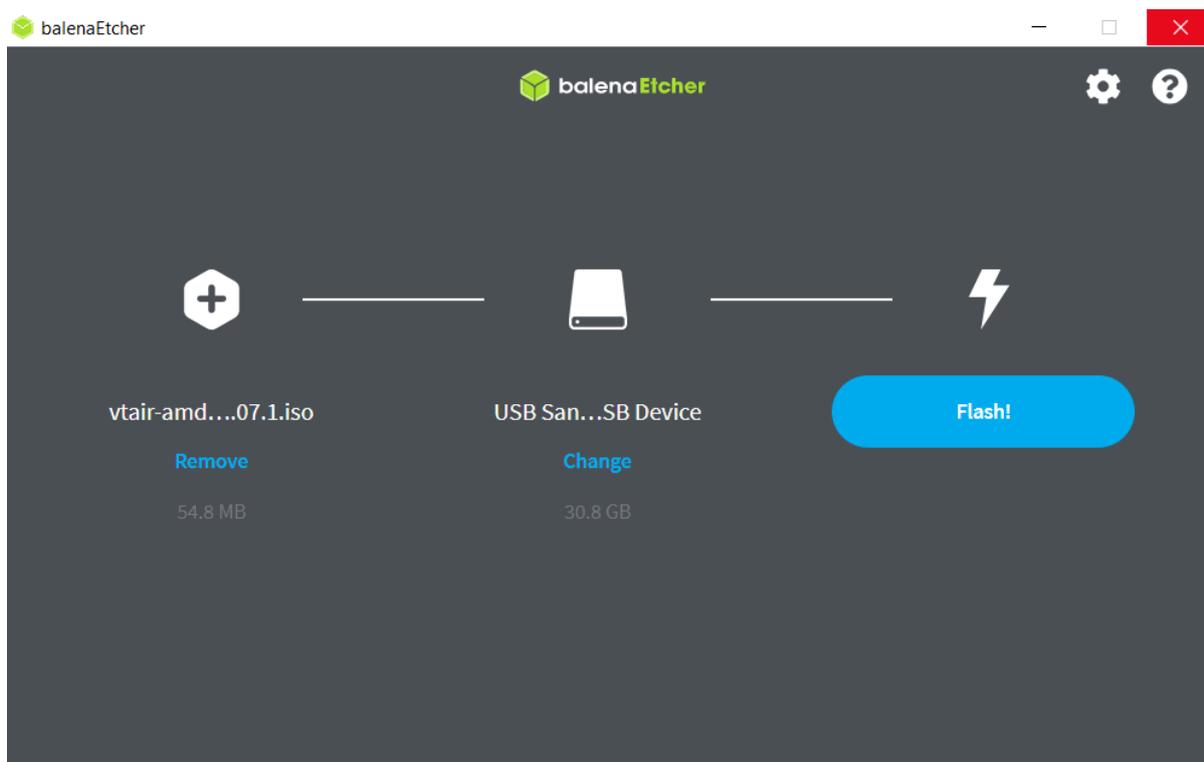
Press *Flash from file*



Select the downloaded installer file with the ending *.iso*



Select your USB flash drive as target



Press *Flash!* to complete and wait until the process is finished. Close the software and remove the USB flash drive from your computer.

Install the Software

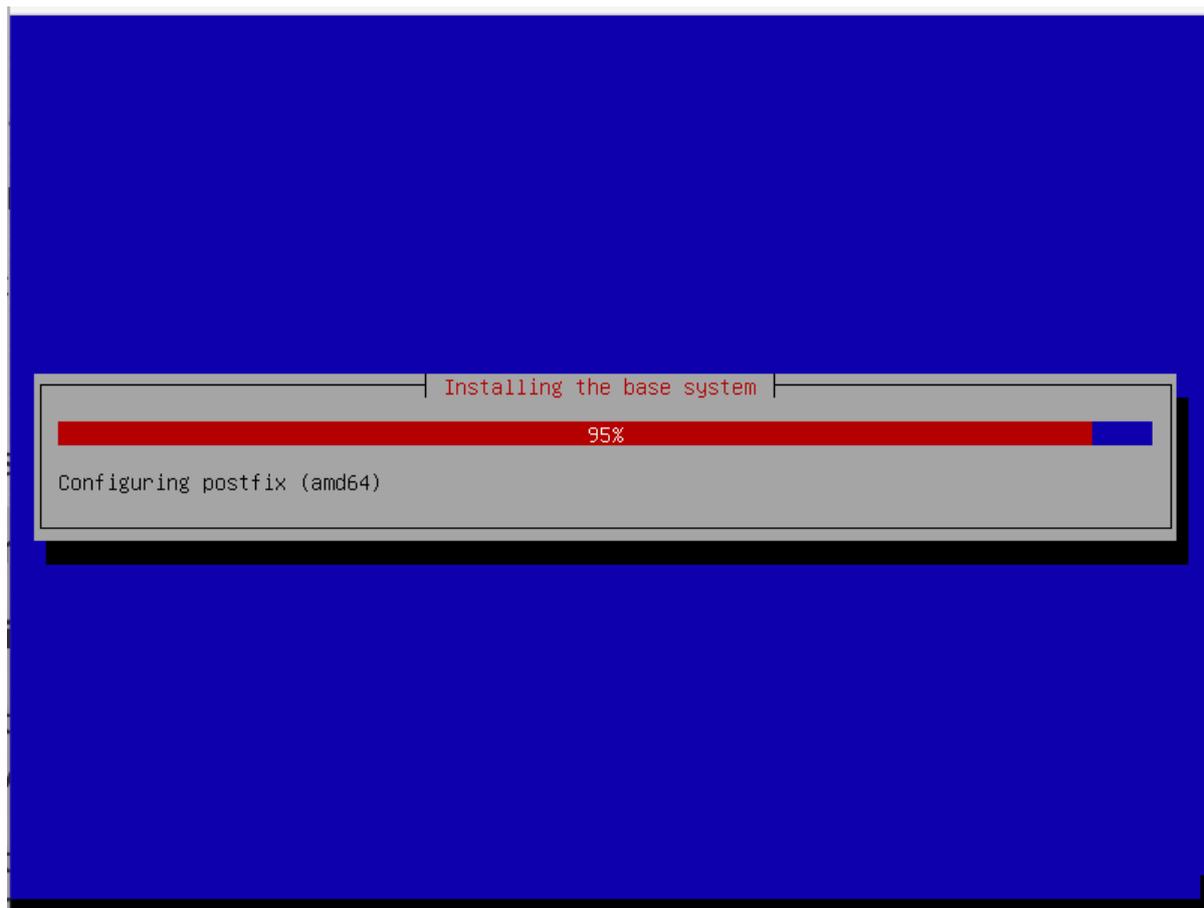
Insert the USB flash drive with the new VT AIR operating system in your VT AIR's USB port.

VGA Monitor Installation

Connect a monitor and keyboard to your VT AIR device. Reboot the device and press *F8* during the boot process to get into the boot menu. Select the USB key and boot from it.

In the installer choose **Install**.





The installer runs without any user inputs.

3.6.9 LEDs

The VT AIR 1200 has multiple LEDs. They are indicating for example power on, connection and port activity. Ethernet port related LEDs are embedded in the RJ45 connectors, while the power indicator LED is located next the serial port.

The RJ45 NIC LEDs are configured the following way:

LED Activity	Explanation
Off	No connection
Green Light Only	100Mbit/s Speed
Green and Yellow Light	1000Mbit/s Speed

3.6.10 Operational Data

Operational Voltage

Item	Voltage	Current	Ambient Temperature
AC Voltage	100 - 240 V	0.5 - 2.5 A	Max. 45°C

Environmental Data

The environmental temperature data are based upon the component with the lowest available temperature. Please make sure to check which addons you ordered and make sure not to exceed the allowed

ambient temperature.

Warning: Failure to comply with the allowed ambient temperature may void the warranty of your device.

Ambient Temperature	Minimum	Maximum
Base Device	0°C	45°C
Humidity (non-condensing)	8 %	90 %

3.6.11 Warranty Terms and Conditions

Voleatech GmbH guarantees its hardware products against defects in workmanship and material for a period of one (1) year from the date of shipment. Under warranty, the customer's sole remedy and Voleatech's sole liability shall be, at Voleatech's sole discretion, to either repair or replace the defective hardware product at no charge. This warranty is void if the hardware product has been altered or damaged by an accident, misuse or abuse or is not operated according to this manual. For additional information on warranty and related topics like RMA, please visit voleatech.de.

Disclaimer of Warranty THIS WARRANTY IS MADE IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESSED, OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR A SPECIFIC PURPOSE, NON-INFRINGEMENT OR THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION, EXCEPT THE WARRANTY EXPRESSLY STATED HEREIN. THE REMEDIES SET FORTH HEREIN SHALL BE THE SOLE AND EXCLUSIVE REMEDIES OF ANY CUSTOMER OR PURCHASER WITH RESPECT TO ANY DEFECTIVE PRODUCT.

Limitation on Liability UNDER NO CIRCUMSTANCES SHALL VOLEATECH GmbH BE LIABLE FOR ANY LOSS, DAMAGE OR EXPENSES INCURRED OR WITH RESPECT TO ANY DEFECTIVE PRODUCT. IN NO EVENT SHALL Voleatech GmbH BE LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES THAT CUSTOMER MAY SUFFER DIRECTLY OR INDIRECTLY FROM THE USAGE OF ANY PRODUCT. BY ORDERING THE VT AIR 1200, THE CUSTOMER APPROVES THAT THE VT AIR 1200, HARDWARE AND SOFTWARE, WAS THOROUGHLY TESTED AND HAS MET THE CUSTOMER'S REQUIREMENTS AND SPECIFICATIONS.

3.6.12 Legal Notice

Voleatech GmbH (hereinafter "Voleatech") products and services are sold subject to Voleatech terms and conditions of sale, delivery and payment supplied at the time of purchase order acknowledgement. Voleatech warrants the performance of its products according to actual specifications at the date of shipment. Voleatech reserves the right to make changes to its products and specifications or to discontinue any product, product line or service without prior notice. Customers should make sure to obtain in each case the latest version of relevant product information from Voleatech and to always verify for themselves that their requirements are met and reference is up to date. Product testing and all additional quality control techniques are utilized to the extent that Voleatech deems necessary to support their warranty and warranty terms. Therefore detailed testing of all parameters in any product is not necessarily performed in full unless required by law or regulation. In order to minimize risks that may be associated with customer products, applications or services, the customer must use adequate design and operating safeguards to minimize any possible hazards. Voleatech is not liable for any applications assistance or customer product design and thus it is the customer's sole responsibility to make the selection and usage of Voleatech products. Voleatech is not liable for any such selection or usage thereafter and neither is liable for the usage of any circuitry or components other than completely and entirely embodied in a Voleatech product. Furthermore Voleatech is not liable for its products commercial fit for any market segment envisioned by the customer. Voleatech products are not intended for use in life support systems, appliances, nuclear systems or systems where malfunction can reasonably be expected to result in personal injury, death or severe property or environmental damage. Any use of Voleatech's

products by the customer for such purposes is completely at the customer's own risk. Voleatech does not grant any license -expressed or implied- on any patent right, copyright, mask work right, type or model protection or any other intellectual property right (IPR) of Voleatech covering or relating to any product combination, hardware, machine, software or process in which its products or services might be or are used. Any provision or publication of any third party's products or services does not constitute Voleatech's approval, license, warranty or endorsement thereof. Any third party trademarks contained in this document belong to the respective third party owner. Reproduction of content and information from Voleatech documents and manuals is permissible only if reproduction is without alteration and is accompanied by all associated copyright, proprietary and other notices (including this notice) and related conditions. Voleatech is not liable for any un-authorized alteration of such content and information or for any reliance related to alterations thereon. Any representations made, warranties given, and/or liabilities accepted by any person which differ from those contained in this manual or in Voleatech's standard terms and conditions of sale, delivery and payment are made, given and/or accepted at customer's own risk. Voleatech is not liable for any such representations, warranties or liabilities or for any reliance thereon by any person.

3.6.13 Regulatory

This chapter provides regulatory and compliance information about Voleatech's VT AIR 1200 -related information. Product name: VT AIR 1200

Safety Notice

Before you begin using this product, please read the following safety information. Attention to these warnings will help prevent personal injuries and damage to the products. It is your responsibility to use the product in an appropriate manner. This product is designed for use solely indoor environments or, if expressly permitted, also in the field and must not be used in any way that may cause personal injury or property damage.

You are responsible if the product is used for any intention other than its designated purpose or in disregard of Voleatech's instructions. Voleatech shall assume no responsibility for such use of the product. The product is used for its designated purpose if it is used in accordance with its product documentation and within its performance limits.

Safety Information and Notices

Never turn on or connect to power any equipment when there is evidence of mechanical damage, fire, exposure to water, or structural damage.

When not in use, avoid placing or storing the product in the following places or under the following conditions

- Ambient temperature above 45°C
- Exposed to direct sunlight
- Humid or exposed to dust

<p>Warning: This product does not contain any user replicable or serviceable parts. Do not take apart or attempt to service the product yourself.</p>
--

Never remove the cover or any part of the housing of the product. The internal battery is not user replicable.

In the event of an equipment malfunction, all repairs must be performed either by Voleatech GmbH or by an authorized agent. It is the customer responsibility to report the need for service to Voleatech GmbH or to one of the authorized agents. For service information, contact Voleatech GmbH customer support.

Be careful not subject the product to strong impact.

If the product was subjected to a strong impact and/or falling over check carefully for any damage to the product. If such damage is observed the use of the product must be stopped immediately.

Operation

The product may be operated only under the operating conditions as specified by Voleatech GmbH. When the product is used for an extended period of time, and/or at high ambient temperature and/or exposed to direct sunlight it is normal for the product body to feel warm.

Avoid overheating the product. The product's ventilation should not be obstructed or blocked. If proper ventilation is not provided it can result in battery overheating or explosion of the battery resulting fire, burns or other injuries.

Stop using the product immediately if it emits smoke or a strange smell, or otherwise behaves abnormally.

Following are the required operating position and conditions:

- Do not place the product on unstable surfaces
- Do not place the product on elevated surface and secure it from falling from high places on passerby
- Do not place the product on heat-generating surface or near heat emitting devices or direct flame. Verify that there is sufficient clearance between the product and any other device exhaust warm air.
- The product operating ambient range can be found at Environmental Data. Voleatech GmbH recommends that an ambient temperature of 0 to 40 °C (32 to 104 °F) and relative humidity of 30-50% is maintained during normal operation as this will result in better performance and longer life of the equipment. Temperature must not exceed the maximum temperature specified in Environmental Data.
- Do not expose the product to moisture or dust.
- The product is not liquid proof; therefore, the equipment must be protected against penetration by liquids. If the necessary precautions are not taken, the user may suffer electric shock or the product itself may be damaged, which can also lead to personal injury.
- Never use the product under conditions in which condensation has formed or can form in or on the product, e.g. if the product has been moved from a cold to a warm environment. Penetration by water increases the risk of electric shock.

Electronic Emission Notices (EMC)

Federal Communications Commission Declaration of Conformity The following information refers to VT AIR 1200. This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

Responsible Party: Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany

WEEE and recycling statements

The WEEE marking on Voleatech GmbH products applies to countries with WEEE and e-waste regulations (for example, the European WEEE Directive). Appliances are labeled in accordance with local regulations concerning waste electrical and electronic equipment (WEEE).

These regulations determine the framework for the return and recycling of used appliances as applicable within each geography. This label is applied to various products to indicate that the product is not to be thrown away, but rather put in the established collection systems for reclaiming these end of life products.

Users of electrical and electronic equipment (EEE) with the WEEE marking must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to them for the return, recycle and recovery of WEEE and to minimize any potential effects of EEE on the environment and human health due to the presence of hazardous substances. Voleatech GmbH electrical and electronic

equipment (EEE) may contain parts and components, which at end-of-life might qualify as hazardous waste.

EEE and waste electrical and electronic equipment (WEEE) can be delivered free of charge to the place of sale or any distributor that sells electrical and electronic equipment of the same nature and function as the used EEE or WEEE.



Restriction of Hazardous Substances (RoHS) European Union RoHS

This product, with included parts (cables, cords, and so on) meets the requirements of Directive 2011/65/EU and directive 2015/863/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment ("RoHS recast" or "RoHS 2").

3.6.14 Contact Information and Resources

Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany

www.voleatech.de info@voleatech.de +49 7121 539 550

3.7 VT AIR 1500

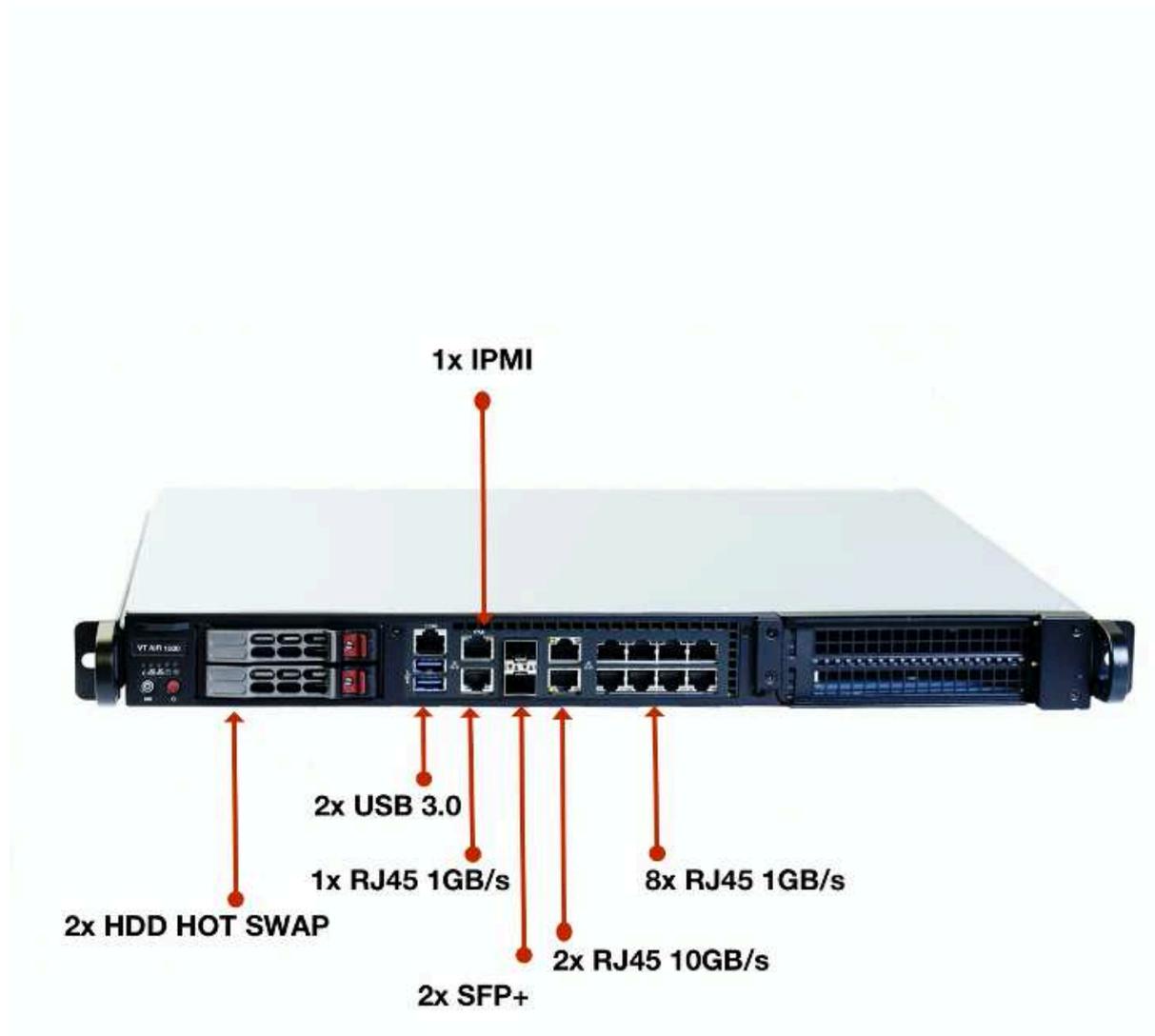


3.7.1 Overview

Summary of Features

CPU	Intel Xeon D 2146NT, 2.3 GHz, Intel Quick Assist
CPU Cores	8 Cores
NIC	2x 10GbE Intel SFP+ Ports 2x 10GbE Intel RJ45 Ports 9x 1Gbps Intel RJ45
Re- mote Man- age- ment	1x 1Gbps RJ45 IPMI
SSD	2x 256 GB Datacenter SSD SATA Hot Swap (RAID1)
RAM	32 GB DDR4 ECC Reg
Ex- pan- sion	2x PCI-E 3.0 16x slots
Conso- le Port	1x VGA
USB Ports	2x USB 3.0 ports
LED	Power/Status/SATA Activity
Size	Standard 19" 1U rack mount
Cool- ing	Active control chassis fans
Power	100-240V, Internal Power Supply German Powercord IEC320-C13
En- vi- ro- ment	0°C to 45°C Operating Temp 8% to 90% Operating Relative Humidity (non-condensing)
Cer- tifi- cates	Electromagnetic Emissions: FCC Class B, EN 55032 Class B, EN 61000-3-2/3-3, CISPR 32 Class B Electromagnetic Immunity: EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11) Other: VCCI-CISPR 32 and AS/NZS CISPR 32 Environmental: Directive 2011/65/EU, Deligated Directive (EU) 2015/863, and Directive 2012/19/EU Safety: CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)
Soft- ware	VT AIR Linux

3.7.2 External Connectors



Certified Cables

The following is a list of industry-standard cables, sorted by type, with the necessary compliance requirements that have been proven to work well with the VT AIR product family.

These examples are the cables which Voleatech uses for testing and should provide enough information to source products from your preferred cable vendor.

- Ethernet cable: Monoprice 24AWG Cat6A 500MHz STP (max. 30m)
- USB Cable: SuperSpeed USB 3.0 Type A Male to Male Cable

USB Connector

The front USB connector supports USB 3.0, connector type A. It can deliver up to 500 mA of power.

3.7.3 Packaging

The following items will be in the packaging of your VT AIR 1500. Please make sure to check all items upon arrival of the device:

- VT AIR 1500 Device in the enclosure
- Power cable
- Rack mount

3.7.4 Ports

Front Connectors

Network Ports						
IPMI	eno13	eno11	eno3	eno5	eno7	eno9
eno1 (LAN)	eno12	eno10	eno2 (WAN)	eno4	eno6	eno8

Label	Software Name	Features
WAN	eno2	RJ45 1000/100/10 Mbit/s
LAN	eno1	RJ45 1000/100/10 Mbit/s
	eno3	RJ45 1000/100/10 Mbit/s
	eno4	RJ45 1000/100/10 Mbit/s
	eno5	RJ45 1000/100/10 Mbit/s
	eno6	RJ45 1000/100/10 Mbit/s
	eno7	RJ45 1000/100/10 Mbit/s
	eno8	RJ45 1000/100/10 Mbit/s
	eno9	RJ45 1000/100/10 Mbit/s
	eno10	RJ45 10000/1000 Mbit/s
	eno11	RJ45 10000/1000 Mbit/s
	eno12	SFP+ 10000/1000 Mbit/s
	eno13	SFP+ 10000/1000 Mbit/s

The RJ45 ports support Autonegotiation and Full Duplex or Half Duplex on all speeds.

The SFP Port supports the following Modules:

- 10Gb SR/LR
- 1Gb NOT SUPPORTED

SFP modules must be Intel coded. The Speed of the 10Gb modules can be set to 1Gb in VT AIR to connect to a 1Gb SFP.

Extension Card

Network Ports Extension Cards				
Slot 1	enp23s0f0	enp23s0f1	enp23s0f2	enp23s0f3
Slot 2	enp100s0f0	enp100s0f1	enp100s0f2	enp100s0f3

3.7.5 IPMI

The model comes equipped with an IPMI controller. The IPMI controller has a separate Network Interface but can also get its IP from a shared Network Port.

Warning: If you see a dhcp address being taken on the LAN port by default than is is the IPMI IP and not the Webgui

Note: Login Data are User: **ADMIN** (capital letters) Password: Provided on a sticker on the bottom or side of the device

3.7.6 Power

The VT AIR 1500 has 1 power cable connector.

3.7.7 VGA Console

The VT AIR 1500 has a VGA port where you can connect a VGA monitor to see the console.

First Connection to TBF Appliance

All TBF Appliances have a default LAN IP Address of *192.168.1.1* and the DHCP Server is active on LAN. Please make sure to locate the *LAN* interface of your appliance in the manual.

Connect your computer to the LAN Interface and receive an IP Address from the DHCP Server. It will be in the 192.168.1.X range.

After receiving the IP Address open a supported browser and navigate to **https://192.168.1.1** A certificate warning will appear, since the TBF is using a self signed certificate. Please accept the certificate and continue to the page.

You will now be presented with the TBF login screen and you can use the default User and Password to login.

Note: User: admin Password: vtair

Please change the password after the first login.

3.7.8 VT AIR Reinstallation

Your VT AIR device comes pre-installed with its operating system. Should you ever need to reinstall the VT AIR operating system follow this guide.

Download the Installer File

You can download the installer file from your Portal (see [Downloads](#) for details). Make sure to download the file for your specific model/architecture.

USB Flash Drive Preparation

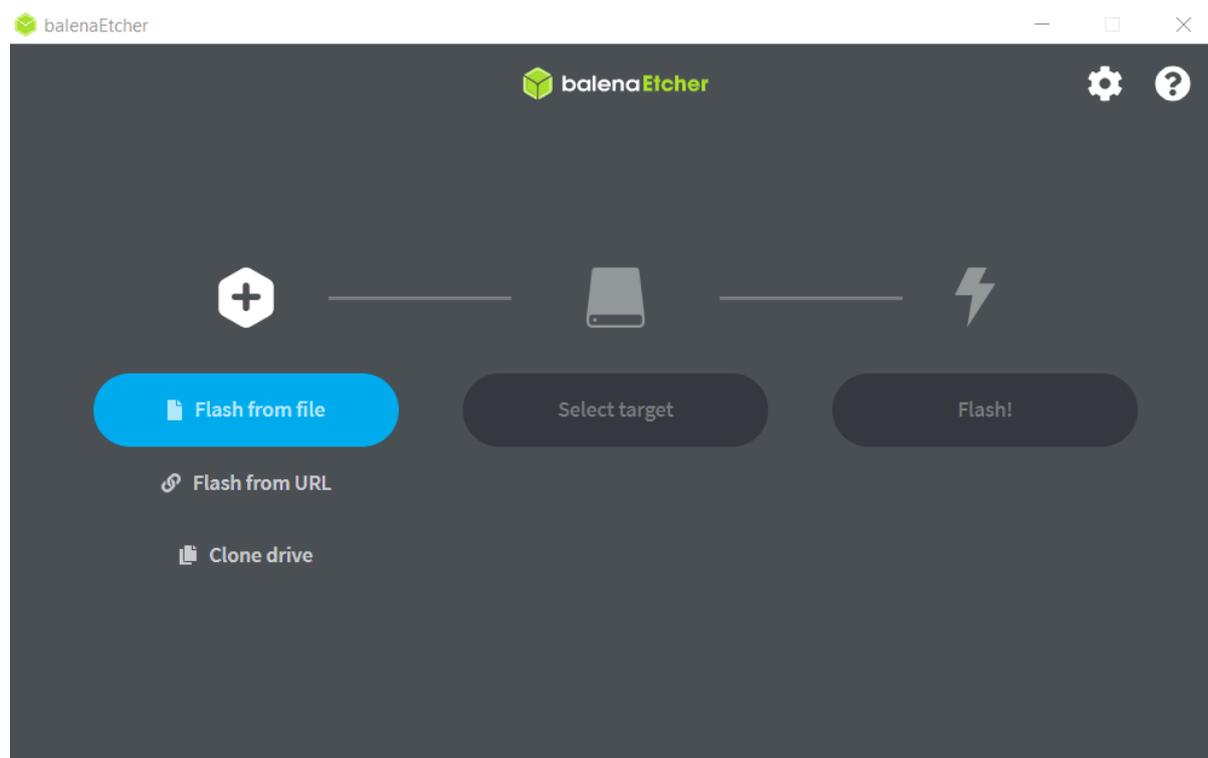
Once you downloaded the file make sure your USB flash drive is at least 2 GB in size. Also backup all your files from the USB flash drive since it will be formatted in the process and all files on it will be deleted.

Download the Software

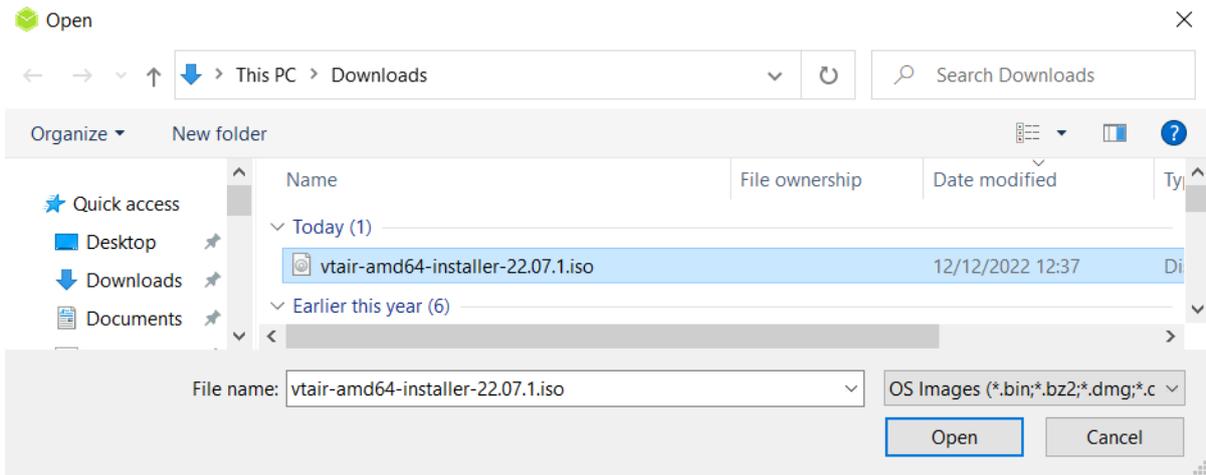
Download and install the software *balenaEtcher* from www.balena.io/etcher. It is available for Windows, macOS and Linux. Select the software for your specific operating system.

Use the Software

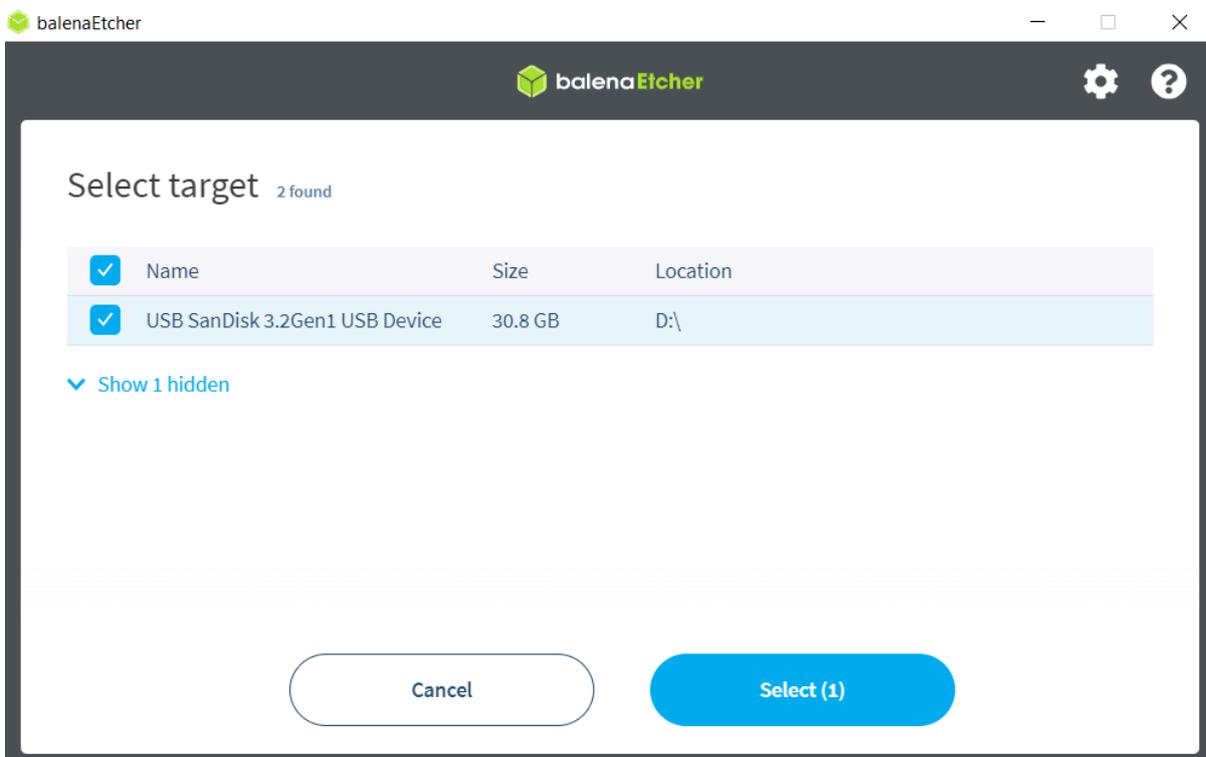
Insert your USB flash drive into the computer. Start the *balenaEtcher* software.



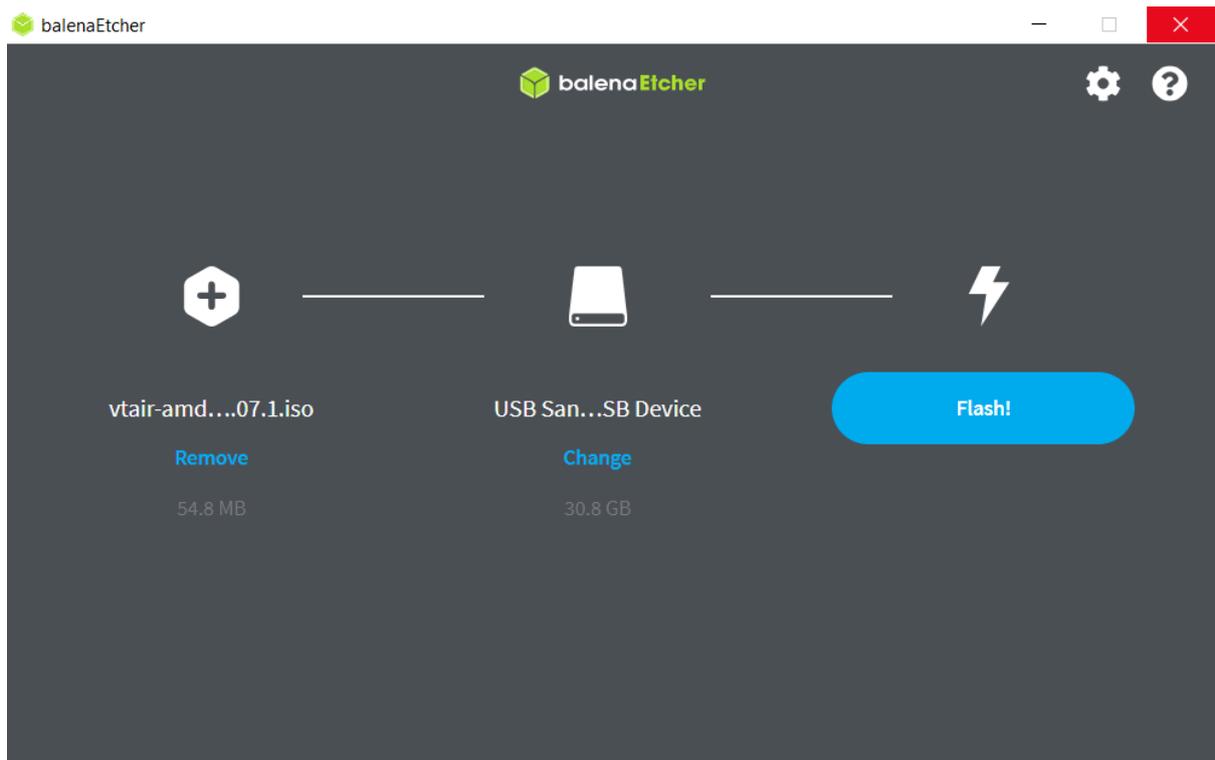
Press *Flash from file*



Select the downloaded installer file with the ending .iso



Select your USB flash drive as target



Press *Flash!* to complete and wait until the process is finished. Close the software and remove the USB flash drive from your computer.

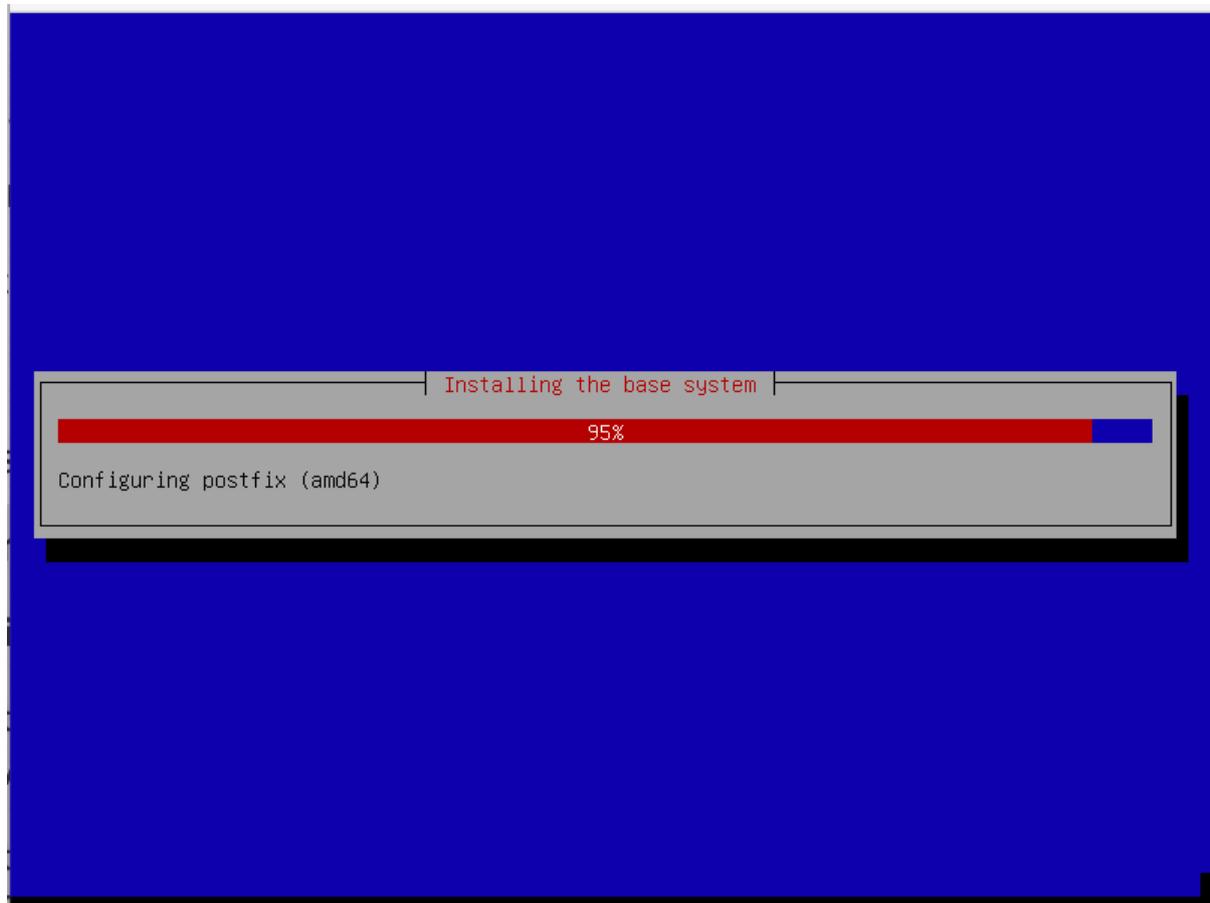
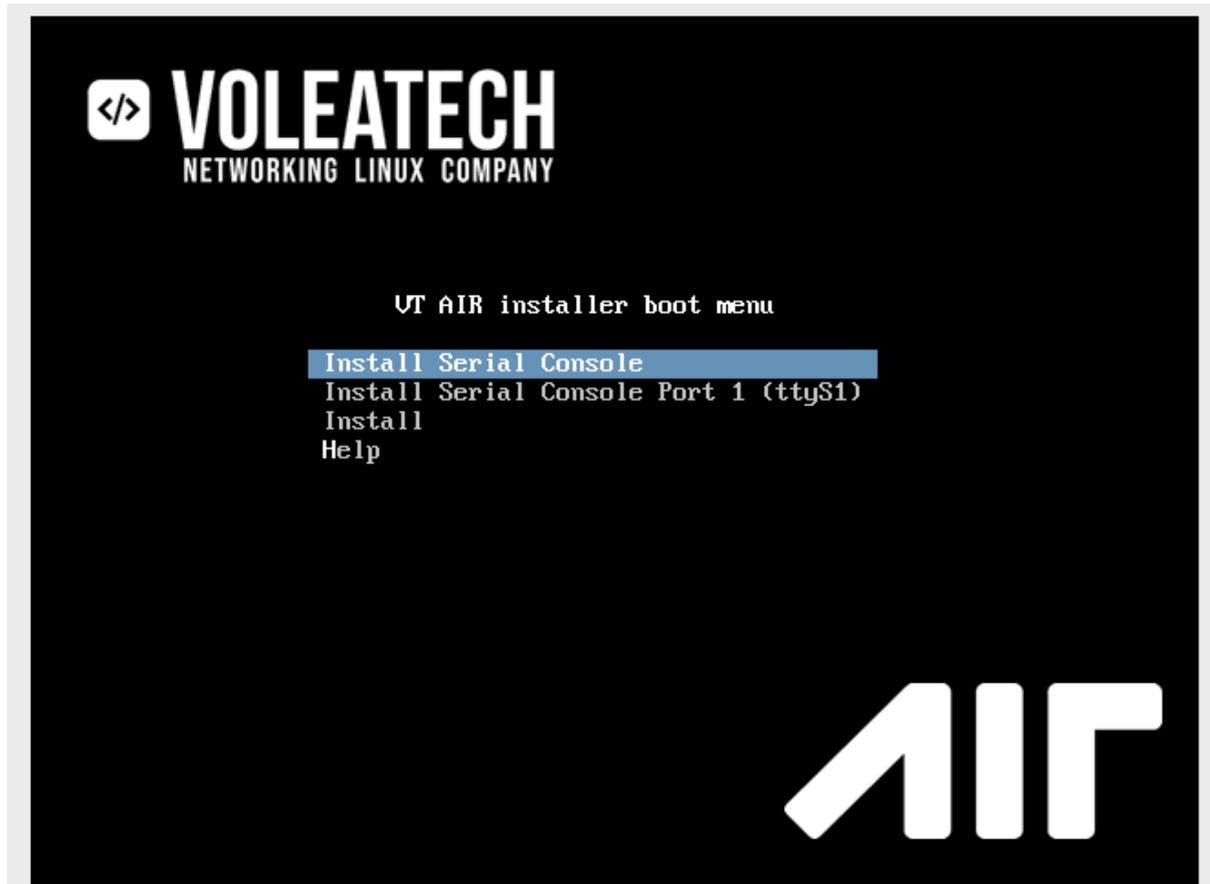
Install the Software

Insert the USB flash drive with the new VT AIR operating system in your VT AIR's USB port.

VGA Monitor Installation

Connect a monitor and keyboard to your VT AIR device. Reboot the device and press *F8* during the boot process to get into the boot menu. Select the USB key and boot from it.

In the installer choose **Install**.



The installer runs without any user inputs.

3.7.9 LEDs

The VT AIR 1500 has multiple LEDs. They are indicating for example power on, connection and port activity. Ethernet port related LEDs are embedded in the RJ45 connectors, while the power indicator LED is located next the serial port.

The RJ45 NIC LEDs are configured the following way:

LED Activity	Explanation
Off	No connection
Green Light Only	100Mbit/s Speed
Green and Yellow Light	1000Mbit/s Speed

3.7.10 Operational Data

Operational Voltage

Item	Voltage	Current	Ambient Temperature
AC Voltage	100 - 240 V	0.5 - 2.5 A	Max. 45°C

Environmental Data

The environmental temperature data are based upon the component with the lowest available temperature. Please make sure to check which addons you ordered and make sure not to exceed the allowed ambient temperature.

Warning: Failure to comply with the allowed ambient temperature may void the warranty of your device.

Ambient Temperature	Minimum	Maximum
Base Device	0°C	45°C
Humidity (non-condensing)	8 %	90 %

3.7.11 Warranty Terms and Conditions

Voleatech GmbH guarantees its hardware products against defects in workmanship and material for a period of one (1) year from the date of shipment. Under warranty, the customer's sole remedy and Voleatech's sole liability shall be, at Voleatech's sole discretion, to either repair or replace the defective hardware product at no charge. This warranty is void if the hardware product has been altered or damaged by an accident, misuse or abuse or is not operated according to this manual. For additional information on warranty and related topics like RMA, please visit voleatech.de.

Disclaimer of Warranty THIS WARRANTY IS MADE IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESSED, OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR A SPECIFIC PURPOSE, NON-INFRINGEMENT OR THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION, EXCEPT THE WARRANTY EXPRESSLY STATED HEREIN. THE REMEDIES SET FORTH HEREIN SHALL BE THE SOLE AND EXCLUSIVE REMEDIES OF ANY CUSTOMER OR PURCHASER WITH RESPECT TO ANY DEFECTIVE PRODUCT.

Limitation on Liability UNDER NO CIRCUMSTANCES SHALL VOLEATECH GmbH BE LIABLE FOR ANY LOSS, DAMAGE OR EXPENSES INCURRED OR WITH RESPECT TO ANY DEFECTIVE PRODUCT. IN NO EVENT SHALL Voleatech GmbH BE LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES THAT CUSTOMER MAY SUFFER DIRECTLY OR INDIRECTLY FROM THE USAGE OF ANY PRODUCT. BY ORDERING THE VT AIR 1500, THE CUSTOMER APPROVES THAT THE VT AIR 1500, HARDWARE AND SOFTWARE, WAS THOROUGHLY TESTED AND HAS MET THE CUSTOMER'S REQUIREMENTS AND SPECIFICATIONS.

3.7.12 Legal Notice

Voleatech GmbH (hereinafter "Voleatech") products and services are sold subject to Voleatech terms and conditions of sale, delivery and payment supplied at the time of purchase order acknowledgement. Voleatech warrants the performance of its products according to actual specifications at the date of shipment. Voleatech reserves the right to make changes to its products and specifications or to discontinue any product, product line or service without prior notice. Customers should make sure to obtain in each case the latest version of relevant product information from Voleatech and to always verify for themselves that their requirements are met and reference is up to date. Product testing and all additional quality control techniques are utilized to the extent that Voleatech deems necessary to support their warranty and warranty terms. Therefore detailed testing of all parameters in any product is not necessarily performed in full unless required by law or regulation. In order to minimize risks that may be associated with customer products, applications or services, the customer must use adequate design and operating safeguards to minimize any possible hazards. Voleatech is not liable for any applications assistance or customer product design and thus it is the customer's sole responsibility to make the selection and usage of Voleatech products. Voleatech is not liable for any such selection or usage thereafter and neither is liable for the usage of any circuitry or components other than completely and entirely embodied in a Voleatech product. Furthermore Voleatech is not liable for its products commercial fit for any market segment envisioned by the customer. Voleatech products are not intended for use in life support systems, appliances, nuclear systems or systems where malfunction can reasonably be expected to result in personal injury, death or severe property or environmental damage. Any use of Voleatech's products by the customer for such purposes is completely at the customer's own risk. Voleatech does not grant any license -expressed or implied- on any patent right, copyright, mask work right, type or model protection or any other intellectual property right (IPR) of Voleatech covering or relating to any product combination, hardware, machine, software or process in which its products or services might be or are used. Any provision or publication of any third party's products or services does not constitute Voleatech's approval, license, warranty or endorsement thereof. Any third party trademarks contained in this document belong to the respective third party owner. Reproduction of content and information from Voleatech documents and manuals is permissible only if reproduction is without alteration and is accompanied by all associated copyright, proprietary and other notices (including this notice) and related conditions. Voleatech is not liable for any un-authorized alteration of such content and information or for any reliance related to alterations thereon. Any representations made, warranties given, and/or liabilities accepted by any person which differ from those contained in this manual or in Voleatech's standard terms and conditions of sale, delivery and payment are made, given and/or accepted at customer's own risk. Voleatech is not liable for any such representations, warranties or liabilities or for any reliance thereon by any person.

3.7.13 Regulatory

This chapter provides regulatory and compliance information about Voleatech's VT AIR 1500 -related information. Product name: VT AIR 1500

Safety Notice

Before you begin using this product, please read the following safety information. Attention to these warnings will help prevent personal injuries and damage to the products. It is your responsibility to use the product in an appropriate manner. This product is designed for use solely indoor environments or, if expressly permitted, also in the field and must not be used in any way that may cause personal injury or property damage.

You are responsible if the product is used for any intention other than its designated purpose or in disregard of Voleatech's instructions. Voleatech shall assume no responsibility for such use of the product. The product is used for its designated purpose if it is used in accordance with its product documentation and within its performance limits.

Safety Information and Notices

Never turn on or connect to power any equipment when there is evidence of mechanical damage, fire, exposure to water, or structural damage.

When not in use, avoid placing or storing the product in the following places or under the following conditions

- Ambient temperature above 45°C
- Exposed to direct sunlight
- Humid or exposed to dust

Warning: This product does not contain any user replicable or serviceable parts. Do not take apart or attempt to service the product yourself.

Never remove the cover or any part of the housing of the product. The internal battery is not user replicable.

In the event of an equipment malfunction, all repairs must be performed either by Voleatech GmbH or by an authorized agent. It is the customer responsibility to report the need for service to Voleatech GmbH or to one of the authorized agents. For service information, contact Voleatech GmbH customer support.

Be careful not subject the product to strong impact.

If the product was subjected to a strong impact and/or falling over check carefully for any damage to the product. If such damage is observed the use of the product must be stopped immediately.

Operation

The product may be operated only under the operating conditions as specified by Voleatech GmbH. When the product is used for an extended period of time, and/or at high ambient temperature and/or exposed to direct sunlight it is normal for the product body to feel warm.

Avoid overheating the product. The product's ventilation should not be obstructed or blocked. If proper ventilation is not provided it can result in battery overheating or explosion of the battery resulting fire, burns or other injuries.

Stop using the product immediately if it emits smoke or a strange smell, or otherwise behaves abnormally.

Following are the required operating position and conditions:

- Do not place the product on unstable surfaces
- Do not place the product on elevated surface and secure it from falling from high places on passerby
- Do not place the product on heat-generating surface or near heat emitting devices or direct flame. Verify that there is sufficient clearance between the product and any other device exhaust warm air.
- The product operating ambient range can be found at Environmental Data. Voleatech GmbH recommends that an ambient temperature of 0 to 40 °C (32 to 104 °F) and relative humidity of 30-50% is maintained during normal operation as this will result in better performance and longer life of the equipment. Temperature must not exceed the maximum temperature specified in Environmental Data.
- Do not expose the product to moisture or dust.

- The product is not liquid proof; therefore, the equipment must be protected against penetration by liquids. If the necessary precautions are not taken, the user may suffer electric shock or the product itself may be damaged, which can also lead to personal injury.
- Never use the product under conditions in which condensation has formed or can form in or on the product, e.g. if the product has been moved from a cold to a warm environment. Penetration by water increases the risk of electric shock.

Electronic Emission Notices (EMC)

Federal Communications Commission Declaration of Conformity The following information refers to VT AIR 1500. This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

Responsible Party: Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany

WEEE and recycling statements

The WEEE marking on Voleatech GmbH products applies to countries with WEEE and e-waste regulations (for example, the European WEEE Directive). Appliances are labeled in accordance with local regulations concerning waste electrical and electronic equipment (WEEE).

These regulations determine the framework for the return and recycling of used appliances as applicable within each geography. This label is applied to various products to indicate that the product is not to be thrown away, but rather put in the established collection systems for reclaiming these end of life products.

Users of electrical and electronic equipment (EEE) with the WEEE marking must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to them for the return, recycle and recovery of WEEE and to minimize any potential effects of EEE on the environment and human health due to the presence of hazardous substances. Voleatech GmbH electrical and electronic equipment (EEE) may contain parts and components, which at end-of-life might qualify as hazardous waste.

EEE and waste electrical and electronic equipment (WEEE) can be delivered free of charge to the place of sale or any distributor that sells electrical and electronic equipment of the same nature and function as the used EEE or WEEE.



Restriction of Hazardous Substances (RoHS) European Union RoHS

This product, with included parts (cables, cords, and so on) meets the requirements of Directive 2011/65/EU and directive 2015/863/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment ("RoHS recast" or "RoHS 2").

3.7.14 Contact Information and Resources

Voleatech GmbH Gratwohlstr. 5 72762 Reutlingen Germany
www.voleatech.de info@voleatech.de +49 7121 539 550

3.8 VT AIR Amazon AWS

VT AIR AWS brings you all VT AIR feature to Amazon's Cloud.

VT AIR AWS AMI can be run in any region where EC2 offers service on various sizes of instance. VT AIR for AWS is available in the [AWS Marketplace](#).

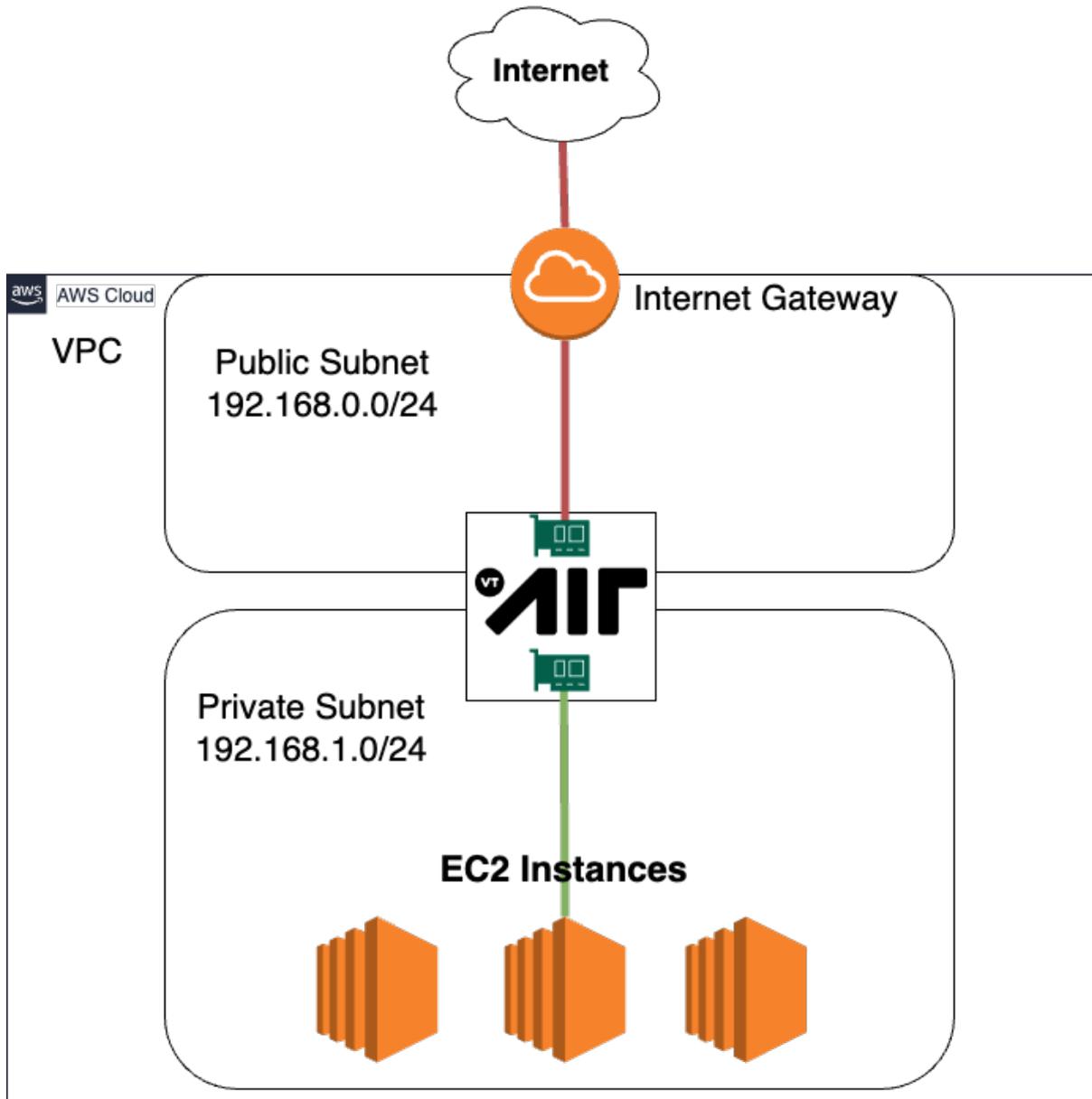
Two different versions are currently available:

- Intel Based VT AIR Version
- Graviton Based VT AIR Version

The graviton version will only run on the AWS Graviton EC2 instances.

All features are available in the AWS Version and you can use VT AIR as a firewall to protect your EC2 instances or as a VPN server to connect via IPSec, OpenVPN or WireGuard.

VT AIR AWS Architecture



In order to configure your AWS environment to utilize VT AIR as a firewall in front of other VMs, a couple of configuration steps have to be done.

1. VPC configuration
 1. New VPC
 2. Public Subnet
 3. Private Subnet
 4. Public Routing Table
 - Internet Gateway for default route
 5. Private Routing Table
 - Default route pointing to VT AIR LAN interface
 6. Public Security Group

7. Private Security Group
2. EC2 VT AIR Appliance
 1. Public Network Interface (WAN)
 - In the Public Subnet
 - Public Security Group
 2. Private Network Interface (LAN)
 - In the Private Subnet
 - Private Security Group
 3. Disable Source and Destination Check
 4. Allocate Elastic IP
 - Connect to the Public Network Interface (WAN)
3. VT AIR configuration
 1. Enable and set LAN Interface
 2. Create DNAT Rules and VPN Configuration
4. EC2 VMs
 1. Add to the Private Network Subnet
 2. Set Private Security Group

3.8.1 Default Login

Default login data for the WebGUI are user **admin** and the password is the **instance id** of the VM. For example **i-0198da08d22664a39**. You can find the instance id in the ec2 console.

For SSH or the console the default user is **admin** and your ssh key from the instance launch is automatically added to the user. You can get root access by using *sudo*.

3.8.2 VPC Configuration

Login to your AWS Account and change to the VPC configuration page.

The screenshot shows the AWS VPC dashboard. At the top, there are navigation links for RDS, EC2, AWS Cost Explorer, Billing, IAM, and VPC. The main content area is titled 'Resources by Region' and shows a list of VPC resources in the US East region. The resources are:

Resource Type	Count	Region
VPCs	2	US East 2
NAT Gateways	0	US East 0
Subnets	8	US East 8
VPC Peering Connections	0	US East 0
Route Tables	4	US East 4
Network ACLs	2	US East 2

We have created videos to show the entire configurations.

New VPC

We will create a new VPC for the VT AIR setup. If you already have a VPC or two subnets configured, you can skip these steps.

Go to *Your VPCs* and click on *Create VPC*.

Choose *VPC only* give the VPC a name, in our case we choose *VTAIR-VPC* and select a network. The network has to be large enough to hold both the *Public* and *Private* Subnet. We are going to use *192.168.0.0/16*.

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

VPC only VPC and more

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.

vtair-vpc

IPv4 CIDR block [Info](#)

IPv4 CIDR manual input
 IPAM-allocated IPv4 CIDR block

IPv4 CIDR

192.168.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

No IPv6 CIDR block
 IPAM-allocated IPv6 CIDR block
 Amazon-provided IPv6 CIDR block
 IPv6 CIDR owned by me

Public Subnet

Navigate to *Subnets* and click on *Create subnet*. Select the newly created VPC *VTAIR VPC* and give the subnet a name. We will use *vtair-public-subnet* and choose the first ip network *192.168.0.0/24*.

Make sure to select the same *availability zone* for both subnets.

[VPC](#) > [Subnets](#) > Create subnet

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.

vpc-05c5ffb1ed04bc09a (VTAIR-VPC) ▼

Associated VPC CIDRs

IPv4 CIDRs

192.168.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

vtair-public-subnet

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1a ▼

IPv4 VPC CIDR block [Info](#)
Choose the IPv4 VPC CIDR block to create a subnet in.

192.168.0.0/16 ▼

IPv4 subnet CIDR block

192.168.0.0/24 256 IPs

< > ^ v

Private Subnet

Navigate to *Subnets* and click on *Create subnet*. Select the newly created VPC *VTAIR VPC* and give the subnet a name. We will use *vtair-private-subnet* and choose the first ip network *192.168.1.0/24*.

Make sure to select the same *availability zone* for both subnets.

VPC > Subnets > Create subnet

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.

vpc-05c5ffb1ed04bc09a (VTAIR-VPC) ▼

Associated VPC CIDRs

IPv4 CIDRs

192.168.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

vtair-private-subnet

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1a ▼

IPv4 VPC CIDR block [Info](#)
Choose the IPv4 VPC CIDR block to create a subnet in.

192.168.0.0/16 ▼

IPv4 subnet CIDR block

192.168.1.0/24 256 IPs

< > ^ v

Public Routing Table

We will create a Public Routing Table that is used with the Public Subnet. It will contain an *Internet Gateway* that we connect to the default route of the Routing Table.

Navigate to *Route Tables* and click on *Create route table*. Select the newly created VPC *VTAIR VPC* and give the routing table a name. We will use *vtair-public-routetable*.

[VPC](#) > [Route tables](#) > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

VPC
The VPC to use for this route table.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="vtair-public-routetable"/>
	<input type="button" value="Remove"/>

You can add 49 more tags.

We need to connect the routing table to the *Public Subnet*.

Navigate to *Subnets* and select the *vtair-public-subnet*. In the menu on the bottom select the *Route Table* tab and press *Edit route table association*.

subnet-0d8ad0b3827ff4d97 / vtair-public-subnet

Details | Flow logs | **Route table** | Network ACL | CIDR reservations | Sharing | Tags

Route table: [rtb-02a938d4d89de082e / vtair-public-routetable](#)

Select the *vtair-public-routetable* in the dropdown menu and save.

[VPC](#) > [Subnets](#) > [subnet-0d8ad0b3827ff4d97](#) > Edit route table association

Edit route table association Info

Subnet route table settings

Subnet ID

Route table ID

Internet Gateway

We need to create an *Internet Gateway* for the *Public Routing Table* as a default route. Navigate to *Internet Gateways* and click on *Create internet gateway*.

We will use the name *vtair-public-gateway*.

VPC > Internet gateways > Create internet gateway

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.

Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
Q Name X	Q vtair-public-gateway X	Remove
<input type="button" value="Add new tag"/>		

You can add 49 more tags.

We now have to connect the *Internet Gateway* with the routing table. Navigate to *Route Tables* and click on the *vtair-public-routetable*. In the menu on the bottom select the *Routes* tab and press *Edit routes*.

rtb-02a938d4d89de082e / vtair-public-routetable

Details | **Routes** | Subnet associations | Edge associations | Route propagation | Tags

Routes (2) Both ▼ Edit routes

Create a new route with destination *0.0.0.0/0* and as target select *Internet Gateway* and select the newly created Gateway in the dropdown.

VPC > Route tables > rtb-02a938d4d89de082e > Edit routes

Edit routes

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
Q 0.0.0.0/0 X	Internet Gateway	Active	No

Private Routing Table

We will create a Private Routing Table that is used with the Private Subnet. It will contain the *VT AIR LAN Interface* that we connect to the default route of the Routing Table. This step needs to be done after the VT AIR EC2 VM is up and running.

Navigate to *Route Tables* and click on *Create route table*. Select the newly created VPC *VTAIR VPC* and give the routing table a name. We will use *vtair-private-routetable*.

VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

VPC
The VPC to use for this route table.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="vtair-private-routetable"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

We need to connect the routing table to the *Private Subnet*.

Navigate to *Subnets* and select the *vtair-private-subnet*. In the menu on the bottom select the *Route Table* tab and press *Edit route table association*.

subnet-05a536d1e6ed12b4b / vtair-private-subnet

Details | Flow logs | **Route table** | Network ACL | CIDR reservations | Sharing | Tags

Route table: **rtb-0e9fa2d8acf9628de / vtair-private-routetable**

Select the *vtair-private-routetable* in the dropdown menu and save.

VPC > Subnets > subnet-05a536d1e6ed12b4b > Edit route table association

Edit route table association [Info](#)

Subnet route table settings

Subnet ID

Route table ID

Public Security Group

We need to create a Public Security Group that will be associated with the VT AIR Public Network Interface. You can customize the group to your needs, we do recommend to add at least the following entries:

- Port 22 (TCP)
- Port 443 (TCP)

and depending on which VPN is used:

- 1194 (UDP) for OpenVPN
- 51280 (UDP) for Wireguard
- 500 and 4500 (UDP) for IPSec
- ESP/AH for IPSec

Navigate to *Security Groups* and click on *Create security group*. Select the newly created VPC *VTAIR VPC* and give the security group a name and a description. We will use *VTAIR-Public-SecurityGroup* and *VT AIR Public Access*.

VPC > Security Groups > Create security group

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

For the inbound traffic we created all rules above.

Security group rule ID	Type info	Protocol info	Port range info	Source info	Description - optional info	
sgr-0fe2156139c001794	Custom Protocol	AH (51)	All	Custom	IPSec	Delete
sg-0619684190b7b2e5	HTTPS	TCP	443	Custom	HTTPS	Delete
sg-079475f47e74c8ff	Custom UDP	UDP	500	Custom	IPSec	Delete
sg-003bd350e7497645b	SSH	TCP	22	Custom	SSH	Delete
sg-071001fa55c29f53b	Custom UDP	UDP	51280	Custom	Wireguard	Delete
sg-0a6d1b3f9b84263ef	Custom Protocol	ESP (50)	All	Custom	IPSec	Delete
sg-061b765ae318a52e	Custom UDP	UDP	1194	Custom	OpenVPN	Delete
sg-0a045bb82d1819f7d	Custom UDP	UDP	4500	Custom	IPSec	Delete

Private Security Group

We need to create a Private Security Group that will be associated with the VT AIR Private Network Interface. We will allow all traffic on the private side as it is protected by the VT AIR Firewall.

Navigate to *Security Groups* and click on *Create security group*. Select the newly created VPC *VT AIR VPC* and give the security group a name and a description. We will use *VT AIR-Private-SecurityGroup* and *VT AIR Private Access*.

VPC > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

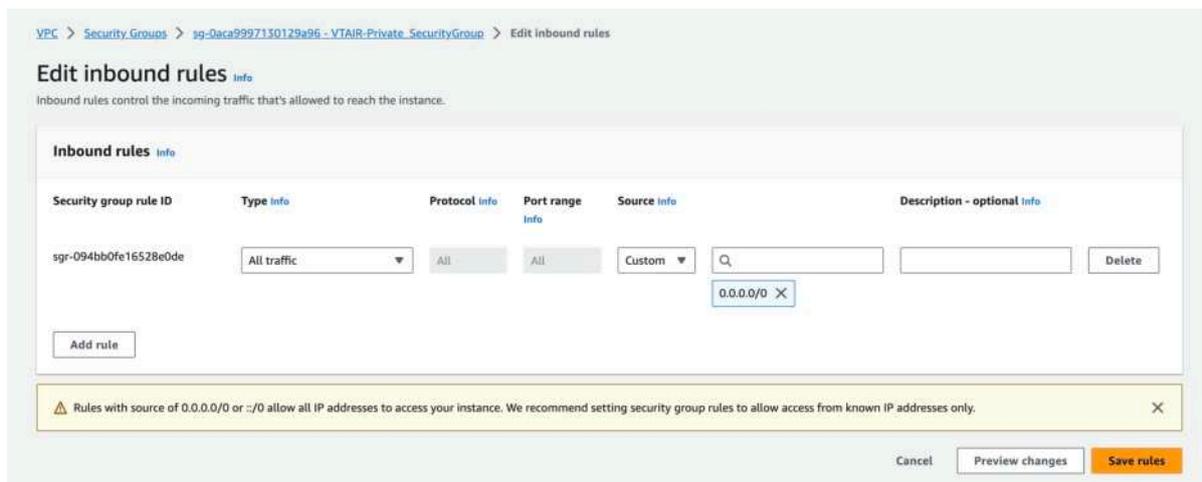
Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info

For the inbound traffic we created the allow all rule.

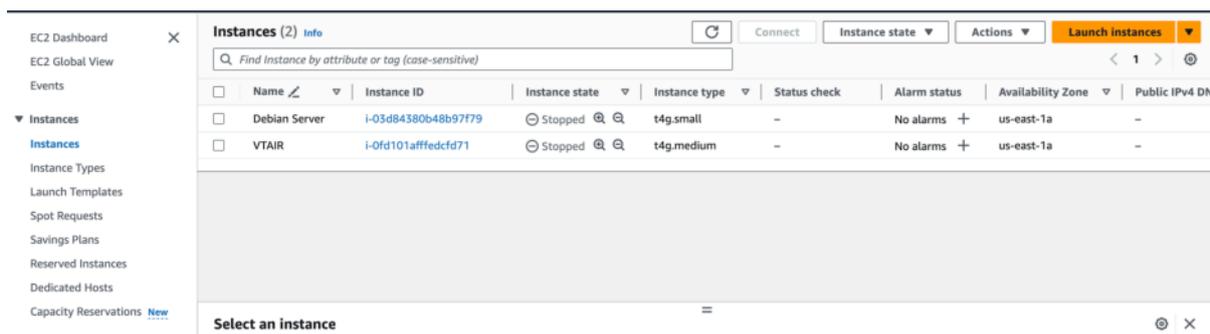


3.8.3 EC2 VT AIR Appliance

It is time to create and start the VT AIR Appliance.

We have created videos to show the entire configurations.

Navigate to EC2 and select *Instances* and press *Launch instances*.



We will name the instance *VTAIR*. Search for *VT AIR* in the Amazon Machine Image.

Choose your preferred *Instance type*.

Select your instance type and a key pair for the default SSH connection.

The instance will also be available via the webgui.

Name and tags [Info](#)

Name

VTAIR [Add additional tags](#)

▼ **Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q VT AIR X

[Recents](#) | [My AMIs](#) | [Quick Start](#)

Recently launched

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

VT AIR 23.07.1 (arm64)-6f3ad8e4-2f15-491f-a7e4-626b8a48f488
ami-0b287c994a7ef4396
2023-09-09T09:07:22.000Z Architecture: 64-bit (Arm) Virtualization: hvm ENA enabled: true Root device type: ebs
Boot mode: uefi

Description

-

Architecture	AMI ID	
arm64	ami-0b287c994a7ef4396	Verified provider

Public Network Interface (WAN)

In the network settings choose the create VPC *VT AIR VPC*. Also choose the public network *vtair-public-subnet*. You need to disable the *Auto-assign public IP* option as it will not working with multiple network interfaces.

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-05c5ffb1ed04bc09a (VTAIR-VPC)
192.168.0.0/16

Subnet [Info](#)

subnet-0d8ad0b3827ff4d97 vtair-public-subnet
VPC: vpc-05c5ffb1ed04bc09a Owner: 963271161047 Availability Zone: us-east-1a
IP addresses available: 250 CIDR: 192.168.0.0/24

Auto-assign public IP [Info](#)

Disable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Common security groups [Info](#)

Select security groups

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► **Advanced network configuration**

For the security group select *Select existing security group*

Click on *Advanced network configuration*

The *Network Interface 1* will be our Public Network Interface (WAN). Select the Security Group *VTAIR-Public-SecurityGroup* for this interface. We also want to give a static IP to the interface, the first 4 or 5 IPs are in use by the subnet so we start at 10. The IP is assigned via DHCP. We set the IP to *192.168.0.10*.

▼ **Advanced network configuration**

Network interface 1

Device index Info <input type="text" value="0"/>	Network interface Info <input type="text" value="New interface"/> ▼	Description Info <input type="text"/>
Subnet Info subnet-Od8ad0b3827ff4d97 <small>IP addresses available: 250</small>	Security groups Info <input type="text" value="Select security groups"/> ▼  <input type="button" value="Show all selected (1)"/>	Primary IP Info <input type="text" value="192.168.0.10"/>
Secondary IP Info <input type="text" value="Select"/> ▼	IPv6 IPs Info <input type="text" value="Select"/> ▼ <small>The selected subnet does not support IPv6 IPs.</small>	IPv4 Prefixes Info <input type="text" value="Select"/> ▼
IPv6 Prefixes Info <input type="text" value="Select"/> ▼ <small>The selected subnet does not support IPv6 prefixes because it does not have an IPv6 CIDR.</small>	Assign Primary IPv6 IP Info <input type="text" value="Select"/> ▼ <small>A primary IPv6 address is only compatible with subnets that support IPv6.</small>	Delete on termination Info <input type="text" value="Select"/> ▼
Elastic Fabric Adapter Info <input type="checkbox"/> Enable <small>The selected instance type does not support EFA.</small>	Network card index Info <input type="text" value="Select"/> ▼ <small>The selected instance type does not support multiple network cards.</small>	

Private Network Interface (LAN)

Click on the *Add network interface* button to create a second interface for the LAN side. As subnet select *vtair-private-subnet* and also choose the security group *VTAIR-Private-SecurityGroup*

We also want to give a static IP to the interface, the first 4 or 5 IPs are in use by the subnet so we start at 10. The IP is assigned via DHCP. We set the IP to *192.168.1.10*.

Network interface 2 Remove

Device index Info <input type="text" value="1"/>	Network interface Info <input type="text" value="New interface"/>	Description Info <input type="text"/>
Subnet Info <input type="text" value="subnet-05a536d1e6ed12b4b"/> <p><small>IP addresses available: 249</small></p>	Security groups Info <input type="text" value="Select security groups"/> <p>+ Show all selected (1)</p>	Primary IP Info <input type="text" value="192.168.1.10"/>
Secondary IP Info <input type="text" value="Select"/>	IPv6 IPs Info <input type="text" value="Select"/> <p><small>The selected subnet does not support IPv6 IPs.</small></p>	IPv4 Prefixes Info <input type="text" value="Select"/>
IPv6 Prefixes Info <input type="text" value="Select"/> <p><small>The selected subnet does not support IPv6 prefixes because it does not have an IPv6 CIDR.</small></p>	Assign Primary IPv6 IP Info <input type="text" value="Select"/> <p><small>A primary IPv6 address is only compatible with subnets that support IPv6.</small></p>	Delete on termination Info <input type="text" value="Select"/>
Elastic Fabric Adapter Info <input type="checkbox"/> Enable <p><small>The selected instance type does not support EFA.</small></p>	Network card index Info <input type="text" value="Select"/> <p><small>The selected instance type does not support multiple network cards.</small></p>	

[Add network interface](#)

Storage

Make sure to select a large enough storage space. We recommend 30GB or more. All settings are finished, you can create and run the instance.

▼ **Configure storage** [Info](#)
Advanced

1x GiB Root volume (Not encrypted)

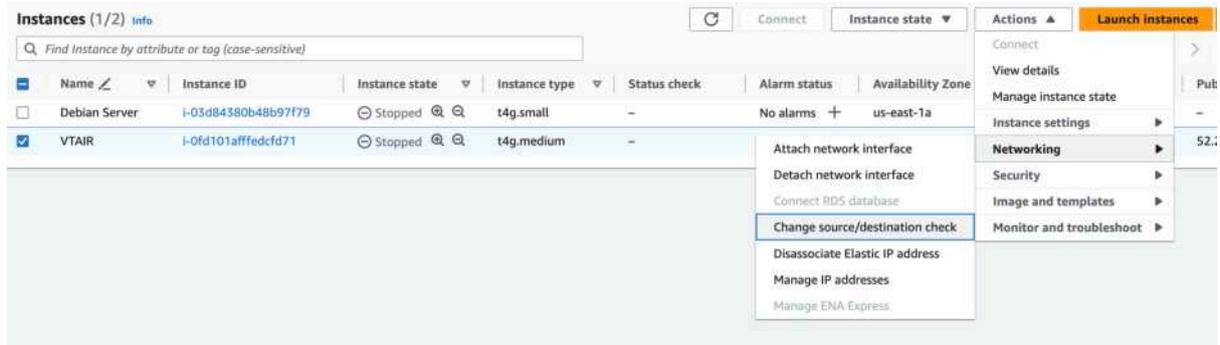
[i](#) Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
✕

[Add new volume](#)

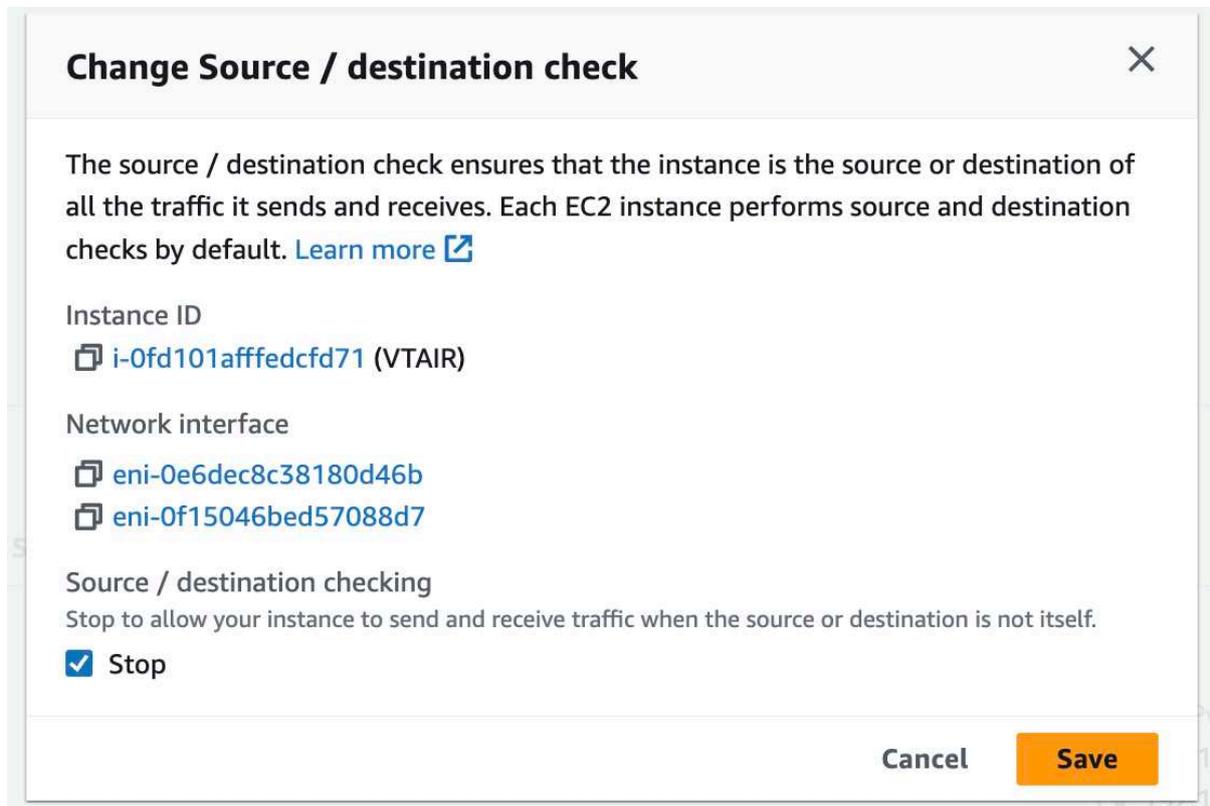
0 x File systems [Edit](#)

Disable Source and Destination Check

In order to forward traffic, the option *Disable Source and Destination Check* has to be disabled. In *EC2* -> *Instances* select the newly created VT AIR instance.



In the menu select *Actions* -> *Networking* -> *Change source/destination check*. A new popup will appear. Select the option *Stop* at the bottom and press *Save*



Allocate Elastic IP

For the VT AIR instance to be reachable via the internet, a new Elastic IP has to be created and attached to the Public Network Interface.

First go to *EC2* -> *Instances* and write down the network interface names. Make sure to select the public network interface for the Elastic IP and the private network interface for the next step to connect it to the private routing table.

Instance: i-0fd101affedcfd71 (VTAIR)

▼ Network Interfaces (2) [Info](#)

Interface ID	Description
 eni-0e6dec8c38180d46b	Private Network LAN
 eni-0f15046bed57088d7	Public Network WAN

Navigate to *EC2 -> Network Security -> Elastic IP* and click on *Allocate Elastic IP address*.

Elastic IP addresses (1/1) Actions

< 1 > 

<input checked="" type="checkbox"/>	Name	Allocated IPv4 add...	Type	Allocation ID	Reverse DNS record
<input checked="" type="checkbox"/>	-	52.20.84.124	Public IP	eipalloc-0a4c1dad0bfebad64	-

Allocate the IP with the appropriate settings.

EC2 > Elastic IP addresses > Allocate Elastic IP address

Allocate Elastic IP address [Info](#)

Elastic IP address settings [Info](#)

Network Border Group [Info](#)

Public IPv4 address pool

- Amazon's pool of IPv4 addresses
- Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) [Learn more](#)
- Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) [Learn more](#)

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more](#)

[Create accelerator](#)

Select the newly created *Elastic IP* and click on the *Action* button. Choose the option *Associate Elastic IP address* and choose the option *Network interface*.

Elastic IP addresses (1/1)

<input checked="" type="checkbox"/>	Name	Allocated IPv4 add...	Type	Allocation ID	record
<input checked="" type="checkbox"/>	-	52.20.84.124	Public IP	eipalloc-0a4c1...	

Actions

- Allocate Elastic IP address
- View details
- Release Elastic IP addresses
- Associate Elastic IP address
- Disassociate Elastic IP address
- Update reverse DNS
- Enable transfers
- Disable transfers
- Accept transfers

Look for the public network interface of the VT AIR instance and also select the IP address, in our case *192.168.0.10*.

EC2 > Elastic IP addresses > Associate Elastic IP address

Associate Elastic IP address Info

Choose the instance or network interface to associate to this Elastic IP address (52.20.84.124)

Elastic IP address: 52.20.84.124

Resource type
Choose the type of resource with which to associate the Elastic IP address.

Instance

Network interface

⚠ If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Network interface

eni-0f15046bed57088d7 ✕ ↻

Private IP address
The private IP address with which to associate the Elastic IP address.

192.168.0.10 ✕

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

Allow this Elastic IP address to be reassociated

Cancel Associate

Save the settings.

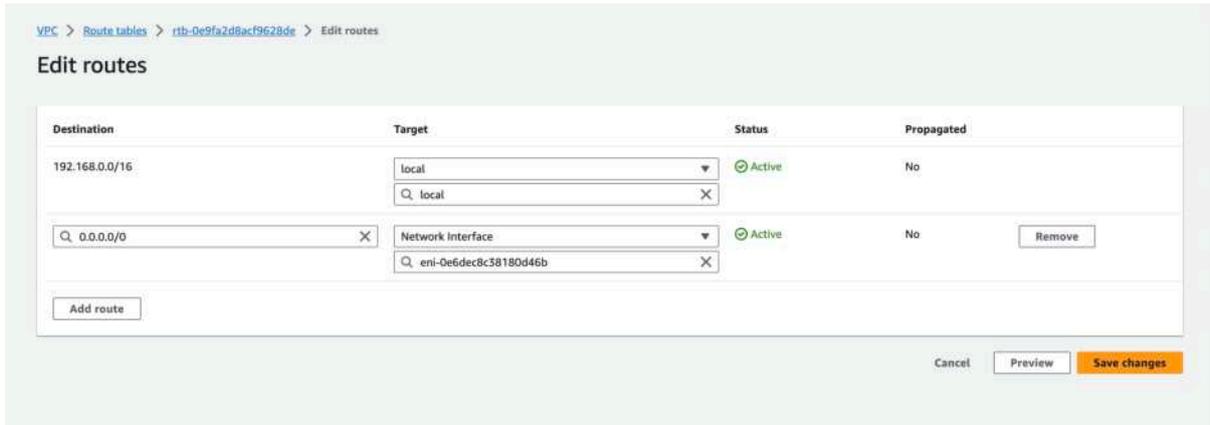
Default route pointing to VT AIR LAN interface

The next step needs to be completed in the VPC settings. The Private Network Interface (LAN) needs to be the default gateway for the *vtair-private-routetable*

Navigate to *Route Tables* and click on the *vtair-private-routetable*. In the menu on the bottom select the *Routes* tab and press *Edit routes*.

The screenshot shows the AWS console interface for a specific Route Table. The breadcrumb path is 'rtb-0e9fa2d8acf9628de / vtair-private-routetable'. There are tabs for 'Details', 'Routes', 'Subnet associations', 'Edge associations', 'Route propagation', and 'Tags'. The 'Routes' tab is active, showing a list of routes. At the top right of the routes list, there are buttons for 'Both' (with a dropdown arrow) and 'Edit routes'. Below the list, there is a search bar labeled 'Filter routes' and pagination controls showing '1' of 1 routes.

Create a new route with destination *0.0.0.0/0* and as target select *Network Interface* and select the *Private Network Interface* from the VT AIR instance.

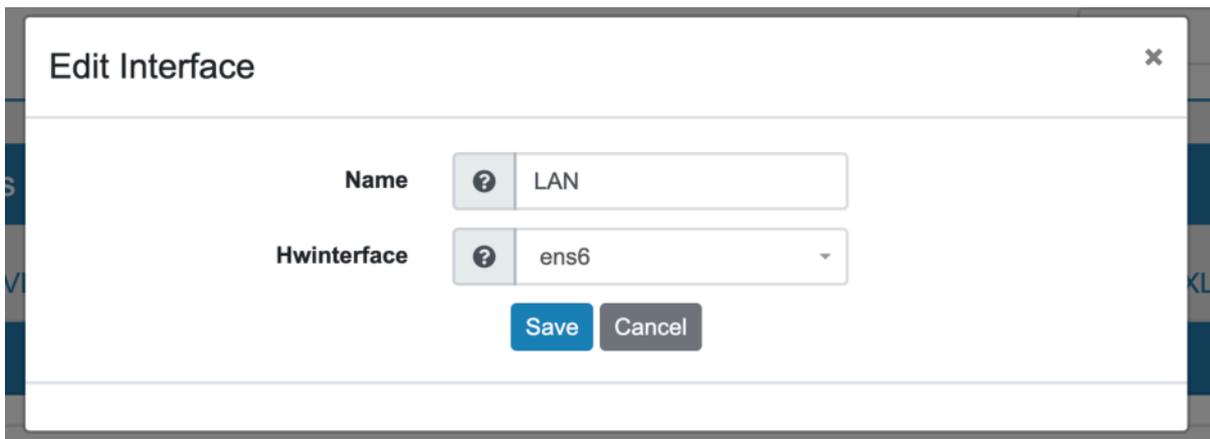


3.8.4 VT AIR configuration

We will now need to login to the VT AIR instance webgui to configure the LAN interface and additional settings.

Enable and set LAN Interface

In the webgui navigate to *Interfaces* -> *Assign*. Select the edit button next to the *LAN* interface and assign the new interface to it.



Switch to the *LAN* interface settings by going to *Interfaces* -> *LAN*. Enable the interface and set the IPv4 type to DHCP. Save the settings.

General (ens6)

Enabled

Name

MAC Address

MTU

MSS

Speed and Duplex

IPv4 Settings

IPv4 Type

Hostname

Lease Time

This will enable the LAN interface and the IP *192.168.1.10* will be assigned.

Dashboard +

System x

Clock x

Name	vtair.localhost
System	VT AIR AWS
Serial Number	ec283fc1-f334-0544-4898-f04fbcecd573
Device ID	c8ed6608d003df7753828d7cbd0cd368
Licence	Valid
Updates until	Lifetime

Interfaces ⚙ x

WAN	↑	N/A	192.168.0.10
LAN	↑	N/A	192.168.1.10
AppBridge	↑	N/A	172.30.0.1

Create DNAT Rules and VPN Configuration

You can now create all the different setting you need for your setup. To make instances behind VT AIR available to the elastic IP, configure a DNAT rule.

You can also configure the different VPN options.

3.8.5 EC2 VMs

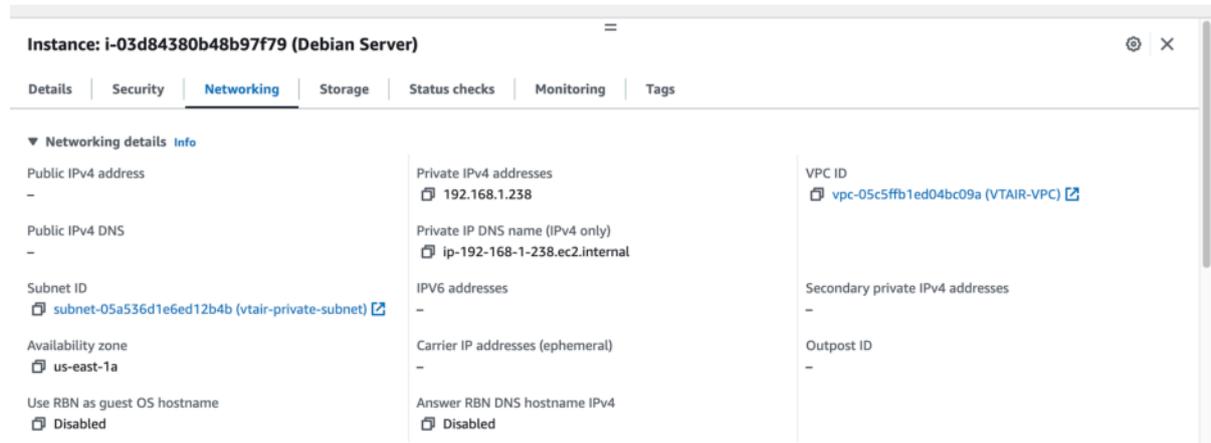
Connect EC2 VMs to the private subnet so they are in the *LAN* network of the VT AIR.

We have created videos to show the entire configurations.

Add to the Private Network Subnet

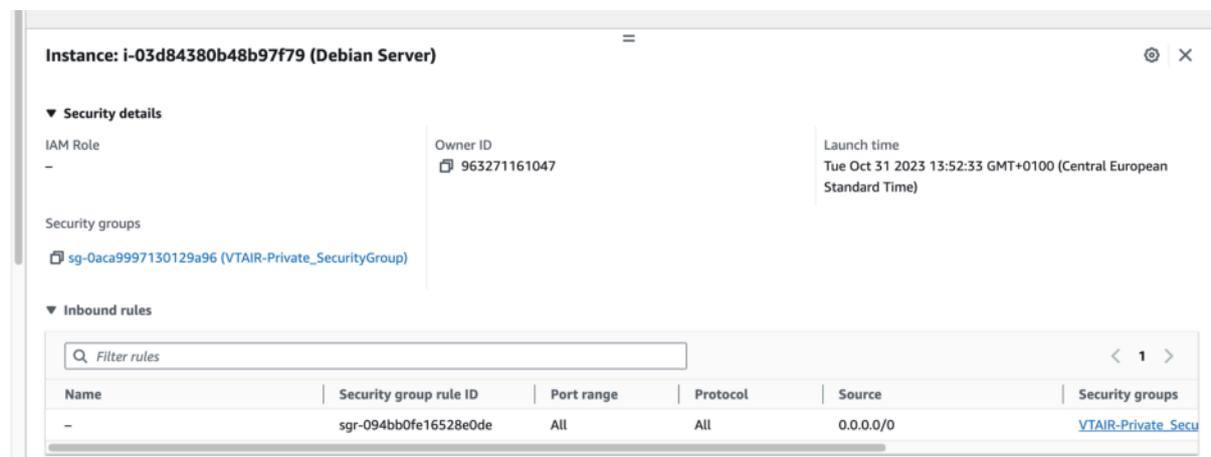
If you have already running instances, you need to create an AMI image of the VM, stop it and relaunch it in the new VPC and private subnet. AWS unfortunately does not offer an option to move a running VM to the new VPC/subnet.

When you create a new VM, you can select the VPC and private subnet in the network settings when you create it.



Set Private Security Group

Make sure to select an appropriate Security Group so the VM can be accessed by the VT AIR.



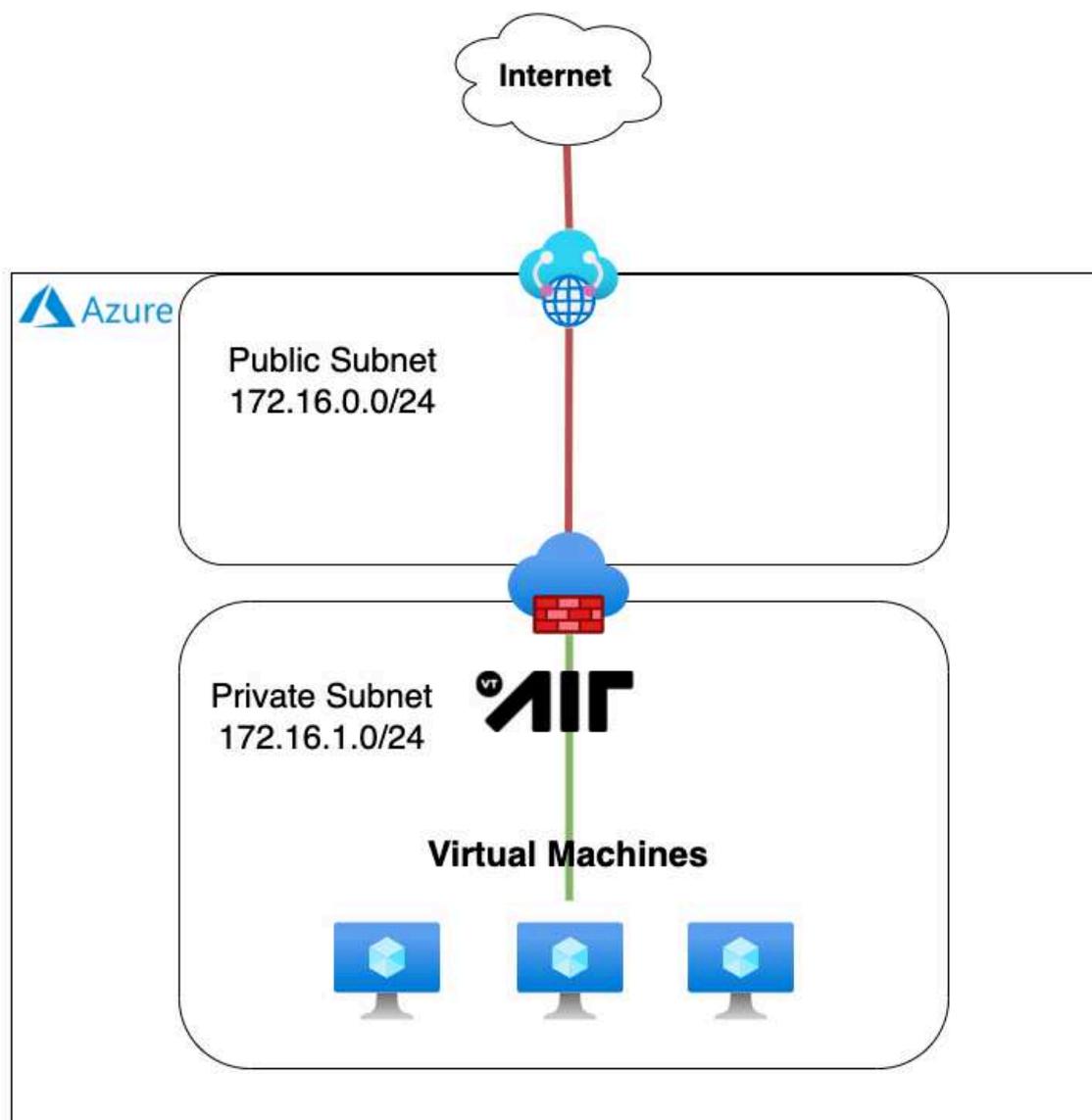
3.9 VT AIR Azure

VT AIR Azure brings you all VT AIR feature to Microsoft Azure Cloud.

VT AIR Azure can be run in any region where Azure offers service on various sizes of instance. VT AIR for Azure is available in the [Azure Marketplace](#).

All features are available in the Azure Version and you can use VT AIR as a firewall to protect your Virtual Machines or as a VPN server to connect via IPSec, OpenVPN or WireGuard.

VT AIR Azure Architecture



In order to configure your Azure environment to utilize VT AIR as a firewall in front of other VMs, a couple of configuration steps have to be done.

1. Virtual Network Configuration
 1. New Virtual Network
 2. Public Subnet
 3. Private Subnet
 4. Private Routing Table
 5. Public Network Security Group
 6. Private Network Security Group
 7. Private Network Interface

- Enable Traffic Forwarding
 - Associate Private Network Security Group
2. Azure VT AIR Appliance
 1. Public Network Interface (WAN)
 - In the Public Subnet
 - Public Network Security Group
 2. Private Network Interface (LAN)
 - Default route pointing to VT AIR LAN interface
 3. VT AIR configuration
 1. Enable and set LAN Interface
 2. Create DNAT Rules and VPN Configuration
 4. Azure VMs
 1. Add to the Private Network Subnet
 2. Set Private Network Security Group

3.9.1 Default Login

Default login data for the WebGUI are user **admin** and the password is **vtair**.

3.9.2 Important Information

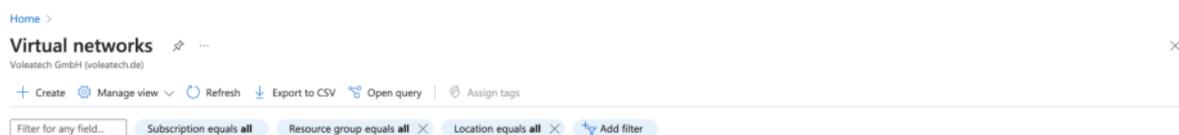
Be aware that not all the usual network operations are possible. There is no support for

1. ARP
2. Multicast
3. Broadcast

in Azure.

3.9.3 Virtual Network Configuration

Login to your Azure Account and change to the Virtual Networks configuration page.



We have created videos to show the entire configurations.

New Virtual Network

We will create a new Virtual Network for the VT AIR setup. If you already have a Virtual Network with two subnets configured, you can skip these steps.

Click on *Create*.

Choose your *Subscription*, *Resource group* and *Region* and give the Virtual Network a name, in our case we choose *VTAIRVirtualNetwork*.

[Home](#) > [Virtual networks](#) >

Create virtual network ...

Basics Security IP addresses Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.
[Learn more.](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group *
[Create new](#)

Instance details

Virtual network name *

Region ⓘ *

[Deploy to an edge zone](#)

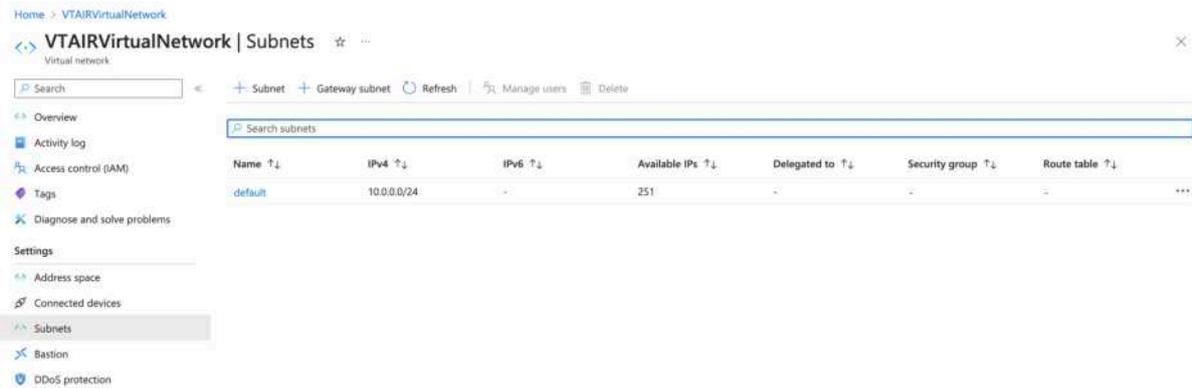
[Previous](#) [Next](#) [Review + create](#)

Public Subnet

A default subnet is created alongside your Virtual Network. We will use it as the public subnet, it has the ip range *10.0.0.0/24*.

Private Subnet

Navigate to the Virtual Network and open *Subnets* in the Settings and click on *Subnet*.



Give the subnet a name. We will use *VTAIRPrivateSubnet* and create the ip network *10.0.1.0/24*.

Add subnet ✕

Name *

VTAIRPrivateSubnet ✓

Subnet address range * ⓘ

10.0.1.0/24

10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space ⓘ

NAT gateway ⓘ

None ▼

Network security group

None ▼

Route table

None ▼

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

0 selected ▼

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None ▼

Save

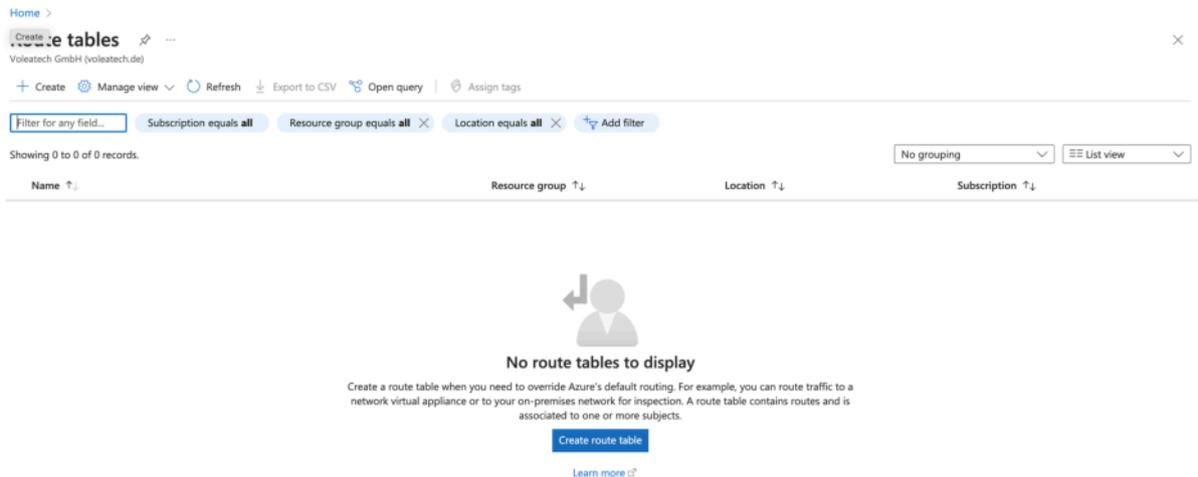
Cancel

 Give feedback

Private Routing Table

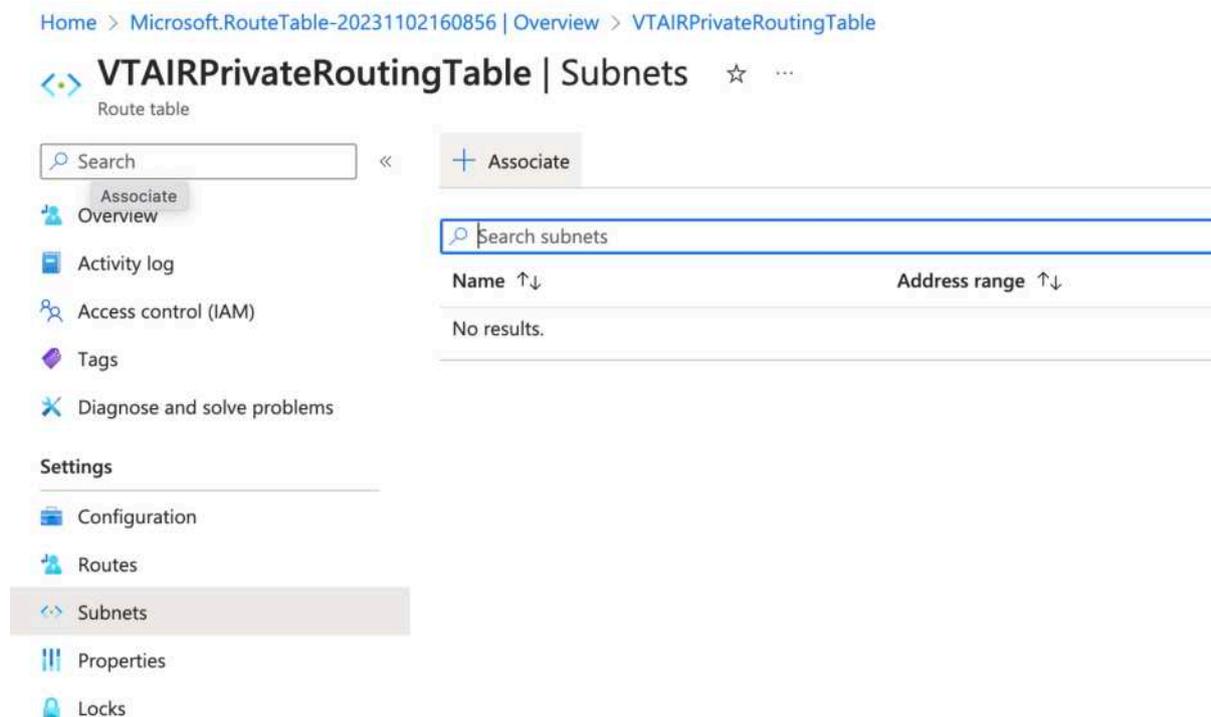
We will create a Private Routing Table that is used with the Private Subnet. It will contain the *VT AIR LAN Interface* that we connect to the default route of the Routing Table. This step needs to be done after the VT AIR Azure VM is up and running.

Navigate to *Route tables* and click on *Create*. Choose your *Subscription*, *Resource group* and *Region* and give the routing table a name. We will use *VTAIRPrivateRoutingTable*.



We need to connect the routing table to the *Private Subnet*.

Open the newly created routing table and navigate to *Subnets* and click on *Associate*.



Select the virtual network *VTAIRVirtualNetwork* and choose the *VTAIRPrivateSubnet*.

Associate subnet ✕

VTAIRPrivateRoutingTable

Virtual network * ⓘ

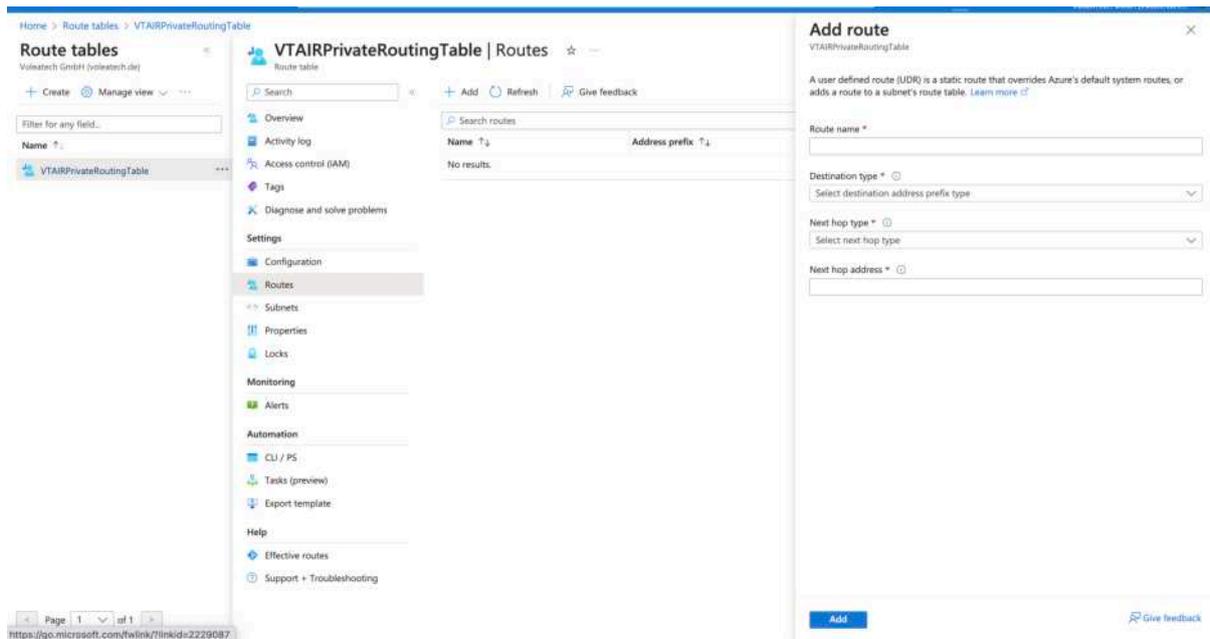
VTAIRVirtualNetwork (VTAIRResourceGroupVM) ▾

Subnet * ⓘ

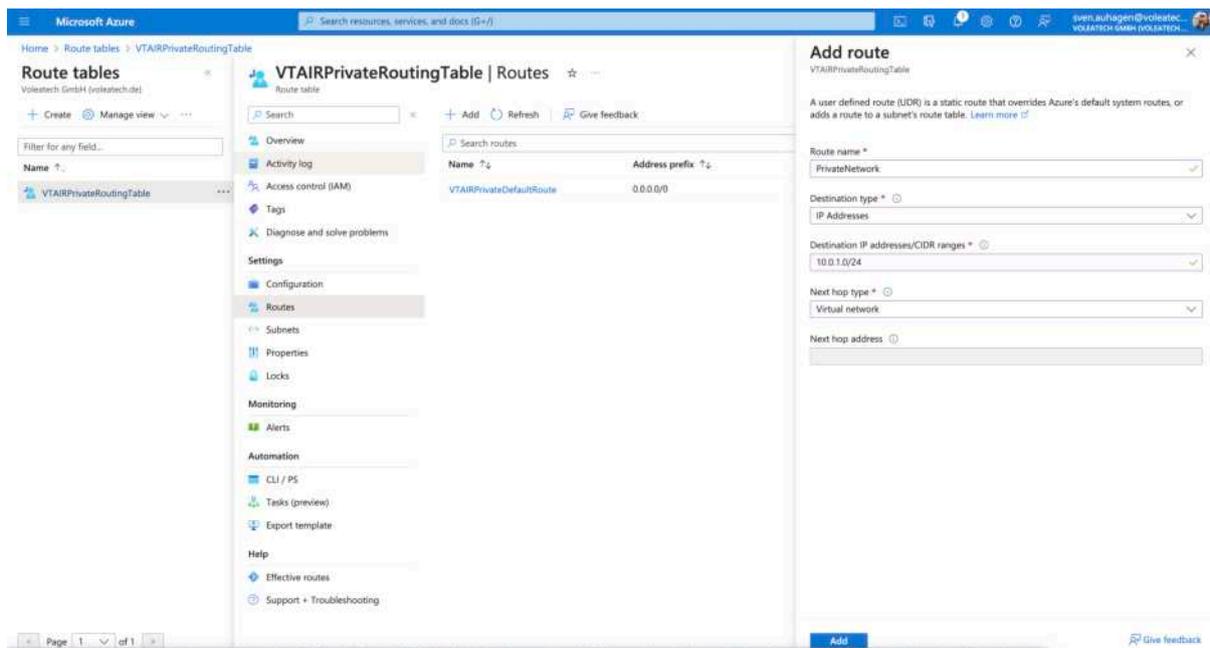
VTAIRPrivateSubnet ▾

OK [Give feedback](#)

We need to add the network route to the routing table. Navigate to *Routes* and click on *Add*.



Give the route a name *PrivateNetwork*, the destination type is *IP Addresses*, the Destination is the network ip range *10.0.1.0/24* and the next hop type *Virtual network*.



Public Network Security Group

We need to create a Public Network Security Group that will be associated with the VT AIR Public Network Interface. You can customize the group to your needs, we do recommend to add at least the following entries:

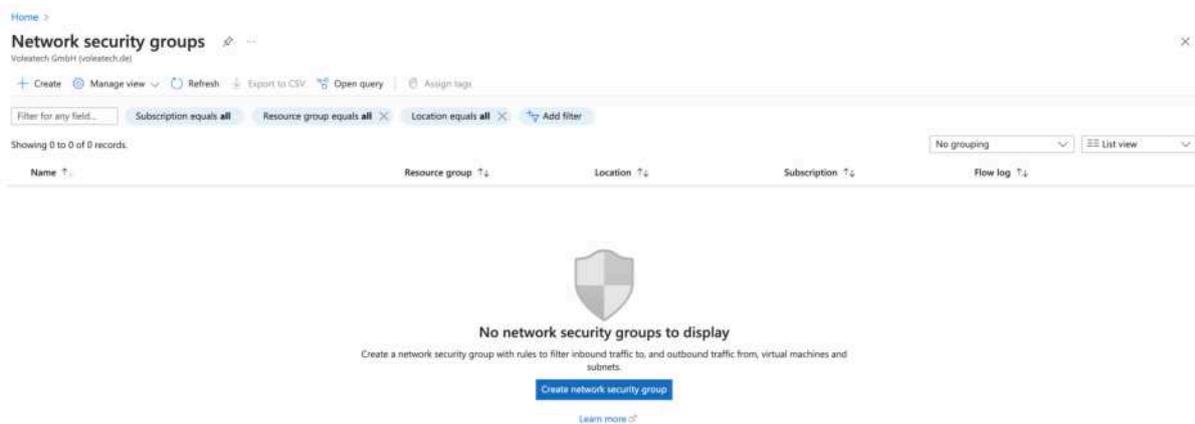
- Port 22 (TCP)
- Port 443 (TCP)

and depending on which VPN is used:

- 1194 (UDP) for OpenVPN
- 51280 (UDP) for Wireguard

- 500 and 4500 (UDP) for IPSec
- ESP/AH for IPSec

Navigate to *Network security groups* and click on *Create*.



Choose your *Subscription*, *Resource group* and *Region* and give the network security group a name. We will use *VTAIRPublicSecurityGroup*.

Home > Network security groups >

Create network security group ...

Basics Tags Review + create

Project details

Subscription *

Resource group * [Create new](#)

Instance details

Name *

Region *

[Review + create](#) [< Previous](#) [Next : Tags >](#) [Download a template for automation](#)

For the inbound traffic we created all rules above.

Home > Microsoft.NetworkSecurityGroup-20231102161435 | Overview > VTAIRPublicSecurityGroup

VTAIRPublicSecurityGroup | Inbound security rules ☆ ...

Network security group

Search + Add Hide default rules Refresh Delete Give feedback

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
100	HTTPS	443	TCP	Any	Any	Allow
110	SSH	22	TCP	Any	Any	Allow
120	IPSec_IKE	500	UDP	Any	Any	Allow
130	IPSec_NATT	4500	UDP	Any	Any	Allow
140	OpenVPN	1194	UDP	Any	Any	Allow
150	Wireguard	51280	UDP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBo--	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Private Network Security Group

We need to create a Private Network Security Group that will be associated with the VT AIR Private Network Interface. We will allow all traffic on the private side as it is protected by the VT AIR Firewall.

Navigate to *Network security groups* and click on *Create*. Choose your *Subscription*, *Resource group* and *Region* and give the network security group a name.

We will use *VTAIRPrivateSecurityGroup*.

[Home](#) > [Network security groups](#) >

Create network security group ...

Basics Tags Review + create

Project details

Subscription *	<input type="text" value="Azure subscription 1"/>
Resource group *	<input type="text" value="VTAIRResourceGroupVM"/> Create new

Instance details

Name *	<input type="text" value="VTAIRPrivateSecurityGroup"/>
Region *	<input type="text" value="West Europe"/>

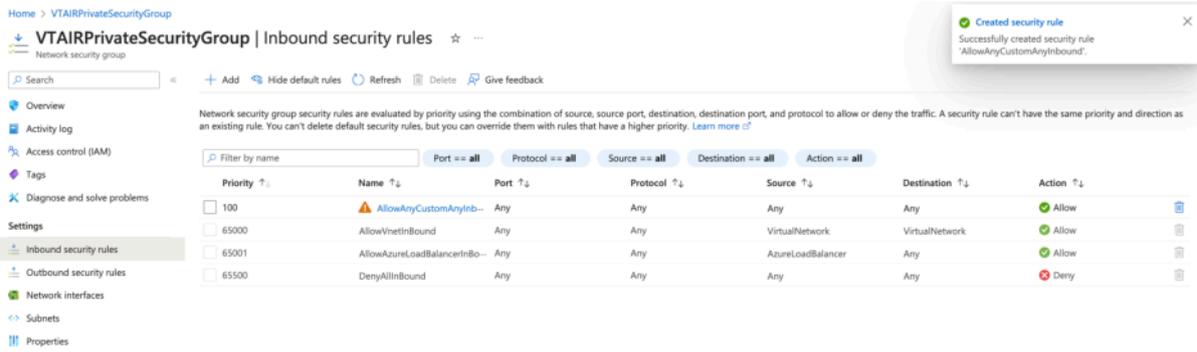
[Review + create](#)

[< Previous](#)

[Next : Tags >](#)

[Download a template for automation](#)

For the inbound traffic we created the allow all rule.



Private Network Interface

We need to create a Private Network Interface that will be associated with the VT AIR Private Network Interface. We will allow all traffic on the private side as it is protected by the VT AIR Firewall.

Navigate to *Network interfaces* and click on *Create*.



Choose your *Subscription*, *Resource group* and *Region* and give the network security group a name.

We will use *VTAIRPrivateNetworkinterface*.

Choose the Virtual Network *VTAIRVirtualNetwork* and the Subnet *VTAIRPrivate Subnet*

[Home](#) > [Network interfaces](#) >

Create network interface ...

[Basics](#) [Tags](#) [Review + create](#)

Create a network interface and attach it to a virtual machine. A network interface enables a virtual machine to communicate with Internet, Azure, and on-premises resources. [Learn more about network interface](#)

Project details

Subscription *	Azure subscription 1
Resource group *	VTAIRResourceGroupVM

[Create new](#)

Instance details

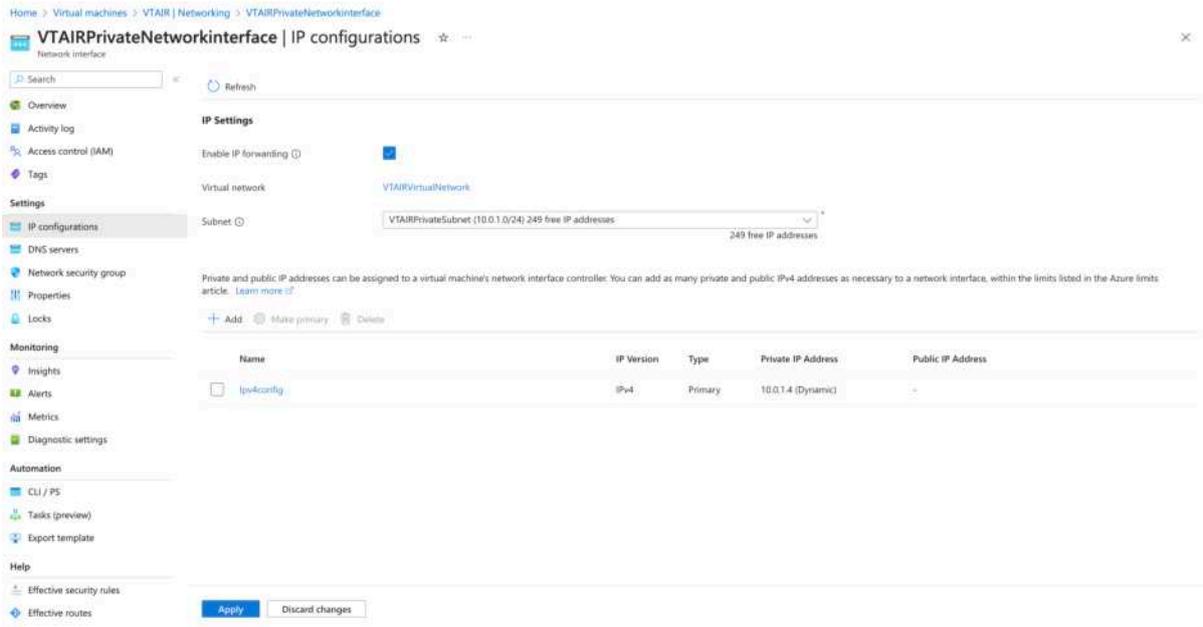
Name *	VTAIRPrivateNetworkinterface
Region *	West Europe
Virtual network * ⓘ	VTAIRVirtualNetwork (VTAIRResourceGroupVM)
Subnet * ⓘ	VTAIRPrivateSubnet
	Edit subnet 10.0.1.0 - 10.0.1.255 (256 addresses)
IP version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv4 and IPv6
Private IP address assignment	<input checked="" type="radio"/> Dynamic <input type="radio"/> Static

[Review + create](#)[< Previous](#)[Next : Tags >](#)[Download a template for automation](#)

Enable Traffic Forwarding

We need to allow the traffic forwarding for the newly created interface. Click on the newly created interface *VTAIRPrivateNetworkinterface*.

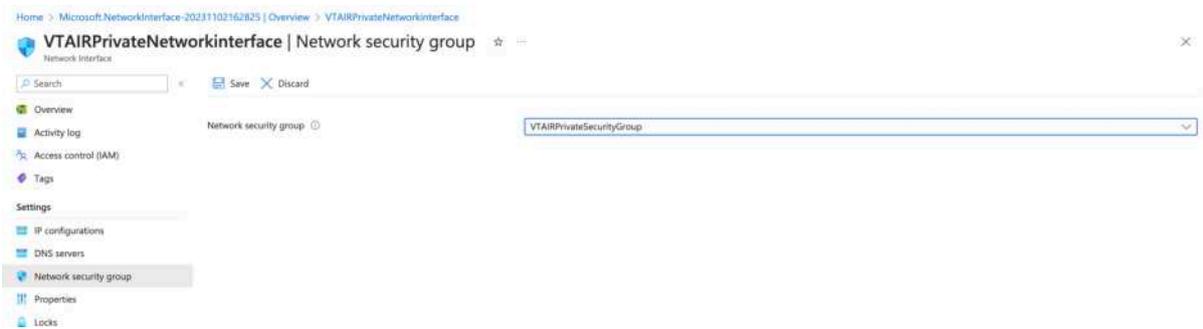
Navigate to *IP configurations* and click on *Enable IP forwarding*.



Associate Private Network Security Group

We need to associate the Private Network Security Group to the newly created interface. Click on the newly created interface *VTAIRPrivateNetworkinterface*.

Navigate to *Network security group* and choose *VTAIRPrivateSecurityGroup*.

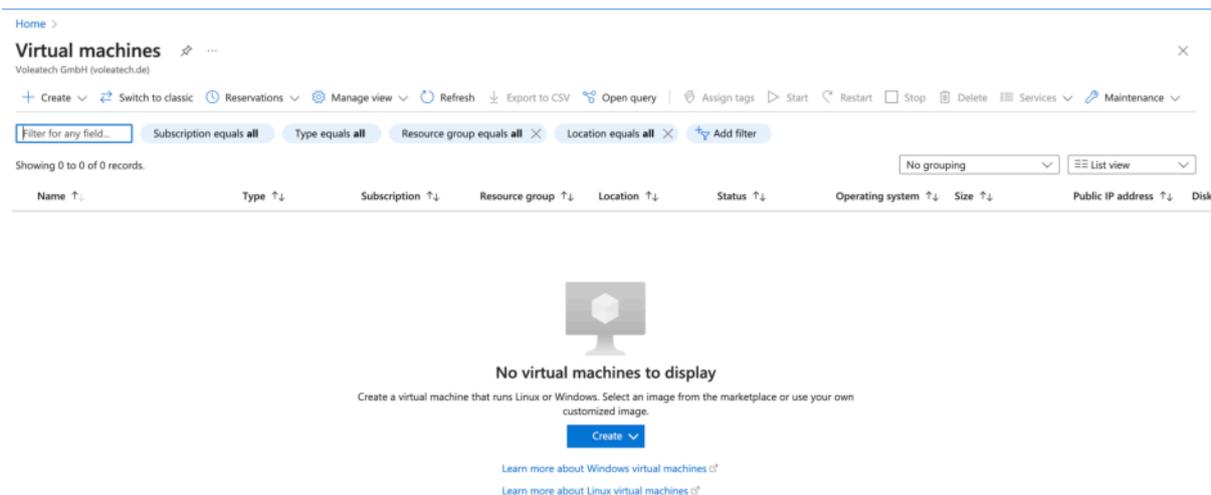


3.9.4 Azure VT AIR Appliance

It is time to create and start the VT AIR Appliance.

We have created videos to show the entire configurations.

Navigate to Virtual machines and select *Create* and pick *Azure virtual machine*.



Choose your *Subscription*, *Resource group* and *Region* and give the virtual machine a name.

We will name the instance *VTAIR*. Search for *VT AIR* in the Azure Machine Image.

Choose your preferred *Size*.

Select your size and a key pair for the default SSH connection.

The instance will also be available via the webgui.

[Home](#) > [Virtual machines](#) >

Create a virtual machine

Availability zone * ⓘ 

 You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#) 

Security type ⓘ 

Image * ⓘ 
[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ Arm64 x64

 Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ

Size * ⓘ 
[See all sizes](#)

Administrator account

Authentication type ⓘ SSH public key Password

 Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username * ⓘ 

SSH public key source 

Stored Keys 

[Review + create](#)[< Previous](#)[Next : Disks >](#)

Storage

Make sure to select a large enough storage space. We recommend 30GB or more.

Public Network Interface (WAN)

In the network settings choose the create Virtual Network *VTAIRVirtualNetwork*. Also choose the default subnet.

Home >

Create a virtual machine

Basics Disks **Networking** Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *

Subnet *

Public IP

NIC network security group None Basic Advanced

i This VM image has preconfigured NSG rules

Configure network security group *

Delete public IP and NIC when VM is deleted

Enable accelerated networking

Select *advanced* in the NIC network security group settings.

For the security group select *VTAIRPublicSecurityGroup*

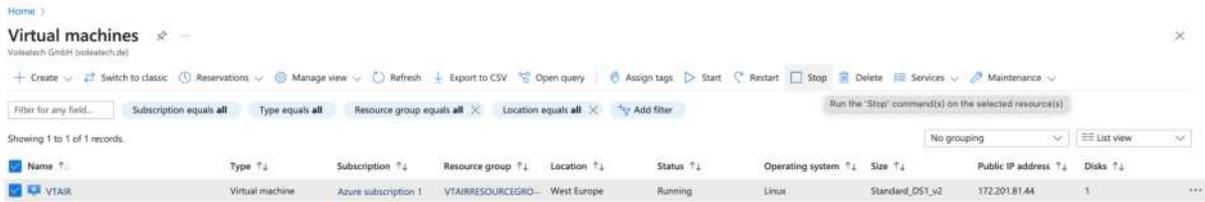
Click on *Advanced network configuration*

Make sure the setting *Enable accelerated networking* is enabled.

You can finish the creation of the Virtual Machine at this point.

Private Network Interface (LAN)

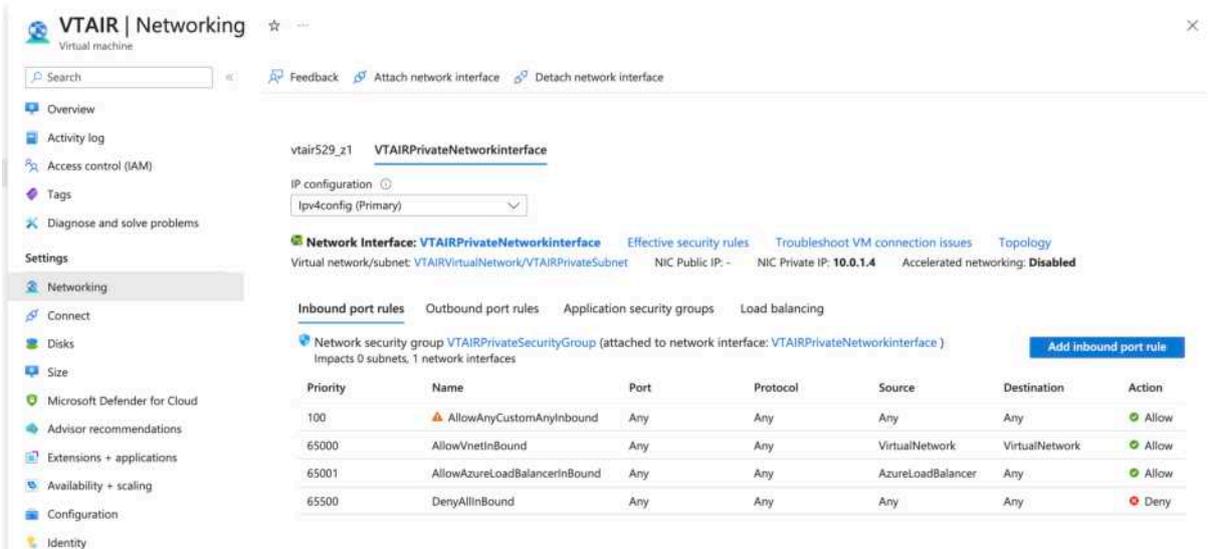
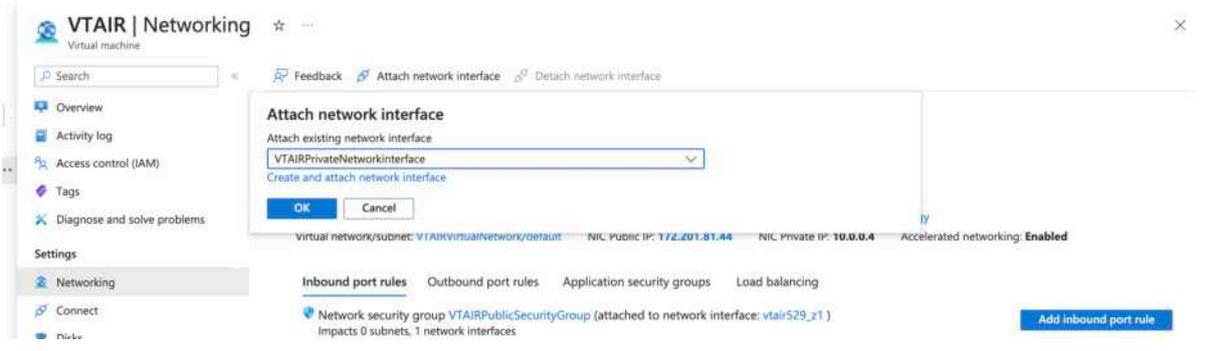
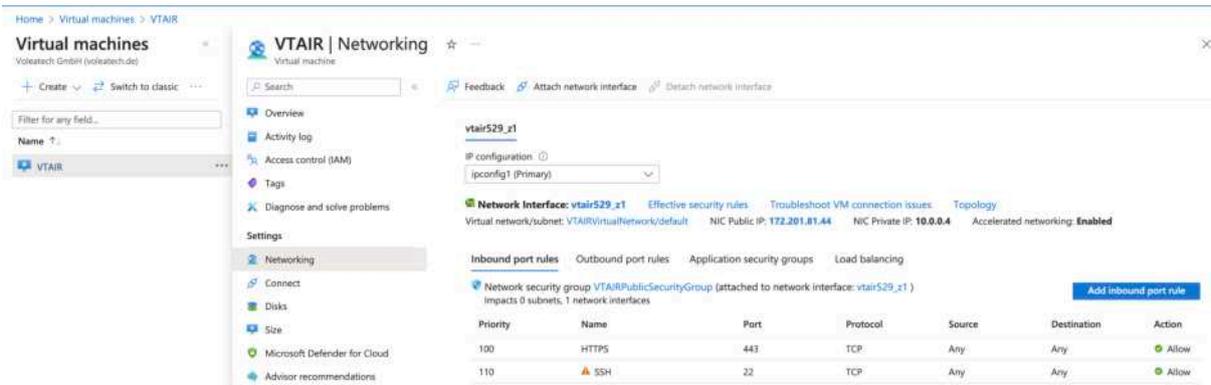
The Private Network Interface must be associated with the Virtual Machine after it is created. Wait until the virtual machine is fully created and running.



Stop the virtual machine at this point and go to the settings of the VM. Switch to *Settings* and *Networking*.

In the top menu click on *Attach network interface* and look for the *VTAIRPrivateNetworkinterface*.

Once the interface is associated with the VM, you can start it again. Also write down the IP Address of the new interface, we need it in the next step to create the default route for the LAN Routing Table. In our case it is *10.0.1.4*.

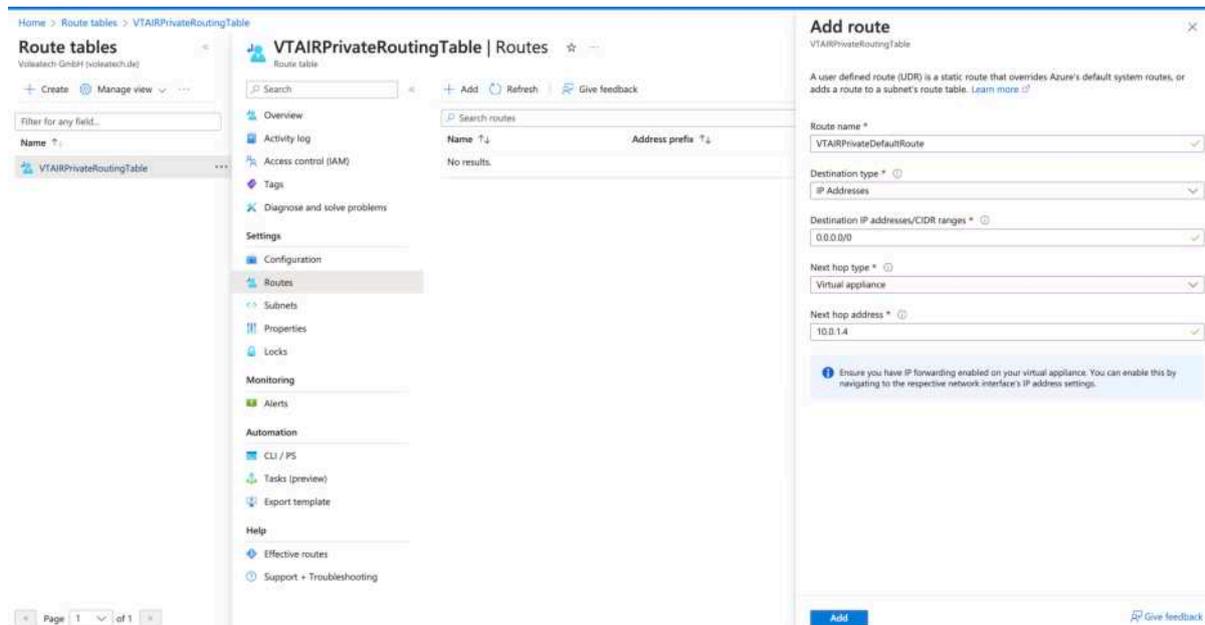


Default route pointing to VT AIR LAN interface

The next step needs to be completed in the *Route tables* settings. The Private Network Interface (LAN) needs to be the default gateway for the *VTAIRPrivateRoutingTable*

Navigate to *Routes* and click on *Add*.

Give the route a name *VTAIRPublicRoutingTableGateway*, the destination type is *IP Addresses*, the Destination is the network ip range *0.0.0.0/0* and the next hop type *Virtual appliance*. The next hop address is the IP Address of the LAN Interface of the virtual machine. In our case *10.0.1.4*.

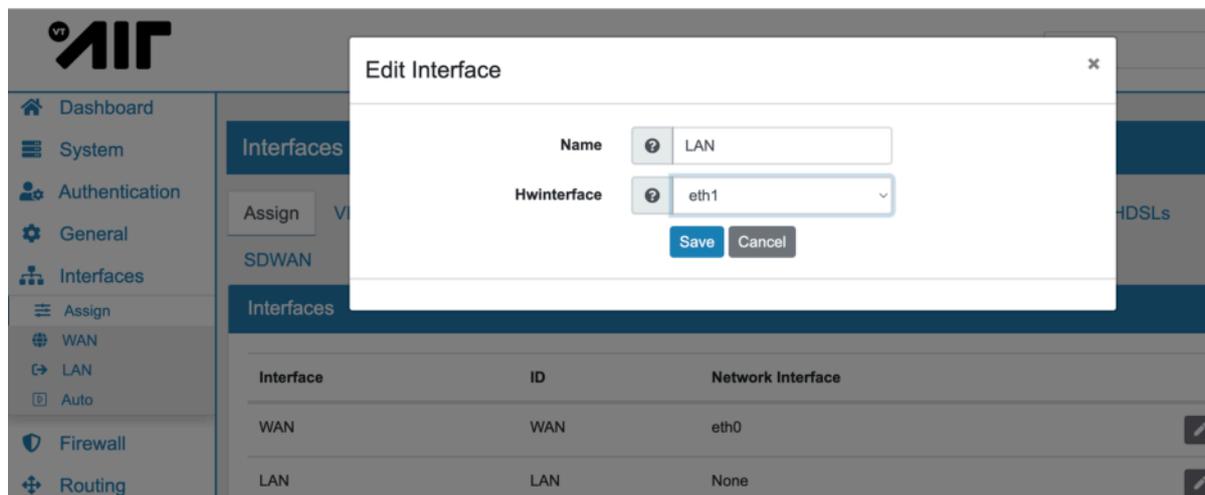


3.9.5 VT AIR configuration

We will now need to login to the VT AIR instance webgui to configure the LAN interface and additional settings.

Enable and set LAN Interface

In the webgui navigate to *Interfaces* -> *Assign*. Select the edit button next to the *LAN* interface and assign the new interface to it.



Switch to the *LAN* interface settings by going to *Interfaces* -> *LAN*. Enable the interface and set the IPv4 type to DHCP. Save the settings.

The screenshot shows the VT AIR web interface. The left sidebar contains a navigation menu with options: System, Authentication, General, Interfaces, Assign, WAN, LAN (selected), Auto, Firewall, Routing, Apps, Services, VPN, Tools, and Diagnostics. The main content area is titled 'Interfaces / LAN' and shows the configuration for the 'eth1' interface. The 'Enabled' toggle is turned on. The 'Name' is 'LAN', 'MAC Address' is 'MAC Address', 'MTU' is 'MTU', 'MSS' is 'MSS', and 'Speed and Duplex' is 'Default (Auto Negotiation)'. The 'IPv4 Settings' section shows 'IPv4 Type' set to 'DHCP' and 'Hostname' set to 'Hostname'.

This will enable the LAN interface and the IP *192.168.1.10* will be assigned.

The screenshot shows the VT AIR Dashboard. The 'System' panel displays the following information:

Name	vtair.localhost
System	VT AIR Azure
Serial Number	0000-0011-4504-4257-3230-1311-97
Device ID	6b141f575211d38eabfb134135c66e6e
Licence	Valid
Updates until	Lifetime
Remote Access until	No Remote Access

The 'Clock' panel shows the date and time: Thu Nov 02 2023 16:37:05. The 'Interfaces' panel shows the status of the network interfaces:

Interface	Status	Speed/Duplex	IP Address
WAN	↑	N/A	10.0.0.4
LAN	↑	50000MB (full-duplex)	10.0.1.4
AppBridge	↑	N/A	172.30.0.1

Create DNAT Rules and VPN Configuration

You can now create all the different setting you need for your setup. To make instances behind VT AIR available to the elastic IP, configure a DNAT rule.

You can also configure the different VPN options.

3.9.6 Azure VMs

Connect Azure VMs to the private subnet so they are in the LAN network of the VT AIR. We have created videos to show the entire configurations.

Add to the Private Network Subnet

If you have already running instances, you need to create a new Network Interface and change the existing network interface on the VM.

When you create a new VM, you can select the Virtual Network and private subnet in the network settings when you create it.

[Home](#) >

Create a virtual machine

Basics Disks **Networking** Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ [Create new](#)

Subnet * ⓘ [Manage subnet configuration](#)

Public IP ⓘ [Create new](#)

NIC network security group ⓘ None Basic Advanced

Public inbound ports * ⓘ None Allow selected ports

Select inbound ports *

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Delete NIC when VM is deleted ⓘ

[Review + create](#) [< Previous](#) [Next : Management >](#)

Set Private Network Security Group

Make sure to select an appropriate Network Security Group so the VM can be accessed by the VT AIR.

3.10 IAF 240

See the docs at [IAF 240](#) .

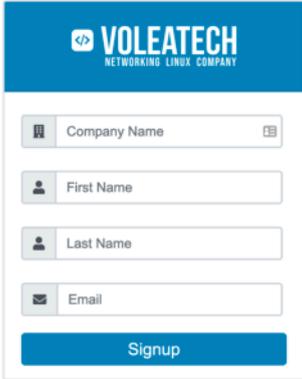
4.1 First Steps

The Voleatech Portal is a (remote) management interface to manage and monitor your companies TBF devices. It gives you access to backups, licensing information, remote control capabilities and more.

To access the portal go to portal.voleatech.de.

4.1.1 Sign-Up Process

To gain access to the portal you first need to register your company account, by entering your company name and an administrator's name.



The image shows a sign-up form for Voleatech. At the top is the Voleatech logo with the tagline 'NETWORKING LINUX COMPANY'. Below the logo are four input fields: 'Company Name', 'First Name', 'Last Name', and 'Email'. Each field has a small icon to its left (a building for Company Name, a person for First Name, a person for Last Name, and an envelope for Email). At the bottom of the form is a blue 'Signup' button.

After registering and confirming your account you can log in to your new account.

4.1.2 Customize your Company Profile

Go to **Company Profile** and enter your company details. Here you can also upload a company logo and customize the color scheme.

VOLEATECH
NETWORKING LINUX COMPANY

Dashboard
Users
Services
Support
Devices
Company Profile
Downloads
Logs

Company Profile

Edit Company Profile

Customer Name:

Custom Logo: No file selected.

Color:

© Voleatech 2017 - 2020

4.1.3 Login

Your User login is your **email address** and the password assigned to the user.

4.2 User Management

Go to **Users** to create, edit and delete users and user groups. Each user can be assigned an email address (username), a language, a password, a role (*User* or *Admin*) and each user can be activated/deactivated. You can also export users and groups as an Excel spreadsheet.

VOLEATECH
NETWORKING LINUX COMPANY

Dashboard
Users
Users
Groups
Services
Support
Devices
Company Profile
Downloads
Logs

Create User

Firstname:

Lastname:

Email Address:

Language:

Password:

Password confirmation:

Role:

Secondary roles:

Active:

© Voleatech 2017 - 2020

Users are added to groups based on their username/email address.

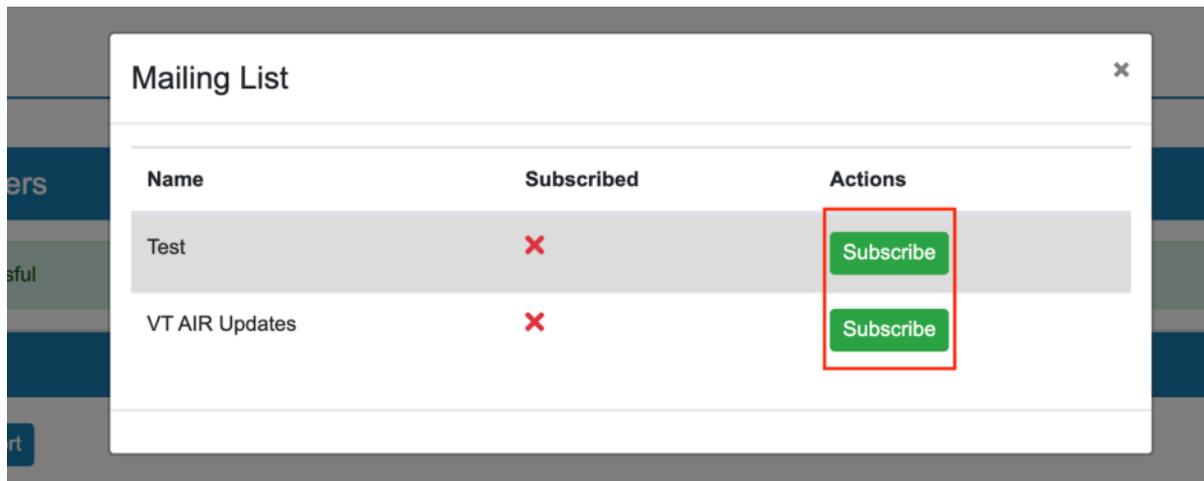
For individual users to be able to manage the devices connected to your Portal you need to assign them the **Secondary Role** *Device Control*. This is independent of being an *Admin* or standard *User*.

4.2.1 Mailinglists

You can subscribe and unsubscribe users to mailinglists with the mail symbol in the user management page.



A new window will open with the available Mailinglists and the options to subscribe/unsubscribe, as well as the status if you are already signed up.



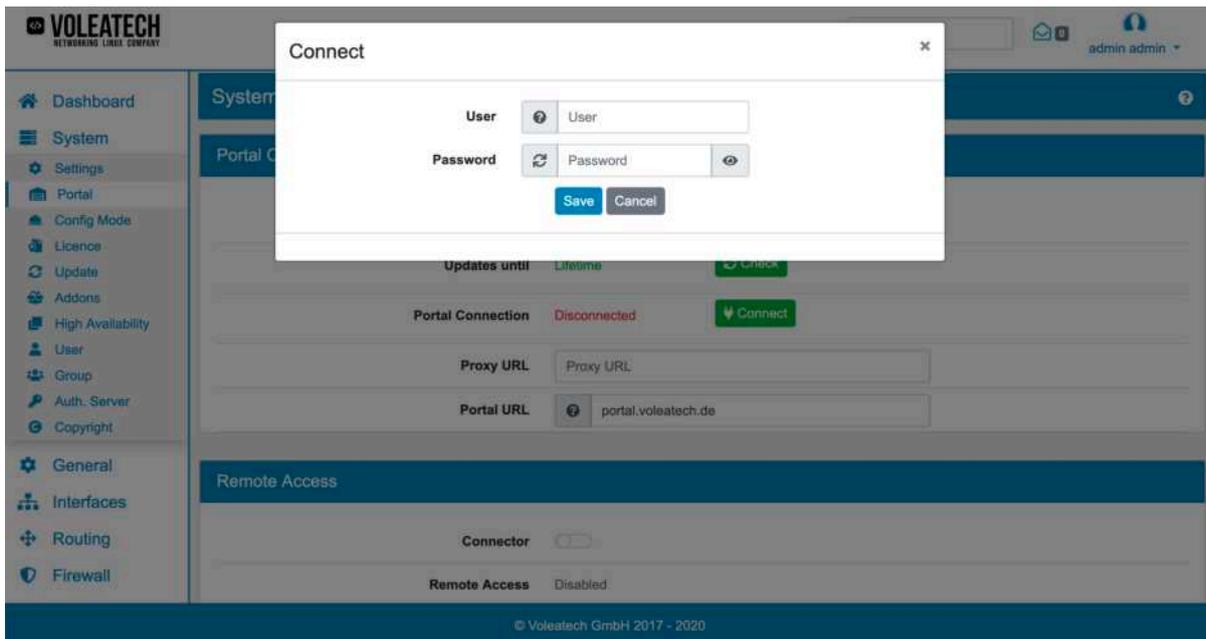
Please contact Voleatech if you want to be added to a Mailinglist without signing up in the Portal.

4.3 Device Management

You can manage, edit and remote control your devices under **Devices**. Your user needs to have the specific rights to do so though. Refer to [User Management](#) for more information.

4.3.1 Register Devices

On your * TBF device** go to **System** → **Portal** and click **Connect** next to **Portal Connection**.



Enter your Portal credentials (must be an admin account) and click **Save**. Should the Portal be reachable through a proxy you can enter its URL under **Proxy URL**.

If you want to allow **Remote Access** on this device from the Portal you need to activate it here.

After successfully connecting to the Portal you can manage your backups through this page and through the Portal too.

Note: After connecting your device to the Portal you cannot delete it from the Portal even if you disconnect your device. By disconnecting your device you will lose the remote functionalities though. Please contact us if you need the device to be removed from your account through the Portal Support.

4.3.2 Manage Devices

In your Portal you should now see a new device under **Devices**. Depending on your settings you can see basic information like the serial number, the device model and how long you'll receive updates for this device.

You can also give it a human readable Note so that you know which specific device you're looking at. This is highly recommended for setups with more than one device.

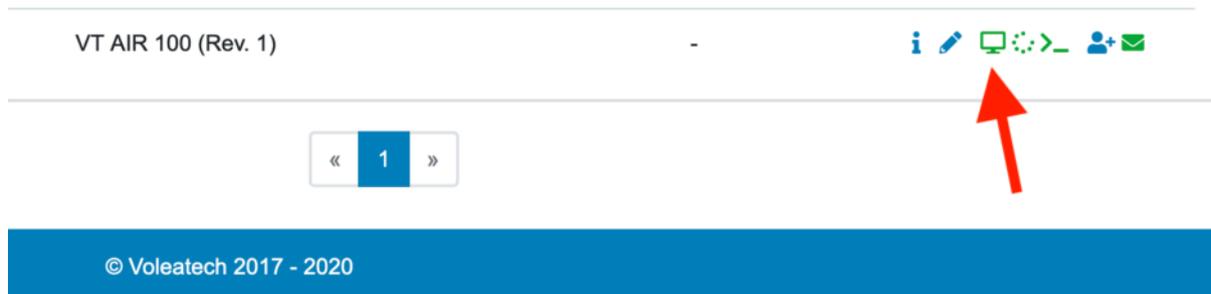
If you chose to activate **Remote Access** you can access the device's web GUI, the remote console and you can also remote update the device's software.

For further details see [Remote Access](#).

4.4 Remote Access

In your Portal under **Devices** you can see the remote access options for your devices. Please note that remote access must be enabled on your device for this to work. See *Device Management* for further details.

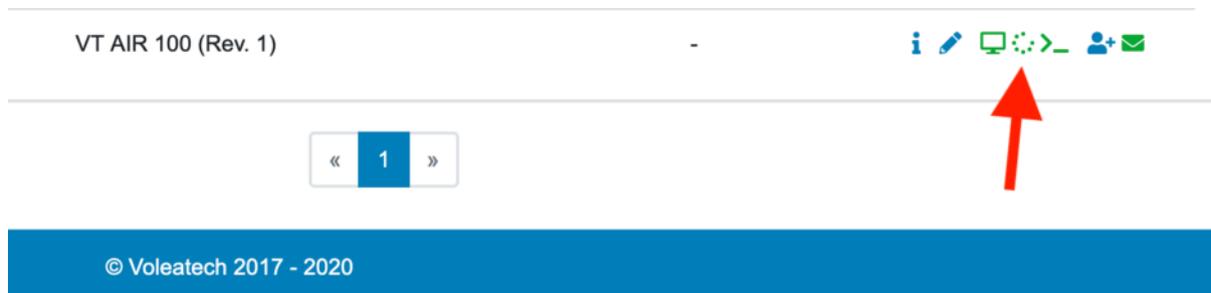
4.4.1 Remotely access the Web GUI



Click the green monitor symbol to remotely access the web GUI of your device. You don't need to make any changes to your firewall settings to be able to access the web GUI this way.

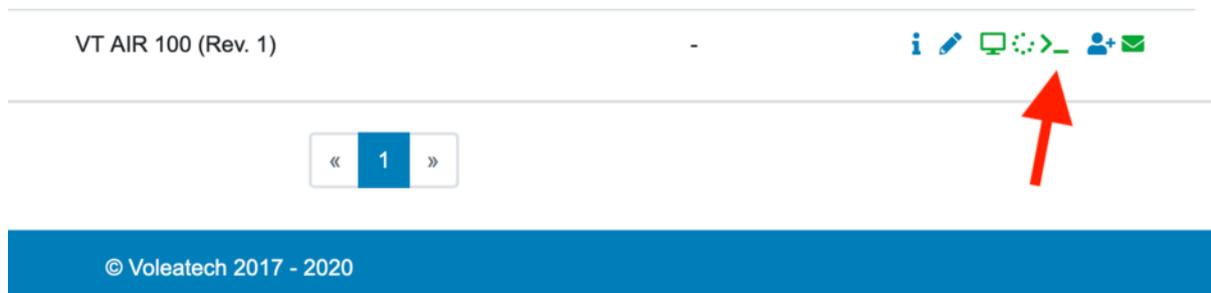
4.4.2 Remote Updates

To perform a remote update of your TBF's software you can click the little green circle symbol. Please note that this symbol is shown independently of the availability of an update.



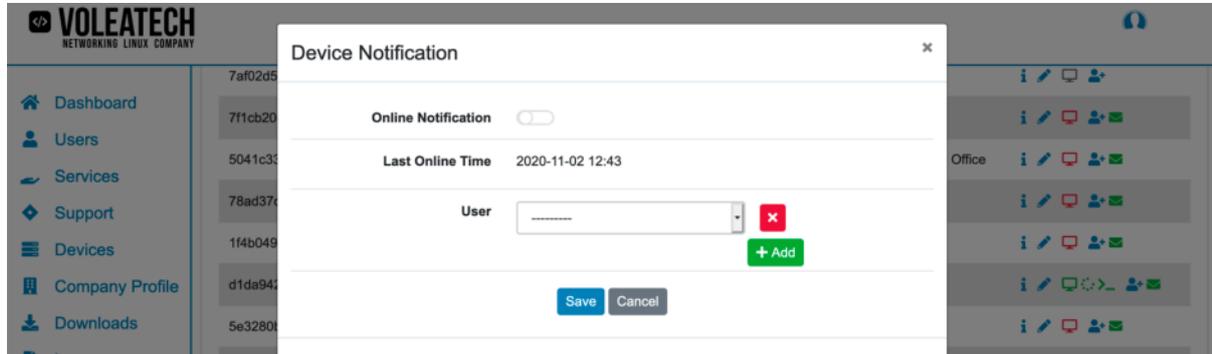
4.4.3 Remote Console

By clicking the Remote Console button you'll be shown a console. After logging in with your credentials you can use it just like on the device itself.



4.4.4 Email Notifications

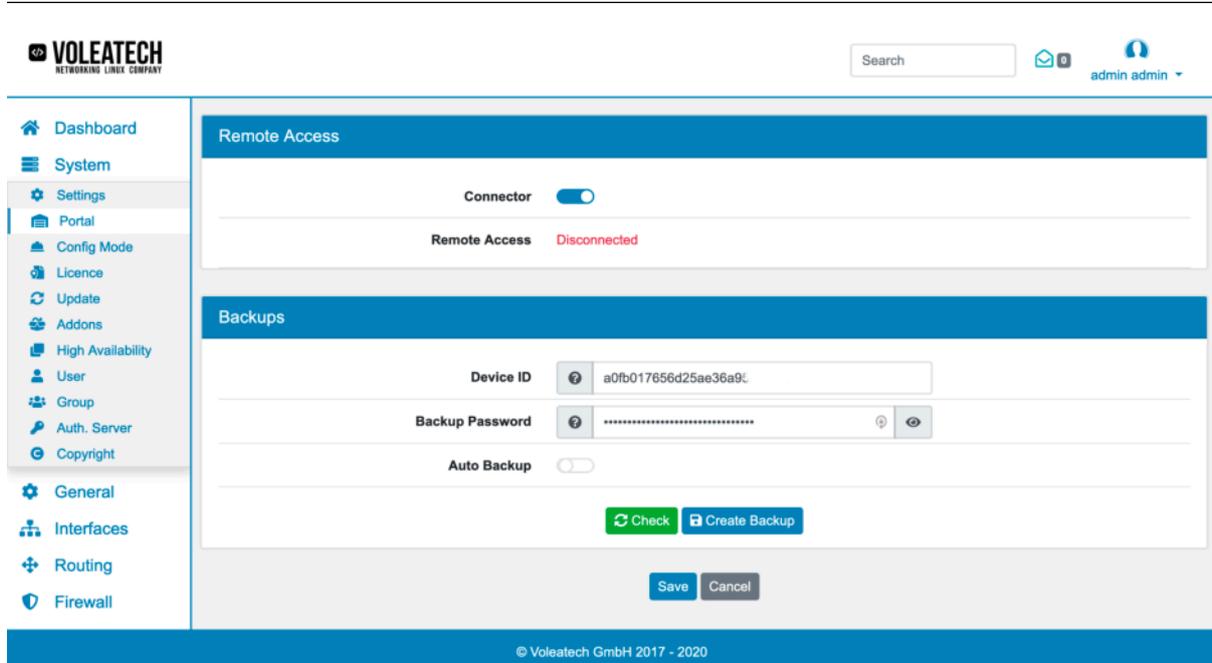
Click the green envelope symbol to configure Email Notifications for your device. Enable them with **Online Notifications** and select a user that will receive the emails. Notifications are sent when your device is no longer connected to the portal or is connected again. There is a grace period of up to 5 minutes so notifications are not send constantly.



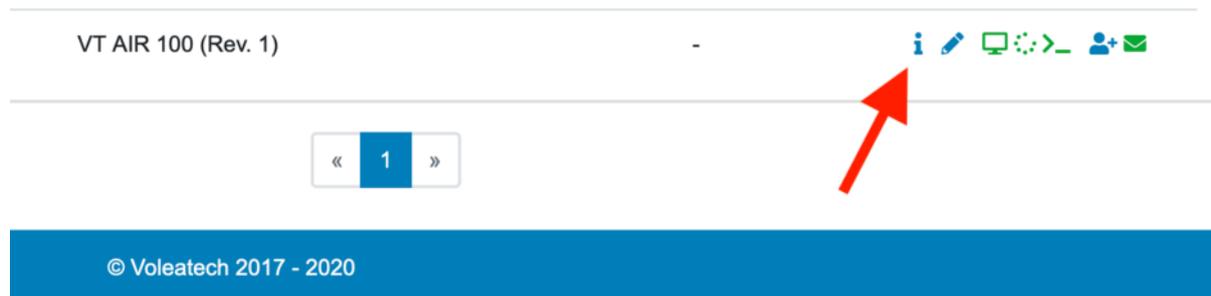
4.4.5 Device Backups

On your TBF device you can enable backups that are automatically synced with the Portal. You can choose between manual backups and automatic backups. You can also check for existing backups. Backups are always encrypted.

Note: This feature is only available with an active connection to the Portal. If your device is not connected/registered with the Portal you cannot use the backup feature.



In your Portal you can find the backups under the little info symbol. Here you can download them individually.



You can also directly restore a backup on a different device if you enter the device ID of your device to get the backups. Both devices need to be registered under your account.

4.5 Support

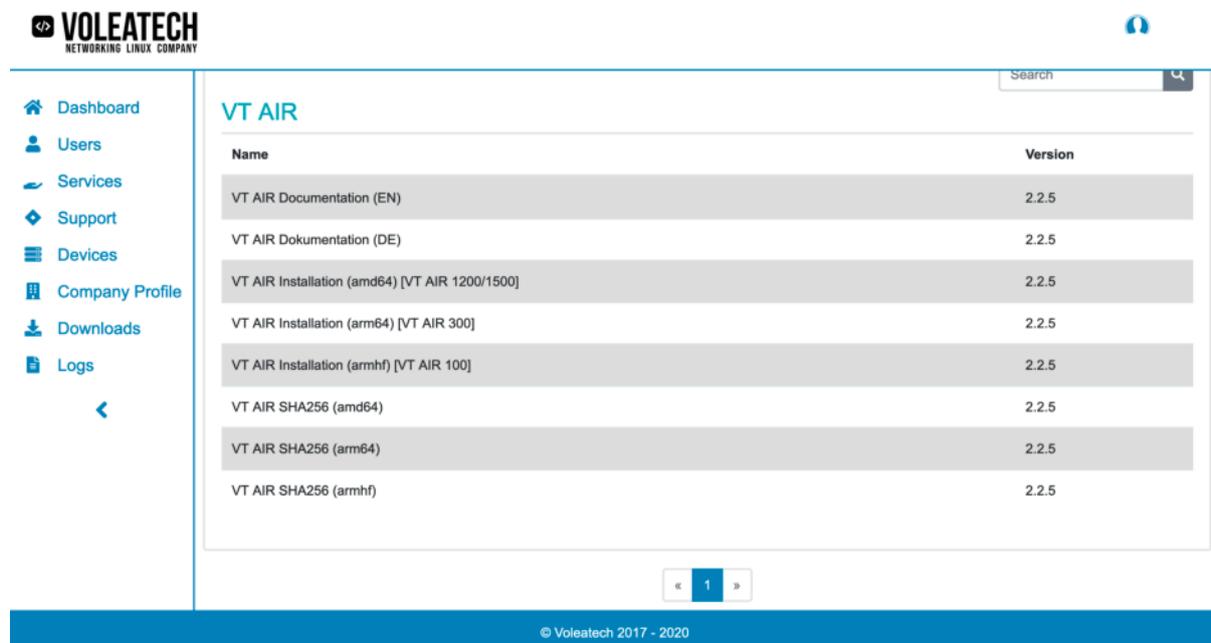
Via the **Support** page of the Portal you can either report bugs in the TBF software or request paid support for specific problems you're having.

To open a new ticket click **Create** and enter a title and a description of the problem. Under the **Closed** section you can find your old support requests that have already been resolved.

4.6 Downloads

Under **Downloads** you'll find various downloadable contents including installers for your TBF software.

If you ever need to reinstall your TBF's operating system download the installer file from this page. Pay special attention to your system's architecture or model name respectively. With the checksum files that are available on the same page you can verify that the downloaded file matches with the file on the server.



The TBF CLI Tool gives you the ability to configure your TBF device via the console instead of the web GUI.

To access the tool open a Console connection via SSH or serial connection and type *vtair-cli*. Then type *help* to see all the configuration possibilities.


```

totpdevice
upnpnat
user
virtualip
vrrpstate
wireguard
wol
((vtair)# interfaces
((vtair-interfaces)# help
Commands

base    Go back to base
down    Go down one command
help    Show help for current command.
login   Login to remote VT AIR
quit    Quit

assign
bond
bridge
hwiinterface
interface
macvlan
ppp
pppoe
qinq
shdsl
tunnel
vdsl
vlan
((vtair-interfaces)# assign
((vtair-interfaces-assign)# help
Commands

base    Go back to base
down    Go down one command
help    Show help for current command.
login   Login to remote VT AIR
quit    Quit

list
create
update
partial_update
((vtair-interfaces-assign)# list

1. id          | 2. name          | 3. internal_id  | 4. interface
3              | WAN              | WAN             | eth0
4              | LAN              | LAN             | eth1
7              | INT1             | INT1            | gretap1

((vtair-interfaces-assign)# █

```

The CLI is organized by category, for example firewall or dns. You can always enter a category by writing the name and pressing *ENTER*. To go down one level enter *down*, to go back to the start enter *base* all followed by an *ENTER*.

```
(vtair)# dns
(vtair-dns)# ?
  Commands

  base      Go back to base
  down      Go down one command
  enter     Execute the current command
  help      Show help for current command.
  login     Login to remote VT AIR
  quit      Quit

  activate
  read
  update
  partial_update
(vtair-dns)# █
```

Entering a ? + *ENTER* will show the current options in the stage of the CLI.

activate is the same as *Apply Change* in the GUI. The difference between *update* and *partian update* is that in partial update not all fields need to be entered. On the other hand some values can not be deleted in *partial update* mode.

```

(vtair-dns)# read
enabled          | True
port             | 53
local_zone_type  | transparent
dnssec           | True
add_ptr          | True
dns_forwarding   | False
interfaces_in    | All
interfaces_out   | All
dnsforwardserver |
  id             | 3
  uuid           | 33180809-bdc7-43f4-bcb0-474734c9a392
  enabled        | True
  ipaddress      | 192.168.10.1
dhcp_registration | False
static_dhcp      | False
ssl_tls_enabled  | False
ssl_tls_port     | 853
ssl_tls_certificate | None
ssl_tls_upstream | False

(vtair-dns)# >

```

`read` will read out the value in this example the DNS settings.

```

(vtair-dns)# partial_update
(vtair-dns-partial_update)# ?
  Commands

base      Go back to base
down      Go down one command
enter     Execute the current command
help      Show help for current command.
login     Login to remote VT AIR
quit      Quit

add_ptr (PTR Records for Host Overrides get added automatically)
dhcp_registration (Enabling this option will register the DHCP leases in the DNS server)
dns_forwarding (DNS Forwarding Mode)
dnsforwardserver
dnssec (Domain Name System Security Extensions)
enabled (Enabled)
interfaces_in
interfaces_out
local_zone_type (System Domain Local Zone Type)
port (DNS Port. By default 53)
ssl_tls_certificate (The certificate for the tls service)
ssl_tls_enabled (If enabled, the server provides TLS service on its TCP sockets. The clients have to use tls-upstream: yes.)
ssl_tls_port (The port number on which to provide TCP TLS service, default 853, only interfaces configured with that port number get the TLS service)
ssl_tls_upstream (Allow DNS server list to be overridden by DHCP/PPP on WAN)
static_dhcp (Enabling this option will register the DHCP host reservations in the DNS server)

```

In this example we will enable the DNS Server by going to `partial_update`. The `?` help will show all available fields with their explanation.

```
(vtair-dns-partial_update)# enabled False
Set enabled to False
(vtair-dns-partial_update)# ?
Commands:

base      Go back to base
down     Go down one command
enter    Execute the current command
help     Show help for current command.
login    Login to remote VT AIR
quit     Quit

add_ptr (PTR Records for Host Overrides get added automatically)
dhcp_registration (Enabling this option will register the DHCP leases in the DNS server)
dns_forwarding (DNS Forwarding Mode)
dnsforwardserver
dnssec (Domain Name System Security Extensions)
enabled (False) (Enabled)
interfaces_in
interfaces_out
local_zone_type (System Domain Local Zone Type)
port (DNS Port. By default 53)
ssl_tls_certificate (The certificate for the tls service)
ssl_tls_enabled (If enabled, the server provides TLS service on its TCP sockets. The clients have to use tls-upstream: yes.)
ssl_tls_port (The port number on which to provide TCP TLS service, default 853, only interfaces configured with that port number get the TLS service)
ssl_tls_upstream (Allow DNS server list to be overridden by DHCP/PPP on WAN)
static_dhcp (Enabling this option will register the DHCP host reservations in the DNS server)
(vtair-dns-partial_update)#
```

We can enable the DNS Server by entering *enabled True* and pressing enter. To submit the new value we have to also press *enter* again.

We can now check if the setting was applied with the *read* command.

CONSOLE ACCESS

You can get to the console menu with the serial or VGA screen of your appliance. The root account will also see the console as the entry menu via SSH.

Default login data for SSH or the console are user **root** and password **vtair**.

6.1 SSH

After enabling SSH as described in [Settings](#) you can log in. When using the root user, you can see the console menu.

```
VT AIR
Model: VT AIR 100 - Serial: 0000000000000000 - Device ID: a0fb017656d25ae36a95f4e5b9d7abf8

WAN: eth0 (WAN)
speed = 1000MB, up = yes
192.168.10.113/24
1.2.3.4/32
fe80::250:43ff:fe02:201/64
LAN: eth1 (LAN)
speed = 1000MB, up = yes
192.168.1.1/24
fe80::7493:eaff:fe07:e7ba/64
AppBridge: brapp (APPBRIDGE)
speed = 0MB, up = yes
172.30.0.1/24
fe80::5018:f3ff:fe8e:1e7/64
INT1: gretap1 (INT1)
speed = 0MB, up = yes
192.168.20.1/24
fe80::6cc5:28ff:fefa:4ddf/64
OVPN_Site2Site: ovpnsl (OVPNS1)
WIREGUARD_WireGuard: wg1 (WG1)
speed = 0MB, up = yes
1.2.3.4/24

Commands

allowallwan Allow all Firewall Rule for WAN
assignlan Assign LAN Interface
assignwan Assign WAN Interface
check-service Check service
default-gateway Assign Default Gateway
factory-defaults Reset to factory defaults
interfaceip Assign IPs or DHCP to an Interface
interfaces-all Show all interfaces in the system
licence Add Licence
reboot Reboot the system
reset-admin Reset the admin password to default
restart-webgui Restart the webgui
route-check Force a Route Service Check
shell Open up a shell
showservices Show all active services
shutdown Shutdown the system
ssh Enable or Disable SSH
unlock-user Unlock a blocked user
update Update from vtair terminal
vtair-cli Open up the cli

(vtair)#
```

Not only can you perform basic tasks like rebooting or shutting down the system but you can also display the configuration of all the interfaces in your system.

Via the *shell* command you can access the same shell that you can use from the web GUI. Leave the shell by typing *exit*.

Press *enter* or *ctrl+d* to clear the console window.

```

Commands

allowallwan      Allow all Firewall Rule for WAN
assignlan        Assign LAN Interface
assignwan        Assign WAN Interface
check-service    Check service
default-gateway  Assign Default Gateway
factory-defaults Reset to factory defaults
interfaceip      Assign IPs or DHCP to an Interface
interfaces-all   Show all interfaces in the system
licence          Add Licence
reboot           Reboot the system
reset-admin      Reset the admin password to default
restart-webgui   Restart the webgui
route-check      Force a Route Service Check
shell            Open up a shell
showservices     Show all active services
shutdown        Shutdown the system
ssh              Enable or Disable SSH
unlock-user      Unlock a blocked user
update           Update from vtair terminal
vtair-cli        Open up the cli

(vtair)# showservices

Name           | Service           | Enabled | Status
-----
Apps           | docker            | True    | active
Conntrackd    | conntrackd        | False   | inactive
DHCP Client    | dhcpcd            | True    | active
DHCPR          | radvd             | False   | failed
DNS            | unbound           | True    | active
DynamicRouting | frr                | True    | active
IPSec          | strongswan        | True    | active
KEA DHCP Control Agent | kea-ctrl-agent | True    | active
KEA DHCP v4    | kea-dhcp4-server  | True    | active
KEA DHCP v6    | kea-dhcp6-server  | False   | failed
MSTP           | mstpd             | True    | active
NTP            | ntp                | True    | active
Nginx          | nginx             | True    | active
OpenVPN Server 1 | openvpn@server1  | False   | inactive
PortalConnector | vtair-portal-connector | False | inactive
Postfix        | postfix           | False   | inactive
Redis          | redis             | True    | active
SNMP           | snmpd             | False   | inactive
SSH            | ssh               | True    | active
Syslog         | rsyslog           | True    | active
UPnP NAT       | miniupnpd         | False   | inactive
VirtualIP      | keepalived        | True    | active
Watchdog       | watchdog          | True    | active

(vtair)# █

```

6.2 Serial

Some TBF models also contain the possibility to use a USB cable to establish a serial connection. We recommend one of the following programs to establish a serial connection.

OS	Program
Windows	Putty
MacOSX	Screen, Serial
Linux	Screen

Follow the steps in [USB Console](#) to find the serial port that your connection will run on. Then enter the information in your serial program and select a baud rate of 115200.

When using Screen type “`screen /dev/ttyNAME 115200`” where NAME is the name of your USB connection (e.g. USB0) and press enter twice.

You’ll see the same menu as if you were connected via SSH (see above).

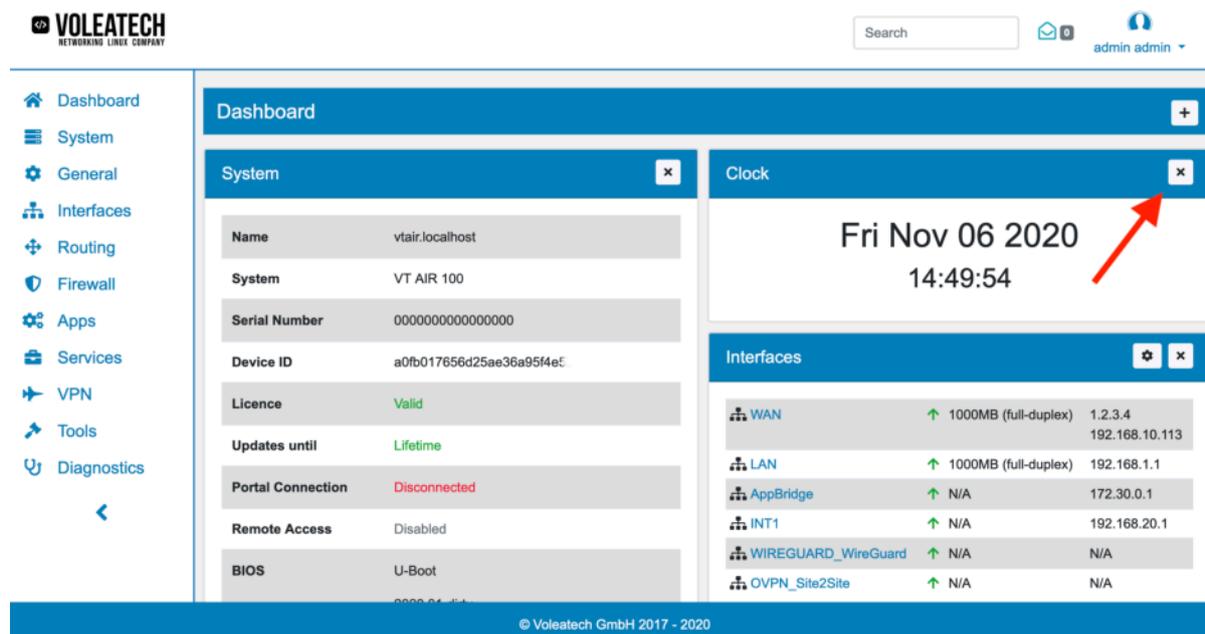
DASHBOARD

The Dashboard is the first thing you see when you login to your TBF. You can always go back to the Dashboard by clicking on the Dashboard Menu entry or on the logo in the top left corner.

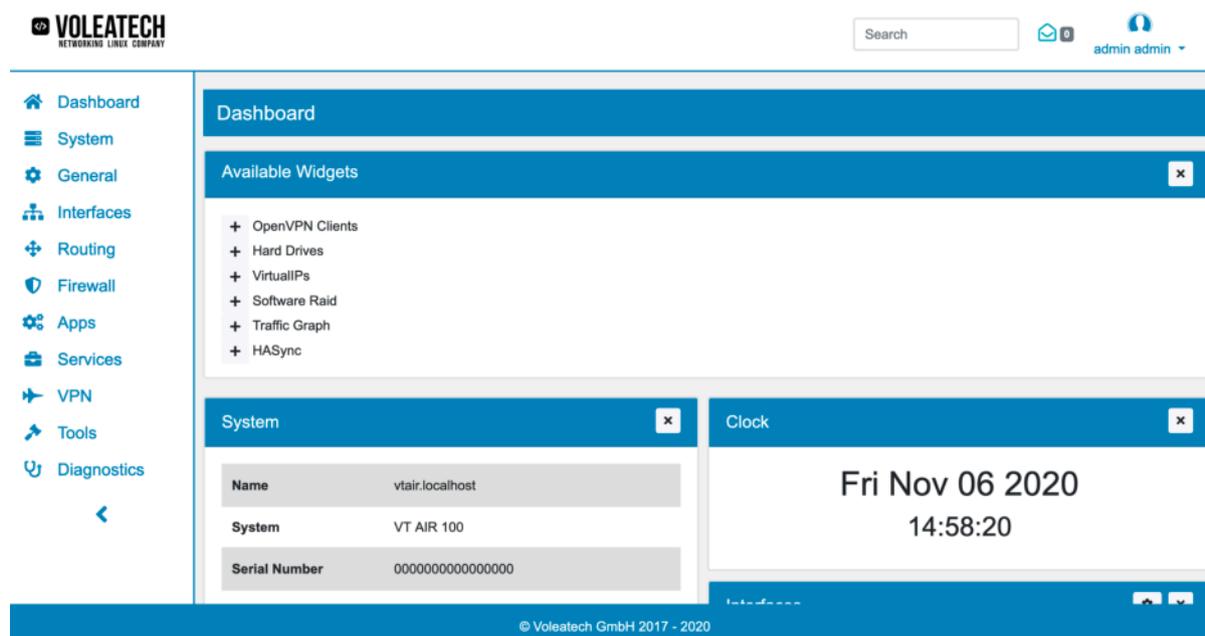
The screenshot shows the Voleatech Dashboard interface. At the top left is the Voleatech logo. To the right is a search bar and a user profile for 'admin admin'. A left sidebar contains navigation icons for Dashboard, System, General, Interfaces, Routing, Firewall, Apps, Services, VPN, Tools, and Diagnostics. The main content area is divided into three widgets: 'System' (with fields for Name, System, Serial Number, Device ID, Licence, Updates until, Portal Connection, Remote Access, and BIOS), 'Clock' (displaying 'Fri Nov 06 2020 14:49:54'), and 'Interfaces' (listing WAN, LAN, AppBridge, INT1, WIREGUARD_WireGuard, and OVPN_Site2Site with their respective speeds and IP addresses). A footer at the bottom reads '© Voleatech GmbH 2017 - 2020'.

The Dashboard has 2 Columns by default and you can add widgets to each column individually. You can move them to a different place as well. The Columns can be changed in the [Settings](#).

You can remove widgets by clicking the X on each widgets upper right corner.



You can add widgets back or new ones to the dashboard by first clicking on the + in the dashboard banner. It will open a list of available widgets. Simply click on the + next to a widget to add it.



Some widgets offer the ability to change their settings. If they do, a wheel symbol will appear next to the X in the upper right corner of the widget.

The screenshot shows the Voleatech dashboard with a left sidebar menu and a main content area. The main content area is divided into two sections: System Information and Services.

System Information:

- Version: 2.2.5-2 (Updates available)
- Uptime: 1 day, 1:59:53
- Datetime: Nov. 6, 2020, 3:02 p.m.
- DNS server(s): 127.0.0.1 ::1
- CPU: ARMv7 Processor rev 1 (v7l), 2 Cores / 2 Threads, 1.6000 GHz / 1.6000 GHz
- Load average: 0.55, 0.60, 0.56
- CPU usage: 8%
- Memory usage: 75.1% of 1.96 GB
- SWAP usage: 10.6% of 976.0 MB
- Disk usage: / 35.5% of 6.16 GB

Services Table:

Name	Service	Status	Actions
✓ Apps	docker	active	🔄 🔄 🔄
✗ Conntrackd	conntrackd	inactive	▶
✓ DHCP Client	dhcpcd	active	🔄 🔄 🔄
✗ DHCPRRA	radvd	inactive	▶
✓ DNS	unbound	active	🔄 🔄 🔄
✓ DynamicRouting	frr	active	🔄 🔄 🔄
✓ IPSec	strongswan	active	🔄 🔄 🔄
✓ KEA DHCP Control Agent	kea-ctrl-agent	active	🔄 🔄 🔄
✓ KEA DHCP v4	kea-dhcp4-server	active	🔄 🔄 🔄
✗ KEA DHCP v6	kea-dhcp6-server	failed	▶
✓ MSTP	mstpd	active	🔄 🔄 🔄
✓ NTP	ntp	active	🔄 🔄 🔄
✓ Nginx	nginx	active	🔄 🔄 🔄
✗ OpenVPN Server 1	openvpn@server1	inactive	▶

A red arrow points to the settings icon (gear) in the Services widget header.

Widgets are updated automatically and do not need a browser refresh or reload.

7.1 States Widget

This widget shows the current number of states compared to the maximum configured number of stats. It also lists the number of offloaded states.

The States widget displays the following information:

- Number of States:** 8 / 100000
- Number of States Offloaded:** 0 / 8

7.2 Security Widget

This widget shows the status of all security services. The **Firewall Stats** show stats of rules by category, e.g. accept, drop, etc. It also lists the number of rules, packets and bytes. The **Intrusion Detection Stats** show stats for each interface the number of packets, drops, bypasses and invalid checksums.

Security ✕

Status	Name	Service
✕	App Control / Intrusion Detection	active
✓	Firewall	active
✕	Virus Scanner	active
✕	Web Filter	active

Firewall Stats

Action	Number of Rules	Packets	Bytes
accept	14	0	0
drop	13	277	64499

Intrusion Detection Stats

Name	Packets	Drop	Bypassed	Invalid Checksums
NFQ#0	0	0	0	0
NFQ#1	0	0	0	0

SYSTEM SETTINGS

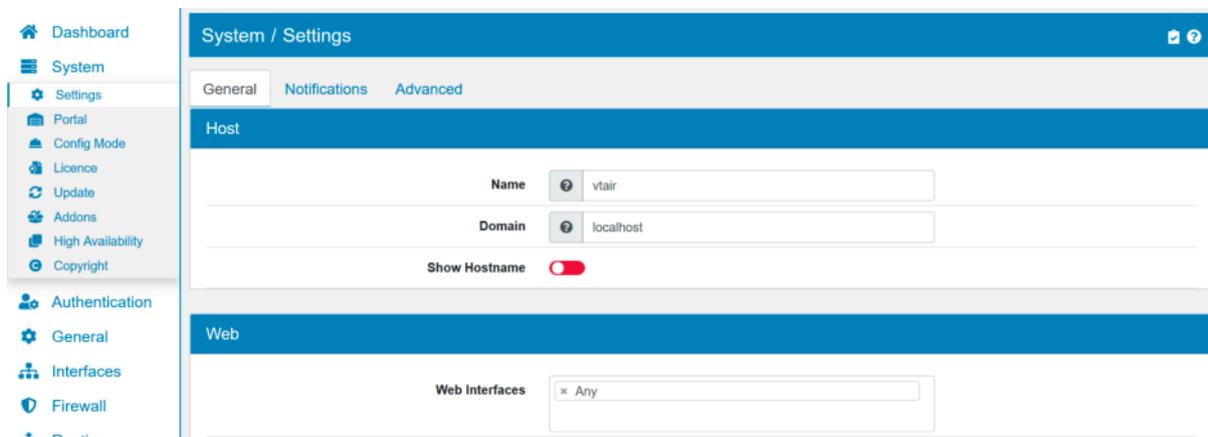
8.1 Global Settings

8.1.1 Settings

You can find the General Settings at **System** → **Settings**. You can configure

- Hostname and Domain
- Webserver Settings
- Global Language and Timzone
- SSH Settings
- ...

It is a good starting point when you want to configure your TBF to look through these options and check if they meet your requirements. The defaults are reasonable and will work right away.



You can also activate **Config Mode** under **System** → **Config Mode**. By doing this none of the changes you're making are applied so you can configure everything and then apply everything at once. This is especially useful for changes you're making during normal operation when your router is supposed to have minimal downtime.

8.1.2 Host

Name is the hostname of your TBF without the domain part.

Domain is the domain part of your host.

Show Hostname will show the full hostname in the top bar and login screen in the webgui, so you can identify the device more easily.

8.1.3 Web

Web Interfaces lets you configure one or more interfaces and ipaddresses for the Web Interface.

HTTP Forward auto redirects HTTP requests to the web interfaces to HTTPS (encrypted).

Web HTTPS Port is the HTTPS Port of the web interfaces.

Web Certificate is the certificate used to secure your HTTPS connection to the web interfaces.

The option **Auto Logout Time** is the time a user stays logged in when not using the webgui in seconds. The default value is 3600 seconds, which is 1 hour.

8.1.4 Localization

Timezone and Language settings for your TBF device.

8.1.5 SSH

You can enable **SSH** and choose to only allow SSH Keys. SSH Keys have to be added to each user to be able to login.

SSH Rate Limit sets the number of connections per IP that can access the TBF. **SSH Rate Limit Time** is the time (Seconds/Minutes) that the Rate Limit should apply to.

For example a rate limit of 5 per Minutes will restrict a single IP to a maximum of 5 connections per minute.

8.1.6 Firewall

Anti Lockout Rules Automatically creates Firewall Rules that prevent you from losing access to the web interface.

8.1.7 DNS

DNS Override allows the DHCP Server to override the DNS Servers.

DNS Localhost uses the internal DNS Server for your network (must be enabled under Services).

DNS Forward Servers are IP addresses of external DNS Servers that you want to use.

8.1.8 NAT & Firewall

NAT Reflection allows your clients to access DNAT forwarded IPs by their external address. Without NAT Reflection a DNAT forwarded WAN IP can not be accessed from inside the local network. *Split DNS* is usually a better solution to fix this problem by pointing the internal DNS entry to the local IP Address of the server.

Auto VRRP VIP Rules will supply automatic firewall rules for the following Services:

- VRRP VIP
- DHCP
- OSPF

They will be updated when you change any relevant settings in these Services. If you want to manage these firewall rules manually, you can deactivate the auto generation here.

8.1.9 Miscellaneous

Dashboard Columns How many columns on the main dashboard will be displayed. It can be 2, 3, 4 or 5. The default value is 2.

Prefer IPv4 over IPv6 When both IPv6 and IPv4 are available for a specific connection your TBF will default to IPv6 unless you enable this option in which case IPv4 will be used.

Enable Watchdog Enable the hardware watchdog which auto-detects severe malfunctions that cause the software to crash and reboots your TBF device.

OpenSSL Engine can be *Dynamic (Default)* or *AF ALG (Kernel Crypto API)*.

Console Password enables the password for the console. The admin password must be used to unlock it.

Disable API disables the REST API.

Log to RAM caches logfiles in the RAM and copies them to the SSD hourly. This saves write operations on your SSD prolonging its life span

Maximum log to RAM size (MB) is the maximum size of the log to ram disk. This will be deducted from the available RAM, so be careful not set this too high.

Logfile Analysis stores critical logfiles like firewall and intrusion protection long term for analysis in the Webgui. This comes at a performance and disk storage cost. Disable the setting if high performance is important.

Maximum Logfile Analysis Days for each logfile to store for analysis. More days requires more disk storage and for small systems it is necessary to keep the entries relatively low.

There is an automatic logfile cleaner in the background that will empty large logfiles if there is not enough space on the hard drive or ram disk. The mechanism ensures that the logfolder will not be full and therefore logfiles are not stored anymore.

8.1.10 Basic Configuration example

When first setting up your TBF device give it a **Hostname** that is easily recognizable in your network and makes clear what device this is. For example if you have multiple TBF devices in your network consider using their location as part of the hostname. This way you can easily identify which device is the right one in case you need physical access to it.

Change the **Domain** to your company's domain to complete your device's FQDN (Fully Qualified Domain Name).

Enable **HTTP Forward** to encrypt the traffic between your computer and your TBF device when accessing the web GUI. Changes to this are only effective after you press save at the bottom of the page and reload the browser tab.

Enter your **Timezone** and **Language** preference for your device.

If you want to access the *Console Access* remotely consider enabling SSH on your device.

If you want to make changes from the Voleatech *Portal*, consider enabling the Portal connections.

Keep the **Anti Lockout Rules** enabled. This creates automatic Firewall rules that prevent you from accidentally being locked out of your firewall due to a wrong Firewall rule.

Leave the **DNS Localhost** enabled unless you have a specific reason for it to not be enabled.

If your ISP supplies you with a Dual Stack (Lite) connection instead of a native IPv4 connection you can enable **Prefer to use IPv4 even if IPv6 is available**. This will route all traffic over IPv4 wherever possible instead of switching to IPv6 when available.

Click **Save** on the bottom of the page.

8.1.11 Updates

You can find the Update Settings at **System** → **Updates**.

Update Tab

On the Update Tab you can see if there are updates available. You can see the currently installed version of each package as well as the latest version. You can update each package individually or update all at once. The update process is possible from the browser and the update progress will be shown in the window.

You can also recheck for new updates as the update check only runs every 24 hours.

Update Settings

In the update Settings you can configure different options.

Auto Update to enable automatic updates. This will enable new options:

Weekday the auto updater should run. **Time** will be a random time between 2am and 5am and automatically be set by the system.

Update Email Notifications enables the possibility to get updates via email. The default email is *root@localhost.com* and can be changed once enabled.

Send Update Information Report is available when *Update Email Notifications* is enabled. If enabled emails for update information reports will be sent. The **Update Email Schedule** is weekly by default and can be changed as well.

Update Email Send all Updates is available when *Send Update Information Report* is enabled. If enabled all available updates are sent and if disabled only new updates compared to the last Email are sent.

Send Update Installation Report is available when *Update Email Notifications* is enabled. If enabled emails for update installation reports will be sent.

Enable Proxy to use a HTTP/HTTPS proxy for downloading the Updates.

Miscellaneous

Prefer to use IPv4 even if IPv6 is available can be enabled oder disabled. By default, if IPv6 is configured and a hostname resolves IPv6 and IPv4 addresses, IPv6 will be used. If this option is selected, IPv4 will be preferred over IPv6.

Strict Reverse Path Filter can be enabled oder disabled. Current recommended practice in RFC3704 is to enable strict mode to prevent IP spoofing from DDos attacks (default). If using asymmetric routing or other complicated routing, then disable this option to set it to loose mode.

Console Password enables the password for the console. The admin password must be used to unlock it.

Disable API disables the REST API.

Dashboard Columns determines how many columns the dashboard will have. Devault is 2.

Troubleshooting

If there are any issues after updates please drop to the console or shell and run the command **apt-get install -f**. It will show any problems of the update process as well as suggestions on how to fix them with further commands.

8.1.12 Notifications

You can find the Notification Settings at **System** → **Settings** → **Notifications**.

You can configure email notifications for the system, which will send you emails if there are errors. The notifications are disabled by default.

Please make sure to configure the available options to your needs

- Disable Notifications
- Email Server
- Email Port
- From and to Email
- Authentication

You can test the email with Send Test E-Mail.

System Messages

If the notifications are enabled, it's possible to enable system messages as well. System messages use the same email server settings as above.

Interface up/down will send a message when an interface comes up or goes down

Gateway up/down will send a message when a default gateway comes up or goes down

VirtualIP change will send a message when the VRRP state has been changed

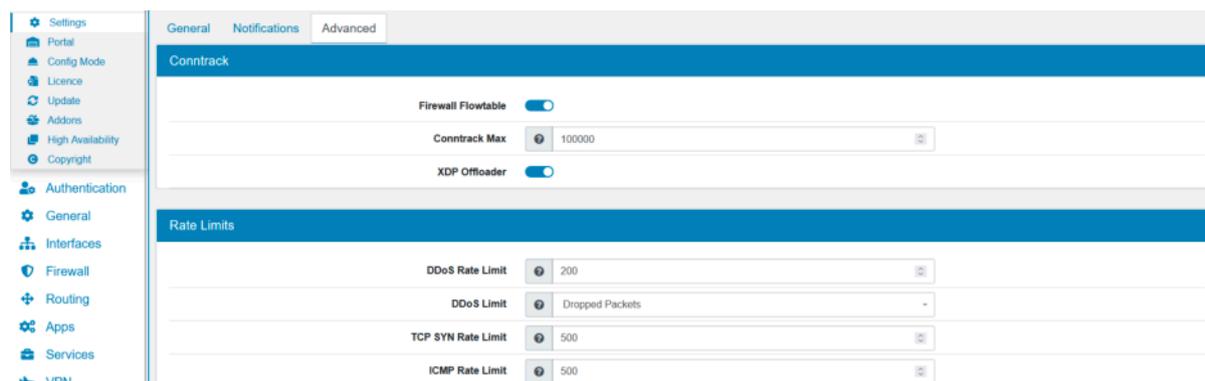
Disk Mail Root Notifications

A builtin service will check errors in the disk mail root directory. Every three hours notifications will be created and displayed in the TBF GUI.

Note: This will only show messages if you do not have the mail notification setting enabled. In that case all notifications are sent to the configured email.

8.1.13 Advanced Settings

You can find the Advanced Settings at **System** → **Settings** → **Advanced**.



XDP Offloader can be enabled here. But Flowtable needs to be enabled for XDP to work.

Rate Limits

DDoS Rate Limit is maximum number of connections per IP per minute before the IP is blacklisted for 60 seconds. Needs to be enabled on each interface to be effective. It's 1000 by default.

DDoS Limit can be either All or Dropped Packets. All will count also valid traffic against the limit, make sure to choose a high enough limit in case of legitimate traffic. The default value is Dropped Packets.

TCP SYN Rate Limit is 500 by default. A value of 0 means disabled. It specifically targets TCP SYN packets to protect against a SYN attack.

ICMP Rate Limit is 500 by default. A value of 0 means disabled. It specifically targets ICMP packets to protect against an ICMP attack.

Timeouts

The screenshot displays the Firewall configuration interface, specifically the 'Timeouts' section. The interface is divided into three main sections: TCP Timeouts, UDP Timeouts, and GRE Timeouts. Each section contains a list of settings with their current values and a help icon (question mark) and a refresh icon (circular arrow).

Setting	Value
TCP Timeout Close	10
TCP Timeout Close Wait	60
TCP Timeout Established	432000
TCP Timeout Fin Wait	120
TCP Timeout Last Ack	30
TCP Timeout Max Retrans	300
TCP Timeout Syn Recv	60
TCP Timeout Syn Sent	120
TCP Timeout Time Wait	120
TCP Timeout Unacknowledged	300
UDP Timeout	30
UDP Timeout Stream	120
GRE Timeout	30
GRE Timeout Stream	180

You can configure Firewall timeouts for

- ICMP
- ICMPv6
- TCP
- UDP
- GRE

as well as the conntrack states table size.

Firewall Helper

The screenshot displays the Firewall configuration interface, specifically the 'Firewall Helper' section. The interface shows four settings, each with a toggle switch:

Setting	Value
Firewall Helper SIP	Off
Firewall Helper FTP	Off
Firewall Helper TFTP	Off
Firewall Helper SNMP	Off

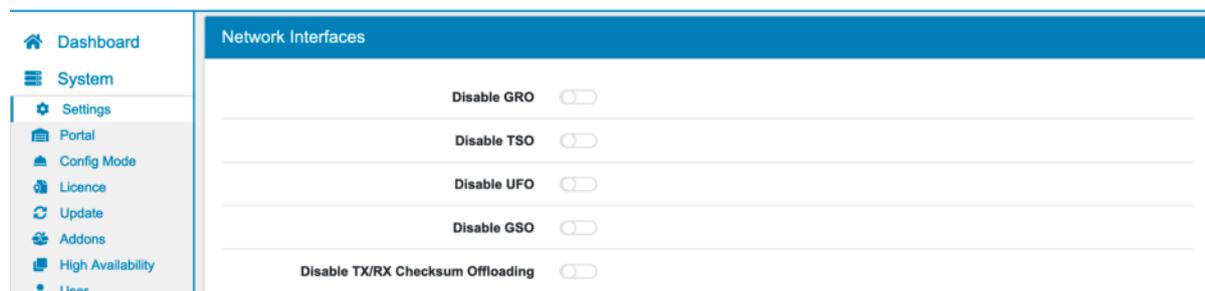
There are 4 firewall helper that help with protocols that need to open up additional random ports

- SIP
- FTP

- TFTP
- SNMP

You can enable each helper individually and the firewall will try to track any additional port that a connection of one of those protocols opens without you adding a new firewall rule for it.

Network Interfaces

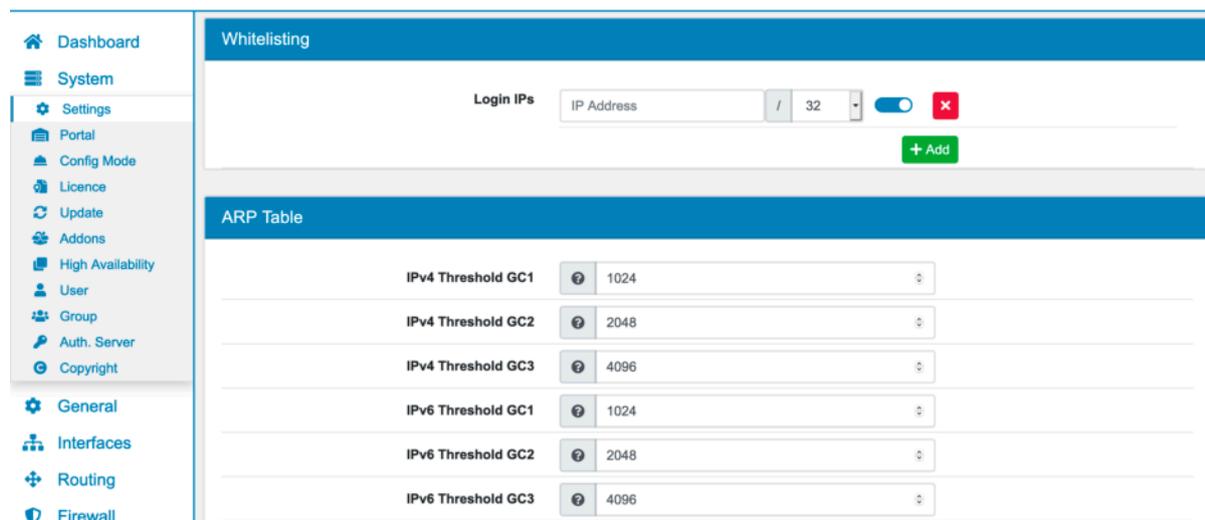


You can disable hardware and software offload features here.

- GRO (Generic Receive Offload)
- GSO (Generic Segmentation Offload)
- TSO (TCP Segmentation Offload)
- UFO (UDP Fragmentation Offload)
- TX/RX Checksum Offload

A restart is not required to disable or enable any of the settings.

Allowlisting



You can add multiple IPv4 or IPv6 addresses or networks which will not be blocked at the TBF login, when the username or password are incorrect. Otherwise the login is secured with a blocking function after 3 unsuccessful logins.

ARP Table

Here you can define the ARP Table cache threshold for IPv4 and IPv6, as well as for GC1, GC2 and GC3. The default values are: 1024 for GC1, 2048 for GC2 and 4096 for GC3. When you have a large amount of clients you might need to increase the values.

Miscellaneous

The screenshot shows the 'Miscellaneous' settings page. On the left is a navigation menu with options: High Availability, Copyright, Authentication, General, Interfaces, Firewall, Routing, Apps, Services, VPN, Tools, and Diagnostics. The main content area contains the following settings:

- Gateway Change Kill States:** A toggle switch that is currently turned on (blue).
- Clear Auditlog Weeks:** A text input field containing the value '52'.
- Clear Auditlog Max Entries:** A text input field containing the value '10000'.
- CPU Mitigation:** A toggle switch that is currently turned on (red).
- CPU Profile:** A dropdown menu with 'Performance' selected.
- VRRP Start State:** A dropdown menu with 'Master' selected.
- VRRP Track Interfaces:** A toggle switch that is currently turned on (blue).
- States Sync Storage:** A dropdown menu with 'External' selected.
- Kernel Boot Options:** A text input field containing 'Kernel Boot Options'.

Gateway Change Kill States can be enabled or disabled. When enabled it will kill all States on Gateway change. This is useful when you want to force a gateway change. Be careful, it disrupts all connections though.

Clear Auditlog Weeks defines how long the auditlogs shall be kept with the System Action. Default is 52 weeks.

Clear Auditlog Max Entries Clears auditlogs with the System Action when there are more entries than this value. A large number of auditlogs will slow down the GUI. Please use the txt auditlog from the logging settings instead. Default is 10.000.

CPU Mitigation can be enabled or disabled. It enables a CPU mitigation like Spectre v2. This usually costs around 20% performance.

CPU Profile sets the systems CPU performance and power profile. *Performance* gives you the maximum speed but also uses more energy and might produce more heat. *Dynamic (schedutil)* will reduce the CPU speed or put CPUs to sleep if they are not needed. It might be slower to use this profile or it takes longer for CPUs to be ready to perform work. On the other hand your system will use less energy and might stay cooler.

VRRP Start State is either *Master* or *Backup*. The master TBF should be master and all other TBF backup. If not set to master the VRRP IPs will disappear upon changes/service reloads for a few seconds.

VRRP Track Interfaces will track Interfaces and fail over all IPs if an interface goes down.

States Sync Storage can either be *External* or *Internal*. Internal will save all states directly into the active state table at a greater processing cost but faster failover time as the states are available immediately. External will save all states in an external table and will load them at failover time. This is more efficient but there is a delay between the failover and when the states are available.

Kernel Boot Options can be used for custom kernel boot options.

Firewall Flowtable

Flowtable is a fast forwarding path for TCP/UDP packages that pass the firewall. Packages first traverse the firewall on the normal way. After a state is established the connection is added to the flowtable. Any incoming package will now be sent from the incoming to the outgoing interface directly, bypassing the firewall infrastructure and therefore saving a lot of processing time.

This feature allows for 2-3 times faster package processing and it is compatible with QoS and logging. It is enabled by default. If you enable IDS/IPS only bypassed traffic will be offloaded to the flowtable. If you enable the limiter inside a firewall rule the matching traffic will not be added to the Flowtable as there is no limiter functionality. If you encounter any issues, please disable this feature.

MTU must be the same on all involved interfaces. Otherwise you might see very low throughput on connections.

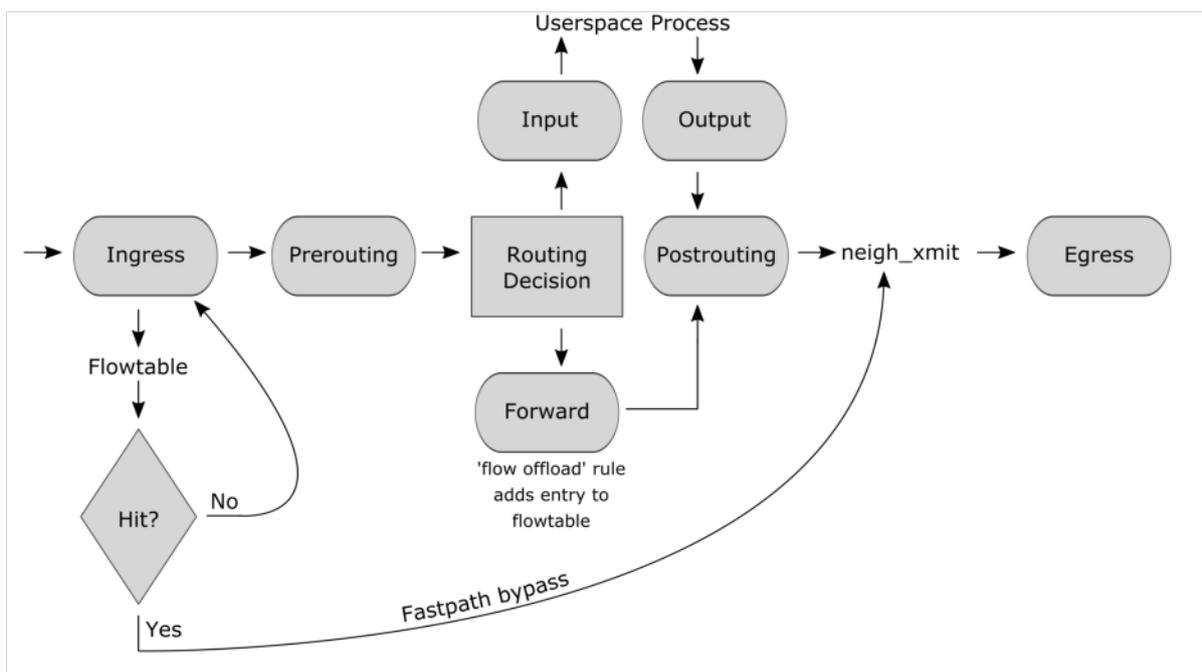


Fig.1: Netfilter hooks and flowtable interactions

General Troubleshooting

In case of very slow download or upload speeds you can go to **System** → **Settings** → **Advanced** and disable **Firewall Flowtable** and/or enable **Disable GRO**. This might improve the speed.

Warning: While disabling GRO and Flowtable Offload might improve network speeds, your Firewall will become much slower with a configuration like this!

8.2 Licence

You can find the Licence at **System** → **Licence**.

TBF needs a Licence to operate. Otherwise the TBF GUI, Terminal and Console will change into read only mode.

Official TBF hardware models from Voleatech have a builtin licence that is automatically activated after installation. You do not need to change the licence in that case.

8.3 Portal Settings

You can find the Portal settings at **System** → **Portal**.

The screenshot displays the Voleatech GUI's 'Portal Settings' page. The top navigation bar shows the Voleatech logo, a search bar, and the user 'admin admin'. The left sidebar lists various system settings, with 'Portal' selected. The main content area is divided into two sections: 'Portal Connection' and 'Remote Access'. The 'Portal Connection' section includes a table with the following data:

Field	Value	Action
Licence	Valid	Check
Updates until	Lifetime	Check
Portal Connection	Disconnected	Connect
Proxy URL	Proxy URL	
Portal URL	portal.voleatech.de	

The 'Remote Access' section below shows a 'Connector' toggle switch and a 'Remote Access' status of 'Disabled'. The footer of the page indicates '© Voleatech GmbH 2017 - 2020'.

8.3.1 Portal Connection

Here you can see if your TBF licence is valid, until when you can update your TBF and check the Portal Connection.

It's possible to manually check the licence and the updates by clicking on their *Check* button.

You can connect the TBF to your Voleatech Portal Account. The Portal Connection can be changed via its *Connect* or *Disconnect* button. To connect to the Voleatech Portal use your portal login user, which is an email address, as well as your portal password. The user must have the permissions to manage devices in the portal.

If the portal connection is established, pieces of information will be displayed in a separate info box.

This is required in order to use the remote access feature via the Voleatech Portal.

8.3.2 Remote Access

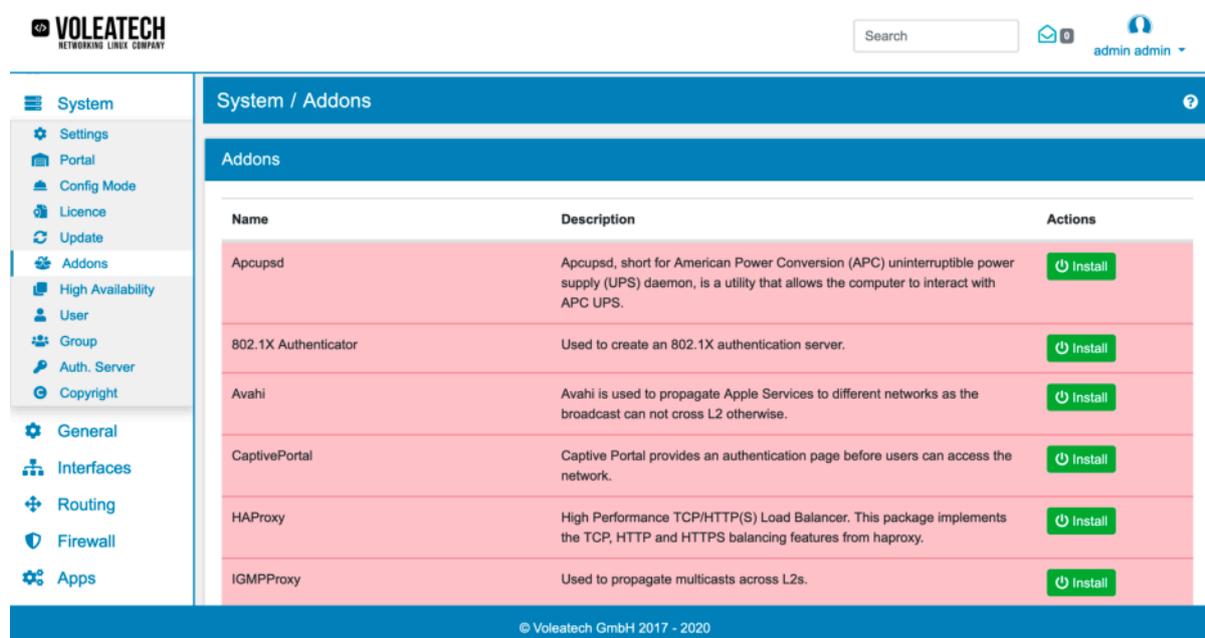
If you have a licence for remote access, you can enable the Portal Connector. The URL for the connector is `portal.voleatech.de`

You can now login to the Voleatech Portal with your account and access the firewalls Webgui remotely. The portal connector creates an encrypted connection to the portal and allows for access from the portal back to the Webgui. You do not need to create a firewall rule for this to work. Since the connection is initiated from the Firewall itself, the Firewall does not need to be accessible from the internet.

8.4 Addons

You can find the Addons at **System** → **Addons**.

Addons are extensions for the TBF that you can install. They will add a new GUI entry and allow you to extend your system easily. Addons will be installed in the background which may take some time.



The screenshot shows the Voleatech WebGUI interface. The top navigation bar includes the Voleatech logo, a search bar, and a user profile for 'admin admin'. The left sidebar contains a menu with 'System' selected, and sub-items like Settings, Portal, Config Mode, Licence, Update, Addons, High Availability, User, Group, Auth. Server, and Copyright. The main content area is titled 'System / Addons' and displays a table of available addons.

Name	Description	Actions
Apcupsd	Apcupsd, short for American Power Conversion (APC) uninterruptible power supply (UPS) daemon, is a utility that allows the computer to interact with APC UPS.	Install
802.1X Authenticator	Used to create an 802.1X authentication server.	Install
Avahi	Avahi is used to propagate Apple Services to different networks as the broadcast can not cross L2 otherwise.	Install
CaptivePortal	Captive Portal provides an authentication page before users can access the network.	Install
HAProxy	High Performance TCP/HTTP(S) Load Balancer. This package implements the TCP, HTTP and HTTPS balancing features from haproxy.	Install
IGMPProxy	Used to propagate multicasts across L2s.	Install

© Voleatech GmbH 2017 - 2020

You need an internet connection to install the addon and a valid update subscription, to connect to the update repository.

The following addons are currently supported:

- Apcupsd
- 802.1X Authenticator
- Avahi
- HAProxy
- IGMPProxy
- Netflow
- Ntopng
- PPPoE Server
- Web Application Firewall
- WebVPN

- ZeroTier

At the bottom of the page there is a **Check Addons** button. It checks whether all packages are installed correctly and if they are not, it tries to reinstall them.

The screenshot shows the Voleatech management interface. On the left is a navigation menu with categories like System, General, Interfaces, Routing, Firewall, and Apps. The 'System' category is expanded, showing sub-items: Settings, Portal, Config Mode, Licence, Update, Addons, High Availability, User, Group, Auth. Server, and Copyright. The 'Copyright' sub-item is selected, displaying a list of installed packages. Each package entry includes the package name, a brief description, and a button to manage its installation status. At the bottom of the list is a green 'Check Addons' button.

Package Name	Description	Action
Avahi	Used to create an Avahi daemonization server. Avahi is used to propagate Apple Services to different networks as the broadcast can not cross L2 otherwise.	Install
CaptivePortal	Captive Portal provides an authentication page before users can access the network.	Install
HAProxy	High Performance TCP/HTTP(S) Load Balancer. This package implements the TCP, HTTP and HTTPS balancing features from haproxy.	Install
IGMPProxy	Used to propagate multicasts across L2s.	Install
Ntopng	Ntopng is a network traffic probe that monitors network usage.	Install
Web Filter	Squid is a caching proxy for the Web supporting HTTP, HTTPS and more. It allows you to set Web Filters for granular control over web activities.	Uninstall
Intrusion Detection and Protection	Suricata is an open source-based intrusion detection system (IDS) and intrusion prevention system (IPS).	Uninstall

© Voleatech GmbH 2017 - 2020

8.5 Copyright

You can find the Copyright of each installed package at **System** → **Copyright**.

The directly used packages for the GUI and management are listed at the *Main* tab and the rest is at the *Other* tab.

You can click the *Licence* name of each package for more details.

USER AUTHENTICATION

9.1 User

You can find the User Settings at **Authentication** → **User**.

The screenshot displays the Voleatech web interface. On the left is a sidebar menu with categories: Settings, Portal, Config Mode, Licence, Update, Addons, High Availability, User, Group, Auth. Server, Copyright, General, Interfaces, Routing, Firewall, Apps, Services, and VPN. The main area is titled 'System / User' and contains tabs for 'Users', 'Groups', and 'Authentication Servers'. The 'Users' tab is active, showing a table with the following data:

First Name	Last Name	Username	Actions
admin	admin	admin	[Edit]
hasync	hasync	hasync	[Edit] [Deactivate] [Delete]

At the bottom right of the table is a '+ Add' button. Below the table is a pagination control showing '1' of 1 items. The footer of the interface reads '© Voleatech GmbH 2017 - 2020'.

On the User screen you can quick edit some user settings like **activating/deactivating** and **deleting** users.

Users are created in the Webgui and are **disabled in the Linux system** by default. You do need to activate them explicitly with the **System Access** option in the users setting.

Users can be in any number of *Groups*.

In order for a user to login to the webgui the **System Admin** or **System User** group membership is required. Other users can be used for services like OpenVPN or WebVPN.

Name	
Active	<input checked="" type="checkbox"/>
First name	admin
Last name	admin
Username	admin
Password	•••••••••• Strong
Retype Password	••••••~••••••~ Strong
Language	English
API Token	8fc15ee70aa9425464bc182c247b4dbe9be6181d
Date joined	2023-07-26 10:24:09

9.1.1 Permissions

Each User can have a set of permissions. Permissions can be configured on the User itself or through group memberships. Permissions are **additive**, meaning all permissions from Groups and users are added together to get the set of all permissions for the user.

Please be careful and consider which permissions each user should have.

The **Admin** user always has all permissions, disregarding which permissions you configure in the GUI. This user is a super user.

9.1.2 Language

Each user can change and configure their own language. By default all users have the global language defined in [Settings](#).

9.1.3 API Token

Each user has automatic generated API Token to access the REST API without a password. The user still needs the correct permissions to access any resource, the token is just to make the authentication process easier. Never the less their user and password do work as well.

9.1.4 SSH

The User can add their SSH Key/s here. If configured in [Settings](#), he can login without a password. The **system access** option is required for SSH access. If a user has *system access** you can also give him **sudo access** to become root.

9.1.5 Authentication Server

A User can have multiple authentication servers. When a user logs in, he will be authenticated against the selected authentication server. The default one is the TBF DB*. To change your Authentication Servers setup please go to **System** → **Auth. Server** and refer to the documentation at [Authentication Server](#).

9.1.6 Bookmarks

The screenshot shows the user profile page in a web interface. On the left is a navigation menu with categories: System, Authentication (User, Group, Auth. Server, Identity, Awareness), General, Interfaces, Firewall, Routing, Apps, Services, VPN, and Tools. The main content area is divided into two sections. The top section, titled 'Bookmarks', contains five rows, each with a 'Bookmark' label and a dropdown menu. The values are: Bookmark 1: - Sysstat; Bookmark 2: - Rules; Bookmark 3: None; Bookmark 4: None; Bookmark 5: None. The bottom section, titled 'OpenVPN Profile', contains a table with the following data:

Name	Description	Type	Tunnel Network	Export
External	-	certificate	222.12.11.0/24	Inline Archive

Each user can have up to 5 bookmarks that will show up in the upper right corner under his profile widget. This is a shortcut to menus. User permissions are required to access a bookmark.

9.1.7 OpenVPN Profile

If a user is part of a OpenVPN setup, as user or with a user certificate, the user can download the OpenVPN config at the OpenVPN profile section. The OpenVPN Profile section is at the bottom of the user update page as well as user settings/user profile page. A user can only download its own OpenVPN config files and not the config files of other users.

9.1.8 Certificate

A user can be linked to a user certificate. If you update an existing user there is also a *Create Certificate* button which opens a user certificate creation window. Otherwise you can go to **General** → **Certificates** and create one there.

Two Factor Authentication

Two Factor Authentication can be used on the Webgui and OpenVPN. We use One Time Passwords and TOTP as an additional authentication on top of the username and password.

You can create and delete the Two Factor Authentication elements here and also see the QR Code of the TOTP, as well as your One Time Passwords. One Time Passwords are deleted after they are used and a new one is generated automatically.

You can use any TOTP enabled App for your phone to use the codes, please make sure that the TBF clock is synchronized as TOTP depends on the clock being correct. There are a lot of different Apps available for this, e.g. Google Authenticator or Authy.

One Time Passwords can also be used to give a third person access to the device where you do not have to reset a user password everytime. Just hand out a one time password in addition to the username and password.

9.1.9 Profile

Each logged in user can edit their own profile by navigating to the right upper corner of the screen and clicking on his name. The profile contains the name settings as well as password, language, SSH key and bookmarks.

9.1.10 Logout

The logout option is also in the upper right corner by clicking on the name. Additionally after a period of inactivity the auto logout will disconnect the user from TBF.

9.2 Groups

You can find the Group Settings at **Authentication** → **Group**.

The screenshot displays the Voleatech web interface. At the top, there is a search bar and a user profile for 'admin admin'. The left sidebar contains navigation options like Portal, Config Mode, Licence, Update, Addons, High Availability, User, Group, Auth. Server, Copyright, General, Interfaces, Routing, Firewall, Apps, Services, and VPN. The main content area is titled 'System / Group' and has tabs for 'Users', 'Groups', and 'Authentication Servers'. The 'Groups' tab is selected, showing a table with the following data:

Name	Users	Actions
Admin	0	[Edit] [Delete]
OpenVPN Access	0	[Edit] [Delete]
User	0	[Edit] [Delete]

At the bottom right of the table area, there is a '+ Add' button. The footer of the page reads '© Voleatech GmbH 2017 - 2020'.

On the Group screen you can quick edit some group settings like **activating/deactivating** and **deleting** groups.

The main purpose of groups is to collect users with the same permissions. Each group has the option to set permissions that will be added to each user in the group.

In order for a user to login to the webgui the **System Admin** or **System User** group membership is required. Other groups can be used for services like OpenVPN or WebVPN.

The group **Read Only** allows for read only users to the GUI. Users must also be added to the **System User** Group to have GUI access in the first place.

9.3 Authentication Server

You can find the Authentication Server Settings at **Authentication** → **Auth. Server**.

On the Authentication Server screen you can quick edit some settings like **activating/deactivating** and **deleting** authentication servers.

Each server can have a **name** and can be **enabled** individually. You can choose either *LDAP* or *RADIUS* as **type**.

After creating the Authentication Server you still need to create a user with the same username in *User*. A password has to be supplied as well which might be random. The user will only be authenticated against the chosen Authentication Server though.

9.3.1 LDAP

Hostname or IP address has to be configured

Port can be configured and is by default 389 for TCP/TLS and 636 for SSL

Transport can be *TCP - Standard*, *TCP - STARTTLS* or *SSL - Encrypted*

Peer Certificate Authority can be selected if *Transport* is *STARTTLS* or *SSL - Encrypted*

Check Certificate can be enabled or disabled

Protocol version can be 2 or 3

Server Timeout is the timeout for LDAP operations in seconds. Default is 25

Search Scope Level can be *Entire Subtree* or *One Level*

Search Scope Base DN is the Base Distinguished Name for the search scope

Bind anonymous can be enabled or disabled

Bind User DN can be set up if *Bind anonymous* is disabled

Bind Password can be set up if *Bind anonymous* is disabled

Method can be *User* or *Custom*

Custom Query can be configured but please use the string USER where the username should be added in the query. It will be replaced with the actual username

Initial Template can be *OpenLDAP*, *Microsoft AD* or *Novell eDirectory*

User naming attribute uniquely identifies an entry and is *cn* by default

Group can be enabled or disabled

Group member attribute can be configured if *Group* is enabled and is *member* by default

Group CN can be configured if *Group* is enabled to find a group the user has to belong to in order to login

Sync User Group if you want matching group names in TBF to get the user added automatically

Group class attribute is the class attribute of the group (e.g. *group* or *posixGroup*)

Group naming attribute usually *CN*

Username Alterations determines whether the username after the @ symbol will be stripped away or not

Sync User can be enabled or disabled. If this option is enabled, it will automatically sync LDAP users to the TBF. If a user exists in the LDAP server but not in the TBF, a new user will be created. If a user was changed in the LDAP server, the corresponding user in the TBF will be updated. The following related settings will be available:

Unique ID is *entryUUID* for *OpenLDAP*, *objectGUID* for *Microsoft AD* and *GUID* for *Novell eDirectory*

User Firstname Attribute is *givenName* by default

User Lastname Attribute is "sn" by default

Sync Import if you want Users and Groups to be synced in the background. A sync job will be executed once an hour. Otherwise only users that login to the Webgui will be synced at login time.

Default Group the user is added to when synced. If you want your Users to have access to the Webgui automatically choose the **System Admin** or **System User** Groups.

9.3.2 RADIUS

Hostname or IP address has to be configured

Protocol can be *PAP*, *CHAP*, *MS-CHAPv1*, *MS-CHAPv2* or *EAP-MS-CHAPv2*

Shared Secret is a shared secret to connect TBF to the radius server

Services Offered can only be *Authentication* for the moment

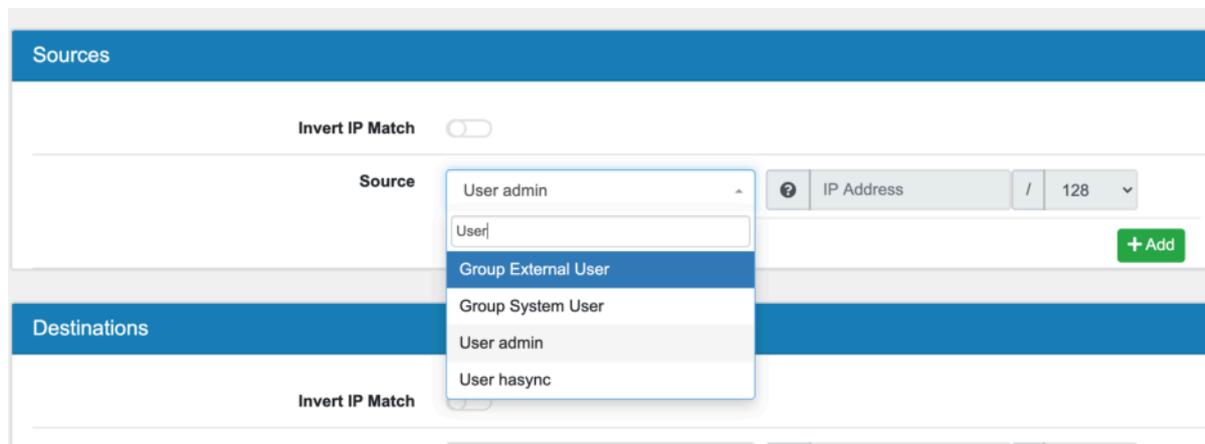
Authentication Port can be set up and is 1812 by default

Authentication Timeout is how long (in seconds) the RADIUS server may take to respond to an authentication request. The default is 5

9.4 Identity Awareness

You can find the Identity Awareness Settings at **Authentication** → **Identity Awareness**.

Identity Awareness allows you to associate *Firewall Rules (Forward and Input)* with Users and Groups. It allows for User associaten in Firewall Rules and management of user aware rules. In contrast to *Network Objects* the User IP Address can be updated dynamically.



A User or Group have to be created in TBF in order to use the User in a Firewall Rule. For larger environments an LDAP or Active Directory with User and Group Sync can be used *Authentication Server*.

9.4.1 Settings

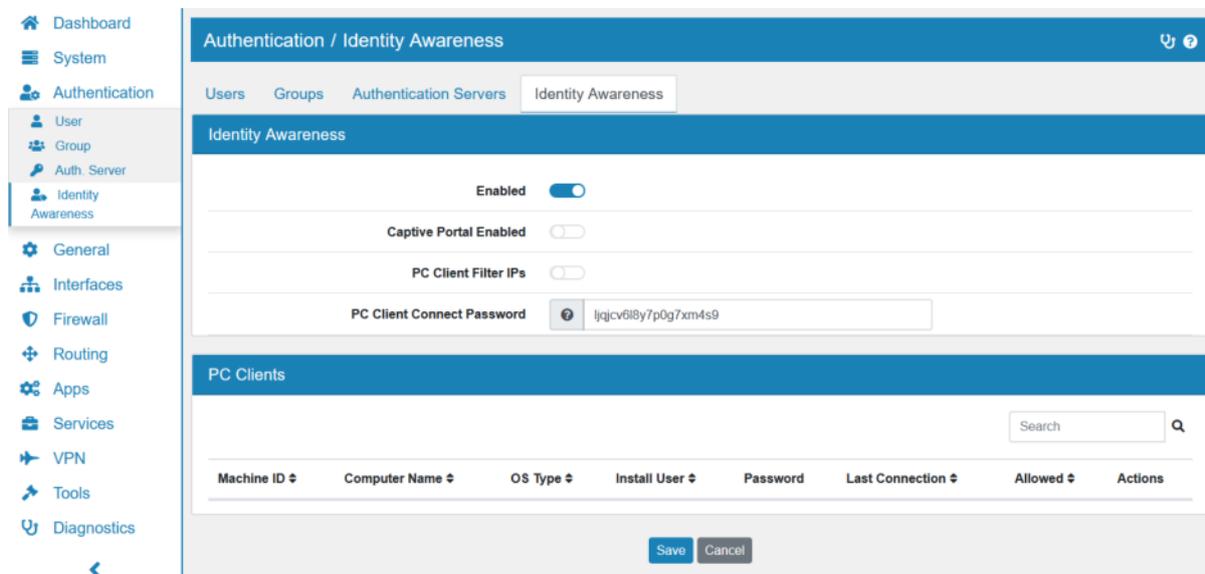
Enabled enables users and groups to be usable in Firewall Rules

Captive Portal Enabled will create a Captive Portal that you can configure and enable for users to login an associate their current IP Address with their user in TBF. It allows for dynamic IP association of a User with their current Dynamic IP.

PC Client Filter IPs will allow only IPs that are set in a network range from a firewall interface.

PC Client Connect Password is the password to initially connect the PC Client to the firewall.

Below is a list of all registered **PC Clients**. Each client has to be manually **allowed** in the actions column, so he can connect to the TBF.



9.4.2 User Settings

Each User has a *Identity Awareness* subpage in the **Authentication** → **Users** page.

First Name	Last Name	Username	Actions
 admin	admin	admin	Edit Identity Awareness 

It allows for static DHCP or static IP Address association with the User.

Authentication / User / Identity Awareness ?

DHCP Entries

DHCP Host Reservation

Available DHCP Host Reservations

Choose all

Chosen DHCP Host Reservations

192.168.10.1 (LAN) (12:34:56:78:90:AA)

Remove all

This is in addition to any Captive Portal dynamic IP the user might be registering.

Hosts

IP Addresses

?	1.2.3.4	?	Description	×
?	IP Address	?	Description	×

+ Add

Save
Cancel

INTERFACES

10.1 Interfaces General

You can find the Interface Settings at **Interfaces**.

Interface in TBF are abstracted by the Interface Object. For each Network Interface to be active it needs to be assigned to a TBF Interface through the **Interfaces** → **Assign** option.

Interface	ID	Network Interface	
WAN	WAN	ens18	Edit
LAN	LAN	ens19	Edit

Currently the following physical Interface types are supported:

- Normal Interface
- VLAN Interface (802.1q)
- Bridges (VLAN Aware)
- Bonds
- Tunnels (GRE, IPIP/GIF, SIT)
- PPPoE
- PPP

Each assigned Interface gets an entry in the Menu below **Interfaces**.

There are automatically generated Interfaces as well, like the App Bridge, OpenVPN and VTI Interfaces. They can be found under **Interfaces** → **Auto**.

10.2 Assign Interfaces

You can find the Interface Assign option at **Interfaces** → **Assign**.

Under the assign page you can either create, change, disable or delete Interfaces in the system. Please be aware that **WAN** and **LAN** can not be deleted but can be set to **Disabled** which effectively disables the interface.

Interfaces always have an internal id which is fix for **WAN** and **LAN**. It otherwise starts with **INT1** and the number increases with each new interface.

You can **rename** the interface however you like this is the human readable name and does not affect the internal id.

The **network interface** corresponds to the actual network interface name in the system.

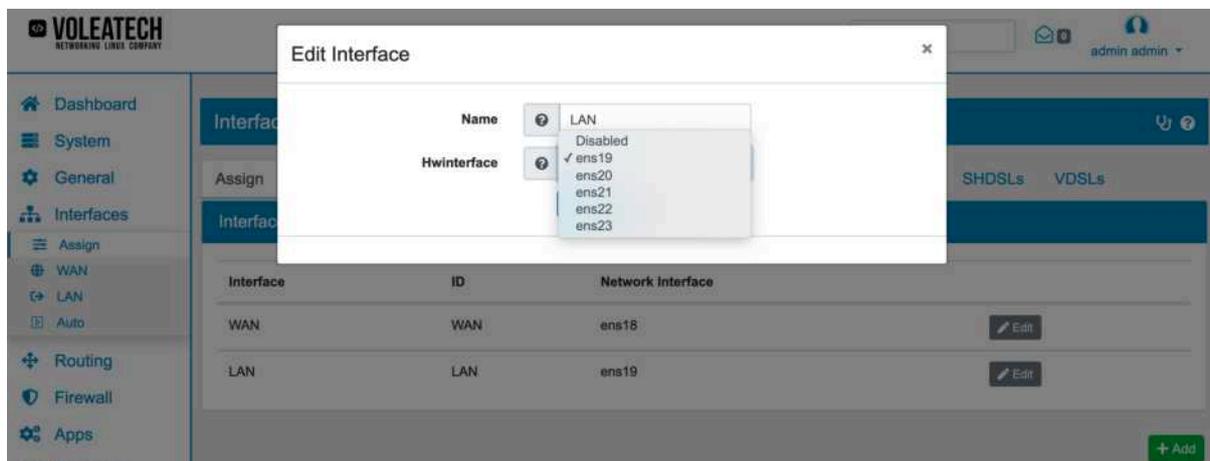
Create Default FW Rules will determine, if the default DNS, ICMP, Local and Internet firewall rules shall be created automatically for the new interface. The default rules are always created for the LAN interface.

Interfaces can have any role in TBF and are not limited to internal, external, LAN or WAN. Those are just labels and interfaces can have any functionality the user wants to configure.

10.2.1 Interface Abstraction

By creating Interface labels like WAN, LAN, INT1 and so on you can abstract the configuration from the physical Interface. This is useful if you want to move your existing configuration from one hardware Interface (network interface) to another without reconfiguring everything. Simply go to the settings page of the Interface with the configuration that you wish to move to another Interface and assign a new underlying network Interface.

That way your existing configuration can also be ported to a new or different TBF Appliance without the need to reconfigure everything.



We have a Video Tutorial regarding the interface abstraction:

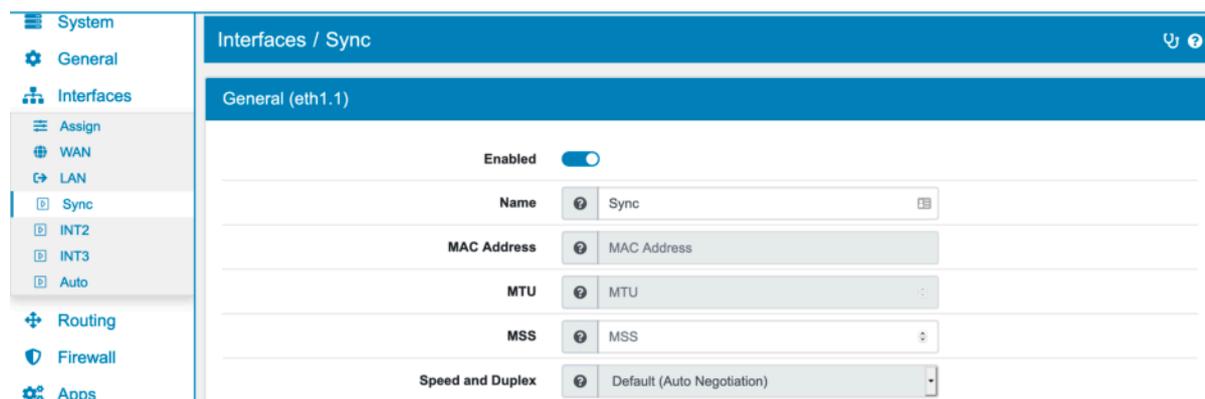
10.3 Configure Interfaces

In order to change an Interface setting in the system you need to navigate to **Interfaces** → **INTNAME** where INTNAME is the interface name you want to edit.

Depending on the underlying interface this represents you have different options and settings on this page.

On a normal Interface you have the following Settings.

10.3.1 General



Enabled to enable or disable the interface

Name can be changed to any name you like. The Interface name is used throughout the GUI for example when defining Firewall rules that belong to this Interface. The name will also be displayed as *ALTNAME* in the shell for each interface.

MAC Address if you want to override the default MAC Address. Be aware that depending on the interface representation this can have consequences on other interfaces. For example all VLANs of an interface share the same MAC.

MTU will change the Maximum Transition Unit. It is 1500 per default and if you plan on using IPv6 the minimum can not be less than 1280.

MSS fix will clamp the TCP connection at this size. It is usually only needed with PPPoE and PPP and on those interfaces it is generated by default.

Speed and Duplex configures whether the connection speed is automatically negotiated on the Interface. Alternatively you can also manually select a desired speed (within the limits of your hardware). On some Interface types like VLANs this option is grayed out since the connection speed depends on the underlying (physical) Interface.

10.3.2 IPv4 Settings

The screenshot shows the configuration interface for an interface. On the left is a navigation menu with categories like System, General, Interfaces, Assign, WAN, LAN, Sync, INT2, INT3, Auto, Routing, Firewall, Apps, Services, VPN, Tools, and Diagnostic. The main content area is titled 'IPv4 Settings' and contains the following fields:

- IPv4 Type:** A dropdown menu set to 'Static'.
- IP Address:** A text input field containing '10.10.20.1' followed by a slash and a dropdown menu set to '24'.
- Gateway:** A dropdown menu set to 'No Gateway' with a '+ Add' button to its right.

Below this is the 'IPv6 Settings' section with a dropdown menu for 'IPv6 Type' set to 'None'. The 'Advanced Settings' section at the bottom contains two toggle switches: 'Disable RFC1918' and 'Automatic Outbound NAT (SNAT)', both of which are currently turned off.

IPv4 settings contain the IPv4 type.

All IPv4 types are:

- None
- Static
- DHCP
- PPP
- PPPoE

Depending on the interface you only see a subset of the available options.

DHCP will use the DHCP Client to get an IP Address and Gateway on the Interface.

Static lets you configure an IP Address and if applicable a Gateway manually.

Gateway is available for static IPs and only affects the IP Addresses of the TBF itself. The IP Addresses of the TBF will always use this Gateway. This is especially needed in a multi WAN Setup so that the interface IP Address is responsive if the default route is with another interface. Otherwise all routing decisions are based on the main routing table, also for interface IP Addresses.

Lease Time is the DHCP Maximum Lease Time in seconds and is available if the IPv4 type is DHCP. The DHCP address will be refreshed after this time. If this is an Cellular interface a low value is necessary in case the Cellular connections changes.

10.3.3 IPv6 Settings

IPv6 settings contain the IPv6 type.

All IPv6 types are:

- None
- Static
- DHCP
- SLAAC
- Track

Depending on the interface you only see a subset of the available options.

Static lets you configure an IP Address and if applicable a Gateway manually.

DHCP will use the DHCP Client to get an IP Address. This requires a Router that advertises itself with RA. **IA_NA** can be set manually otherwise one will be generated. That is needed to obtain an IP Address from the server. **Prefix Delegation** can be enabled to also obtain a Prefix from the DHCP Server that can then be set on other interface via Track. **IA_PD** can be set manually. That is needed to obtain an IP Address from the server. **Prefix Delegation Size** is auto by default. You can also set the size of the prefix you want to request.

SLAAC will get the IP Address with the IPv6 SLAAC mechanism. Make sure there is at least one IPv6 Router that advertises itself in the network.

Track will obtain an IP Address via Prefix Delegation from another Interface. Please also select the interface that obtains a prefix. **IPv6 Prefix ID** If the ISP has delegated more than one prefix via DHCPv6, the IPv6 Prefix ID controls which of the delegated /64 subnets will be used on this interface. For example, if a /60 delegation is supplied by the ISP that means 16 /64 networks are available, so prefix IDs from 0 through 15 may be used.

Router Advertisement (Client) will either obtain the IP Address if SLAAC is enabled and/or the Gateway. The Gateway in IPv6 is always obtained by the Router Advertisement mechanism even if DHCP is used. If you disable Router Advertisement this mechanism will be disabled.

Gateway is available for static IPs and only affects the IP Addresses of the TBF itself. The IP Addresses of the TBF will always use this Gateway. This is especially needed in a multi WAN Setup so that the interface IP Address is responsive if the default route is with another interface. Otherwise all routing decisions are based on the main routing table, also for interface IP Addresses.

10.3.4 Advanced Settings

Disable RFC1918 will automatically create a Firewall rule to block all IPs in the RFC1918 block. Have a look at [Builtin Network Ranges](#) for a description of RFC1918. These IP addresses are used in private networks and it may be useful to block them from communicating on the WAN Interface for example.

Automatic Outbound NAT (SNAT) will automatically create a SNAT rule for this interface.

Note: Pay special attention to this if you have a High Availability setup. It might be required for you to disable this option on your WAN Interface and manually set it up as described in [HA Outbound NAT](#).

Automatic DDoS Limiting will create a rule to limit connections per incoming host per minute. The number of connections per minute can be set in the global settings.

MPLS enables MPLS. It is disabled by default.

VRF lets you choose a VRF. It is disabled by default.

10.3.5 WIFI Client

In case the interface is a wifi interface you can set the SSID and Password in order to join a wifi network.

10.3.6 WPA Authentication (802.1X)

WPA Authentication (802.1X) can be enabled by selecting a **Protocol**. The following protocols are available:

- EAP-TLS
- EAP-PEAP/MSCHAPv2 (both PEAPv0 and PEAPv1)
- EAP-PEAP/TLS (both PEAPv0 and PEAPv1)
- EAP-PEAP/MD5-Challenge (both PEAPv0 and PEAPv1)
- EAP-TTLS/EAP-MD5-Challenge
- EAP-TTLS/EAP-MSCHAPv2
- EAP-TTLS/EAP-TLS
- EAP-TTLS/MSCHAPv2
- EAP-TTLS/MSCHAP
- EAP-TTLS/PAP
- EAP-TTLS/CHAP
- EAP-MD5-Challenge
- EAP-MSCHAPv2

Entering an **Anonymous Identity** is optional. For authentication purposes an **Identity** and **Password** are required.

When selecting a protocol which supports *PEAP* or *TTLS* a **Certificate Authority** and **Certificate** are needed.

Note: The command line utility **wpa-cli** can be used to get information about the WPA Authentication status. It is also possible to create event driven commands on authentication or deauthentication. Please contact us if you need assistance in that regard.

10.3.7 Interface Dependent options

Some interfaces have other options. For example on a *Bridge* you can change the *STP/RSTP* as well as the *Bridge Port Settings*.

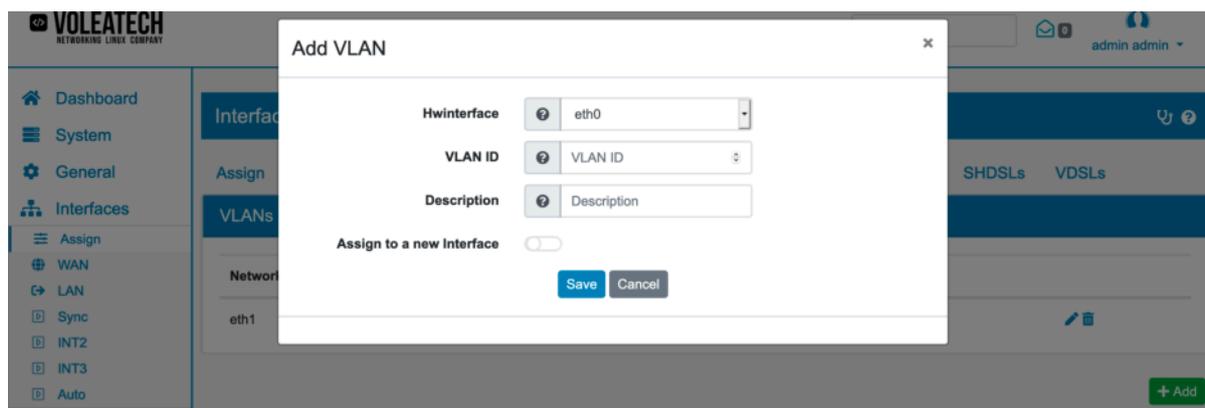
On *PPPoE* and *PPP* interfaces you can also change some of the settings on this page.

10.4 VLAN

You can find the VLAN Settings at **Interfaces** → **Assign** → **VLAN**.

Network Interface	VLAN ID	Description
eth1	1	HA Sync

TBF currently supports 802.1q VLANs.



VLANs can only be configured on top of:

- Physical Interfaces
- Bonds
- Bridges

Bridges are an exception, their VLANs are configured in the Bridge settings. A VLAN on top of a Bridge is only useful if you want to have an IP in that particular VLAN. VLANs defined in Bridges are still routed in L2 on the Bridge and forwarded on the defined Bridge Ports.

VLAN ID can be set on the interface that you select for the VLAN.

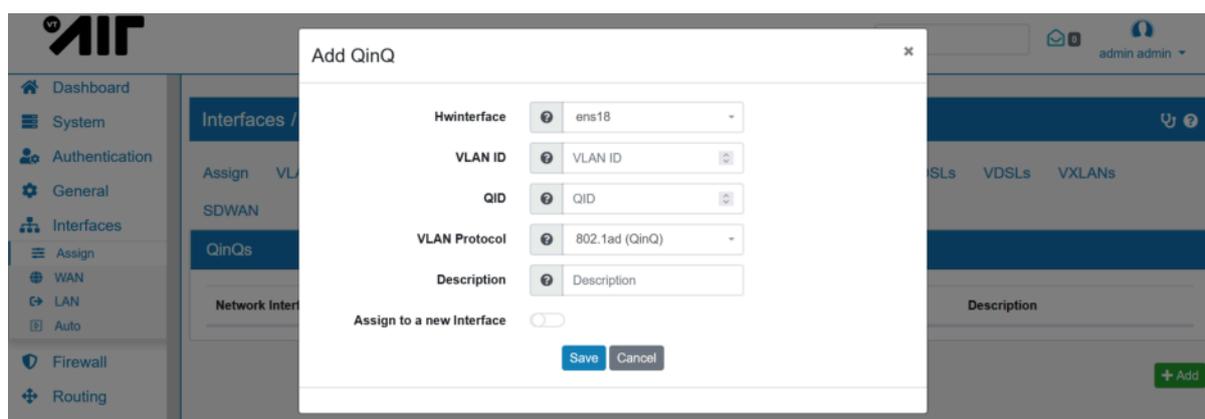
Assign to new Interface is an option shown when you create a new VLAN and it will automatically assign the Interfaces as described in [Assign Interfaces](#).

We have a Video Tutorial regarding the VLAN configuration:

10.5 QinQ

You can find the QinQ Settings at **Interfaces** → **Assign** → **QinQ**.

TBF currently supports 802.1ad QinQs and 802.1q VLANs.



QinQs can only be configured on top of:

- Physical Interfaces
- Bonds
- Bridges

VLAN ID can be set on the interface that you select for the QinQ.

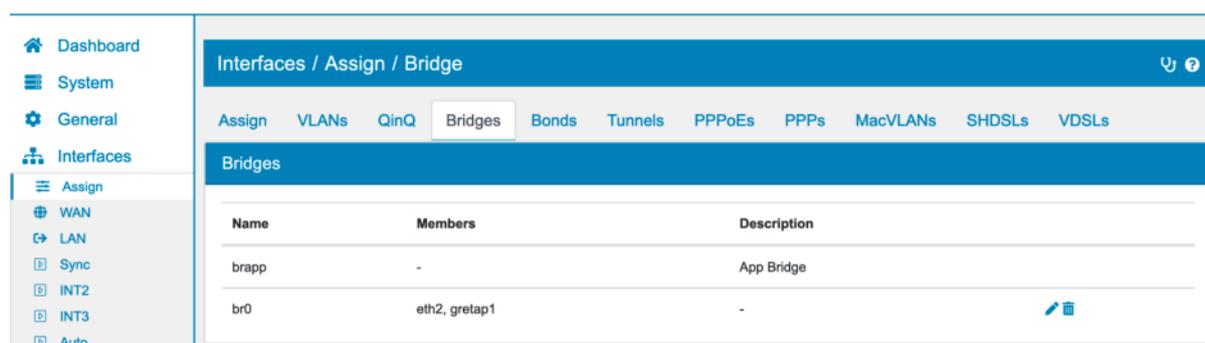
QID can be set on the interface that you select for the QinQ.

VLAN Protocol is the outer VLAN Tag Protocol. Default is the QinQ Tag but some setups may still use the VLAN Tag.

Assign to new Interface is an option shown when you create a new QinQ and it will automatically assign the Interfaces as described in [Assign Interfaces](#).

10.6 Bridge

You can find the Bridge Settings at **Interfaces** → **Assign** → **Bridge**.



Bridges are VLAN aware meaning that you can define VLANs on them and assign them to ports as either tagged or one of them as untagged.

A VLAN aware Bridge works like a switch.

Bridge can only be configured on top of:

- Physical Interfaces
- Bond
- OpenVPN Interface

You can pick and change the interfaces in a Bridge on the Edit or Add option of the Bridge.

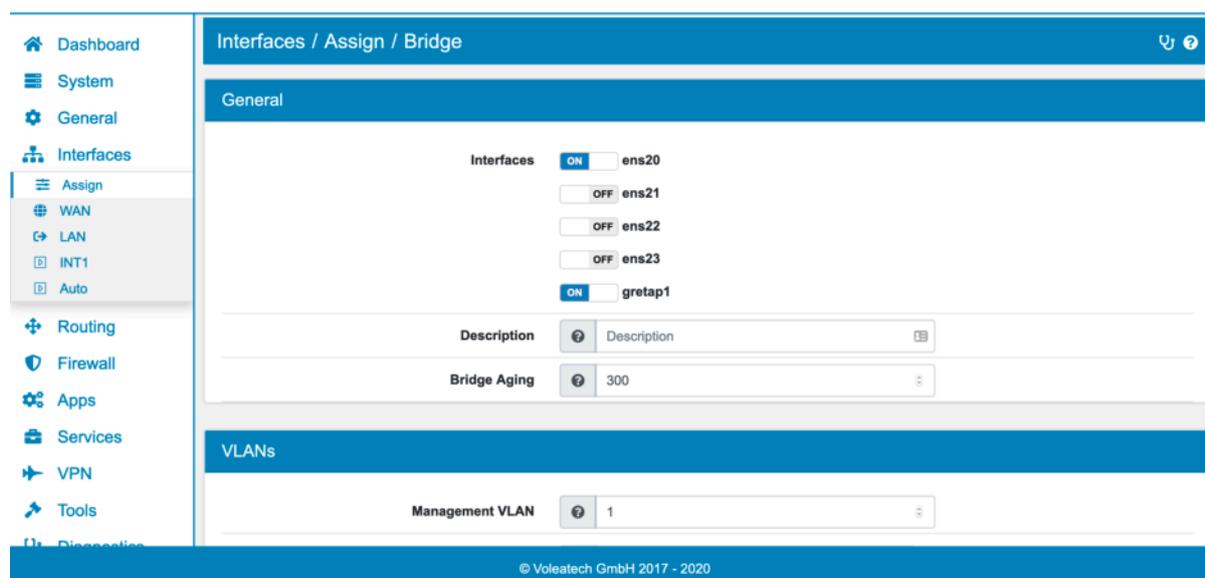
10.6.1 Create New Bridge

In order to create a Bridge between two or more Interfaces, the corresponding Interfaces need to be enabled in their settings page (see [Configure Interfaces](#)).

See also:

To create a Bridge between an Interface and a GRETAP Tunnel Interface, the Tunnel Interface needs to be configured and activated first. See [Tunnel](#) and [Bridging Scenarios](#) for reference.

Go to **Interfaces** → **Assign** → **Bridge** and click **Add** to create a new Bridge and define which Interfaces should be bridged together.



10.6.2 Bridge VLAN

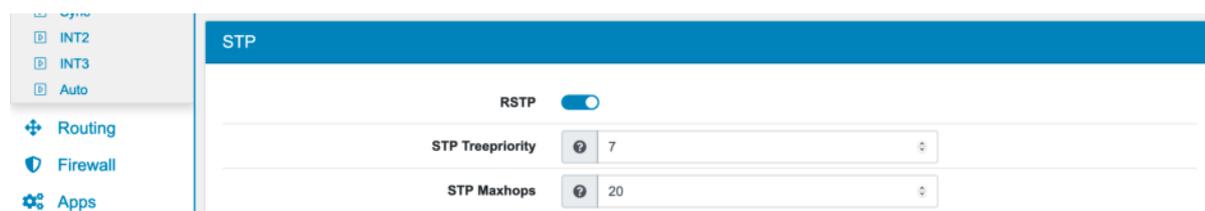
The bridge must have a default (non tagged) VLAN defined. The bridge will not be active and enabled unless you assign the Bridge to an interface and enable it.

You can then define additional VLANs either single VLANs or a range (e.g. 100-200). Only defined VLANs will be forwarded on the Bridge.

In Order to use IP Addresses or firewall rules on the Bridge you have to create a VLAN on the bridge under *VLAN* and assign it to an Interface.

You can not filter traffic on the bridge itself but only on VLAN interfaces on the bridge. The bridge automatically passes all other traffic through the firewall.

10.6.3 STP/RSTP



TBF supports RSTP which works with STP and MSTP. You can enable RSTP and also set the STP Treepriority.

Assign to new Interface is an option shown when you create a new VLAN and it will automatically assign the Interfaces as described in *Assign Interfaces*.

10.6.4 Bridge Port Settings

After you saved the Bridge, you can also configure settings for each individual bridge port.

MTU can be set on a per port basis

Speed and Duplex can be set on a per port basis

Enable Untagged VLAN if you want an untagged VLAN on the port. You can also have only tagged VLANs by disabling this option.

Untagged Port VLAN sets the untagged VLAN.

Bridgevlans can be enabled individually when they are defined on the Bridge. Be aware that you can not enable a subset of the defined VLANs. You would need to define each VLAN or VLAN range that you want to enable individually and enable them on the corresponding ports.

10.6.5 Bridge Port Settings STP/RSTP

Bridge Ports have different options and settings for STP.

STP Port BPDU Filter Filters out the STP BPDU Packets on this port and basically removes any STP information that come into the port

STP Port BPDU Guard BPDU guard prevents loops by moving a nontrunking port into an errdisable state

STP Port Path Costs The path costs are an important part of STP and give the fastest direction to the root bridge. A lower cost is better. 0 means the speed of the interface is used to automatically set a speed. Be aware that interfaces that have no speed get a high cost. This includes tunnels and vpn ports. In order to obtain the costs of a path to the root bridge, the costs from the received BPDU are taken and the configured port costs of the interface where the BPDU arrived on is added to that cost. The cheapest way to the root bridge is taken as the fastest way and those costs are sent to the next hop.

STP Port Priority In case ports have the same overall costs the lowest priority is preferred. Allows values from 0 - 15. Default is 7.

STP Restricted Root Port If enabled the port can not take root role of the port.

STP Edge Port Ports directly connected to end device cannot create bridge loops in the network. Therefore, the edge port directly transitions to the forwarding state, and skips the listening and learning stages. It also does not trigger a change notification when going up or down. It is recommended to enable this option for all ports that are connected to end devices.

The automatic STP Port Path Costs are set the following way

Link Speed	Costs
10 Mb/s	2000000
100 Mb/s	200000
1 Gb/s	20000
10 Gb/s	2000
100 Gb/s	200

10.6.6 Compatibility Rapid-PVST/PVST+

Rapid-PVST is creating a RSTP instance per VLAN. Devices with RSTP are only recognized on the VLAN 1, as their RSTP BPDU is send on the untagged VLAN 1. The spanning tree will therefore only be correct on VLAN 1, all other VLANs will have a spanning tree without the RSTP devices information. This can easily lead to problem with the setup, therefore the use of Rapid-PVST is discouraged. MSTP is working alternative for Rapid-PVST.

10.6.7 Compatibility MSTP

MSTP is backward compatible to RSTP and will recognize BPDUs from a RSTP device. MSTP can also create a RSTP instance per VLAN but it will run on RSTP mode on each port that it recognizes a RSTP BPDU.

10.6.8 Bridging Scenarios

Bridging multiple sites together

In order to create a single network out of multiple physical networks, Tunnels and Bridging can be used. First create a GRETAP Tunnel Interface as described in [Tunnel](#).

Create a new Bridge (as described above) that bridges the local Interface to the GRETAP Tunnel Interface.

The screenshot shows the Mikrotik WinBox interface for configuring bridges. The breadcrumb is 'Interfaces / Assign / Bridge'. The 'Bridges' tab is selected, showing a table with the following data:

Name	Members	Description
brapp	-	App Bridge
br0	ens20, gretap1	-

A '+ Add' button is located at the bottom right of the table.

Note: Pay special attention that none of the selected Interfaces has a local IP address assigned to it! For physical Interfaces set the **IPvX Type** to None. For the GRETAP Tunnel Interface leave the **Local Tunnel IP Address** empty.

Next, create a VLAN under **Interfaces** → **Assign** → **VLANs** as described in [VLAN](#) on the Bidge's Interface (e.g. br0), and assign an ID.

Interfaces / Assign / VLAN

Assign VLANs QinQ Bridges Bonds Tunnels PPPoEs PPPs MacVLANs SHDSLs VDSLs

VLANs

Network Interface	VLAN ID	Description
br0	1	-

+ Add

Enter the VLAN's ID in the VLAN settings of the Bridge under **Interfaces** → **Assign** → **Bridge**.

Bridge Aging 300

VLANs

Management VLAN 1

Bridge VLANs

- 1
- VLANs

+ Add

Go to **Interfaces** → **Assign** and change your LAN Interface's settings to the VLAN on the Bridge's Interface (e.g. br0.1 for Bridge br0 and VLAN 1). Alternatively you can create a new Interface.

Configure your LAN/Interface with your desired **IPvX Type** and activate the Interface.

Interfaces / Assign

Assign VLANs QinQ Bridges Bonds Tunnels PPPoEs PPPs MacVLANs SHDSLs VDSLs

Interfaces

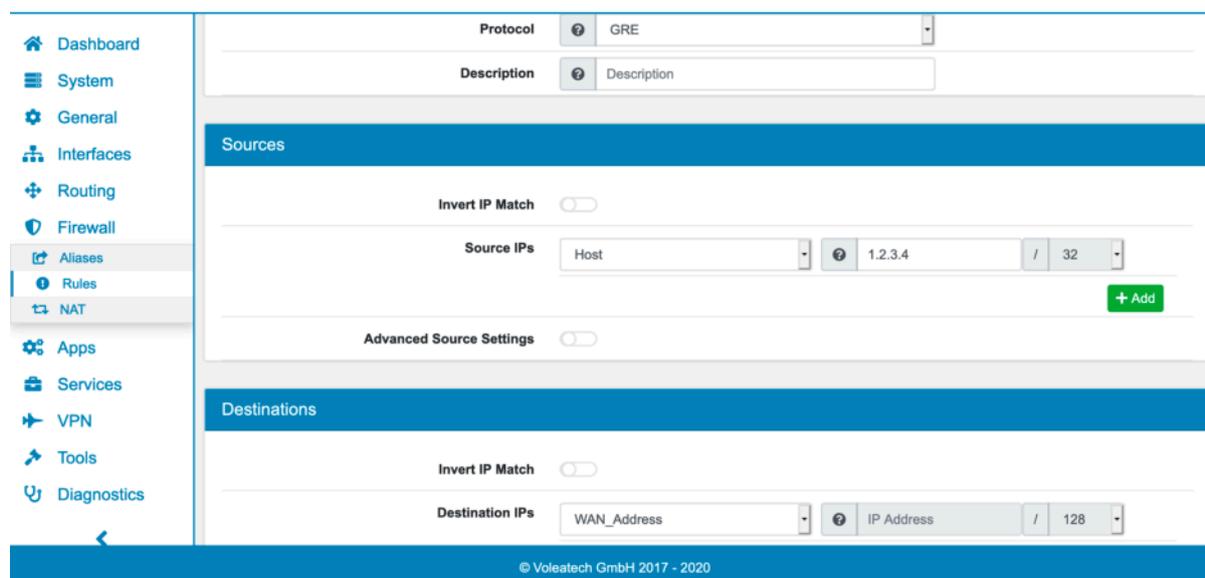
Interface	ID	Network Interface
WAN	WAN	ens18
LAN	LAN	br0.1
INT1	INT1	gretap1

+ Add

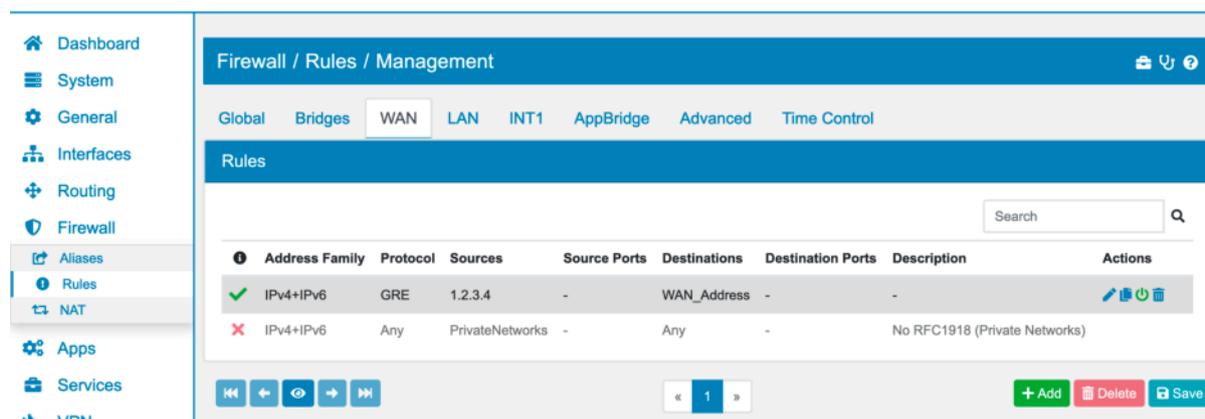
In order for traffic to move through the Tunnel you need to create a set of Firewall rules.

If your GRETAP Tunnel Interface was configured with the WAN address as the Tunnel endpoint go to **Firewall** → **Rules** → **WAN** and click **Add**.

Select GRE as the **Protocol**, enter the **Remote Public IP address** of your GRETAP Tunnel as the **Source IP** and select WAN address as the destination.

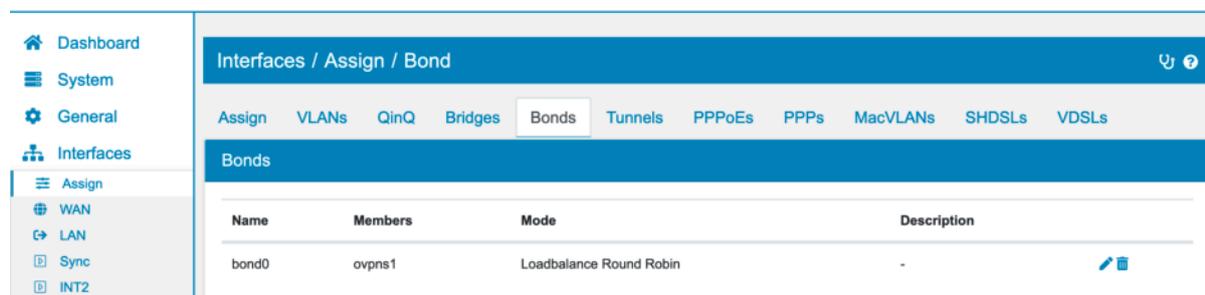


Save the new Firewall Rule. You may wish to encrypt your site-to-site traffic with an IPsec VPN on top of your GRE/TAP tunnel. See *GRE over IPsec* for further details.



10.7 Bond (Link Aggregation)

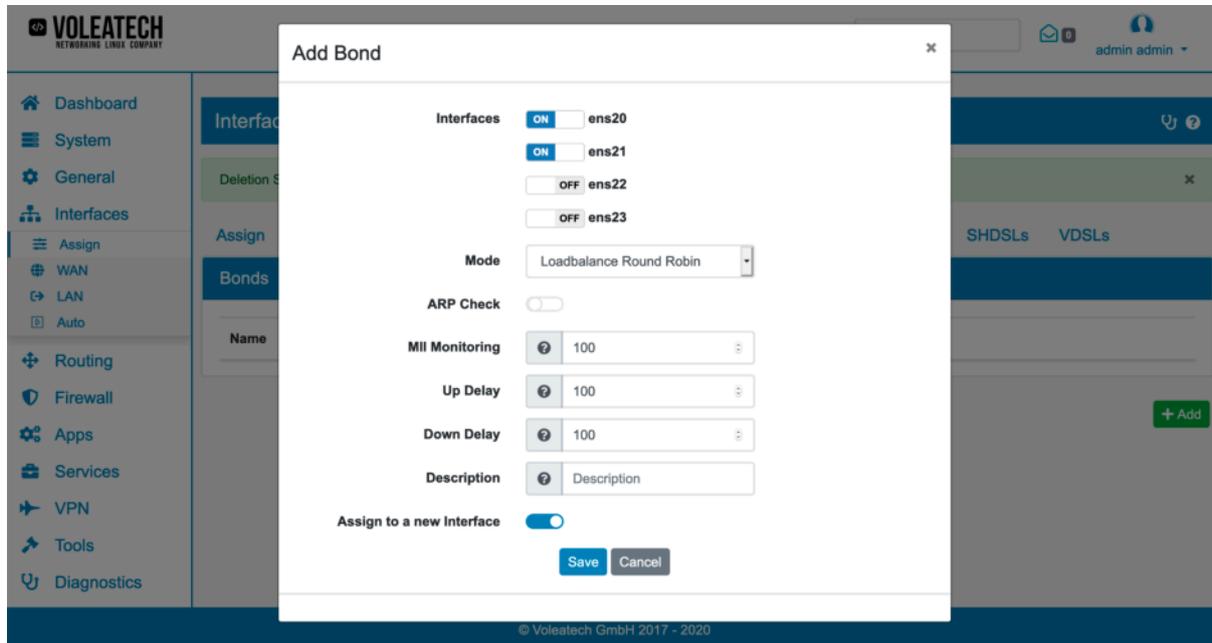
You can find the Bond Settings at **Interfaces** → **Assign** → **Bond**.



Your TBF supports bonding multiple physical Interfaces together as one logical Interface. This can be useful to increase the maximum bandwidth on an Interface, have redundancy or both. This is only possible with physical Interfaces though.

While setting up your new Bond, you will find that physical Interfaces that have already been assigned to an Interface like WAN or LAN are not shown as being available for bonding. Only physical Interfaces that haven't been assigned to an Interface can be bonded together.

Note: Since the WAN and LAN Interface are automatically created on your system by default it might be necessary to set the LAN Interface to None in its settings and then create the Bond afterwards. Otherwise the physical Interface is occupied by the LAN Interface and thus not available for bonding.



We support the following Bond modes:

- balance-rr (Loadbalance Round Robin)
- active-backup (Active/Backup)
- balance-xor (Load Balance with XOR)
- 802.3ad (LAG (802.3ad))
- balance-tlb (Adaptive transmit load balancing)
- balance-alb (Adaptive Loadbalancing)

You can configure the xmit policy that determines how the packets are distributed between Bond members. This is only available for balance-xor, 802.3ad and balance-tlb.

- Layer 2
- Layer 2+3
- Layer 3+4

You can use an ARP check with an IPv4 Address for balance-rr or balance-tlb instead of the MII check for a bond failure.

MII Mon configures the MII monitoring of the Bond ports in milliseconds.

Up Delay configures how long a Bond port is delayed until it is up in milliseconds when MII Mon is used.

Down Delay configures how long a Bond port is delayed until it is shut down in milliseconds when MII Mon is used.

You can pick and change the interfaces in a Bond on the *Edit* or *Add* option of the bond.

In case of **active-backup** you can choose the default active backup in the settings.

Assign to new Interface is an option shown when you create a new VLAN and it will automatically assign the Interfaces as described in [Assign Interfaces](#).

We have a Video Tutorial regarding the Bond configuration:

10.8 Tunnel

You can find the Tunnel Settings at **Interfaces** → **Assign** → **Tunnel**.

Name	Mode	Description
wg1	wg	WireGuard
ovpn1	ovpn	OpenVPN Server
gretap1	gretap	-

Tunnels do not need an underlying interface. They are defined by their source IP Address that must be defined in the system.

We support the following Tunnel modes:

- GRE
- GRETAP
- IPIP/GIF
- SIT

GRE/GRETAP

GRE creates a Layer 3 Tunnel. GRETAP creates a Layer 2 Tunnel, which can be used to create a Layer 2 network between nodes (see [Create New Bridge](#)). Both can be secured with IPsec over GRE encryption (see [GRE over IPsec](#) for more).

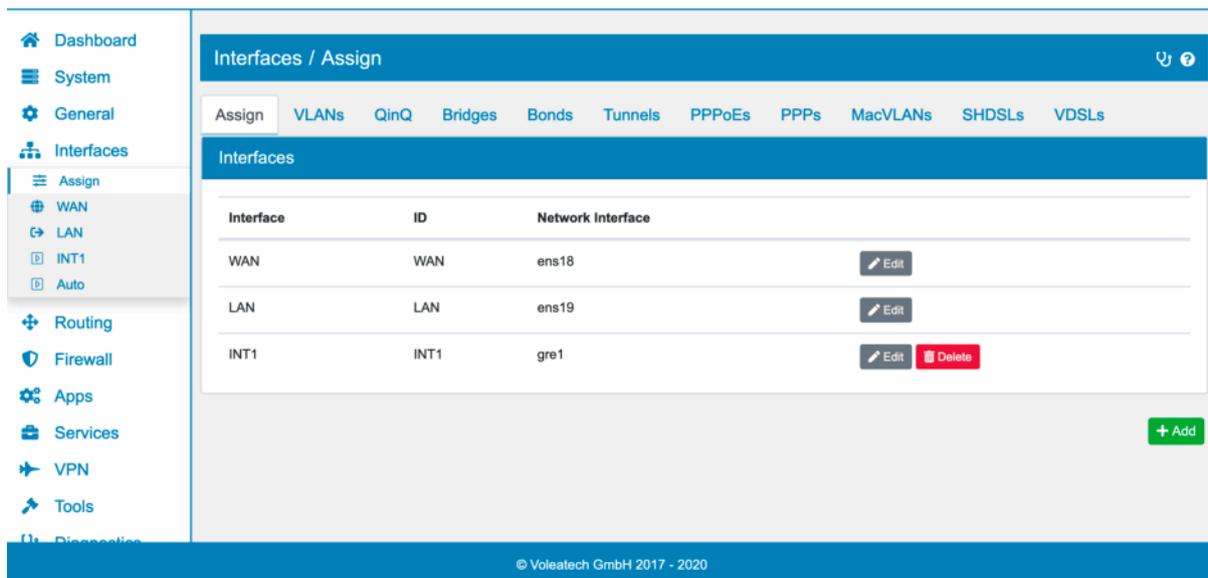
10.8.1 Creating a new Tunnel

To create a new Tunnel go to **Interfaces** → **Assign** → **Tunnel** and click **Add**.

Select a tunnel mode under **Mode** (for example: GRE).

The **Assign to new Interface** option will automatically create a new Interface (INTx) based on your new Tunnel if activated. Alternatively you can manually add your Tunnel to a specific Interface as described in [Assign Interfaces](#).

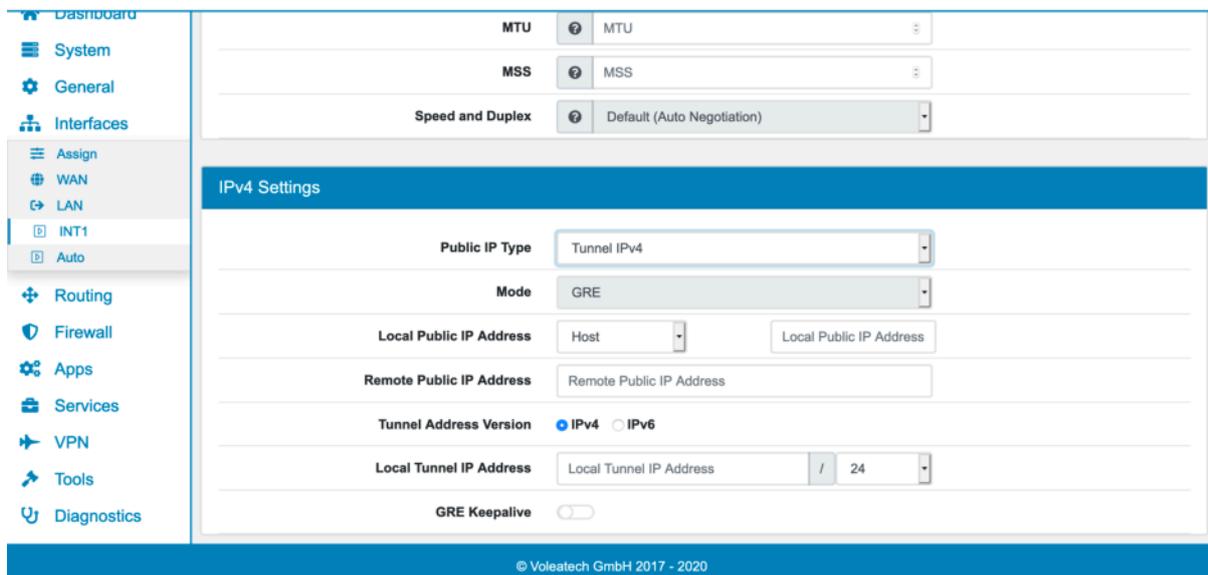
Name	Mode	Description
gre1	gre	-



Specific Firewall Rules for the Tunnel Interface can be configured as described in *Firewall Rules (Forward and Input)*.

10.8.2 Interface Tunnel Settings

The Interface Tunnel configuration can be found in the left sidebar under **INTx** (or the name that you manually assigned to the Tunnel Interface).



A tunnel always has an **outer IP Type** and an **inner IP Type**. The **outer IP Type** is IPv4 or IPv6 depending, on the tunnel type there is no choice. This sets the sender and destination of the Tunnel to an IPv4 or IPv6 Address.

Local Public IP Address is the sender IP Address and it is an Interface or Virtual IP Address of TBF.

Remote Public IP Address is the destination IP Address of the remote endpoint

Tunnel Address Version is depending on the Tunnel Type IPv4 or IPv6 and represents the **inner IP Type**

Local Tunnel IP Address is the local tunnel IP Address and the corresponding subnet mask. Make sure that the remote endpoint has a different IP Address in the same subnet.

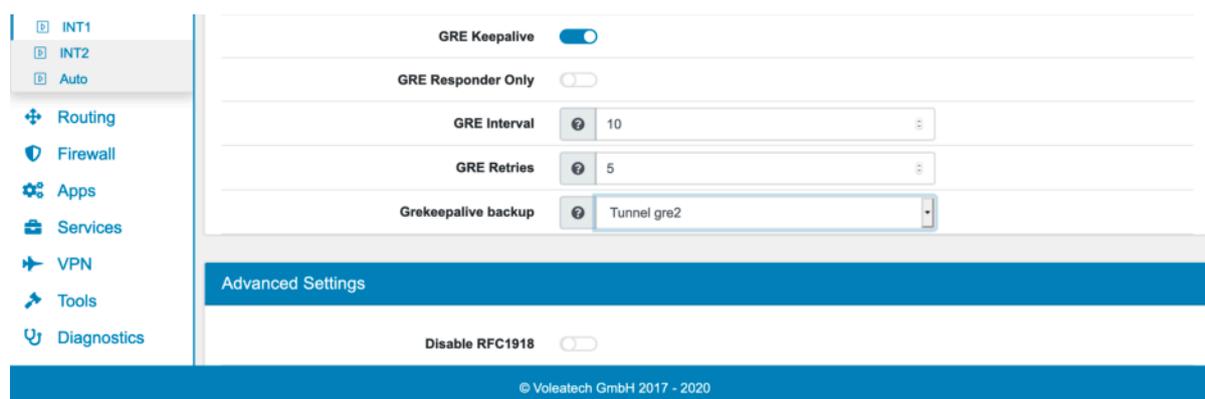
GRE Keepalive enables the GRE Keepalive Feature for IPv4 that can be further configured below.

GRE Responder Only This will only answer the packages sent by the remote Tunnel endpoint device and it does not have any influence on the tunnel status. The tunnel is always considered to be up in TBF. Disable this option to also actively send GRE Keepalive Packets and set the interface to down if no response is received.

GRE Interval The interval to send GRE keepalive packets to the remote address.

GRE Retries Retries before the Tunnel is set to down when no GRE keepalive is answered.

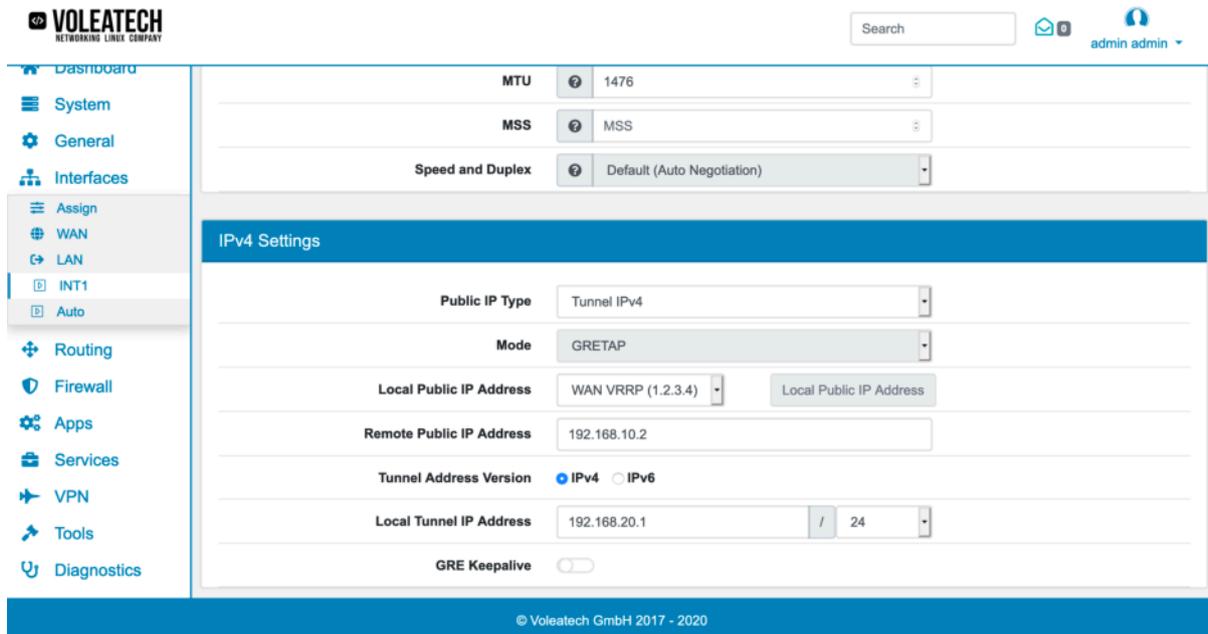
Grekeepalive Backup If multiple GRE Tunnel Interfaces are configured, one of them can act as a backup in case the other one goes down. Both Tunnel Interfaces need an activated GRE Keepalive Feature for this to work. The second Tunnel Interface is then added as a backup in the settings of the primary Tunnel Interface.



10.8.3 GRE with Failover

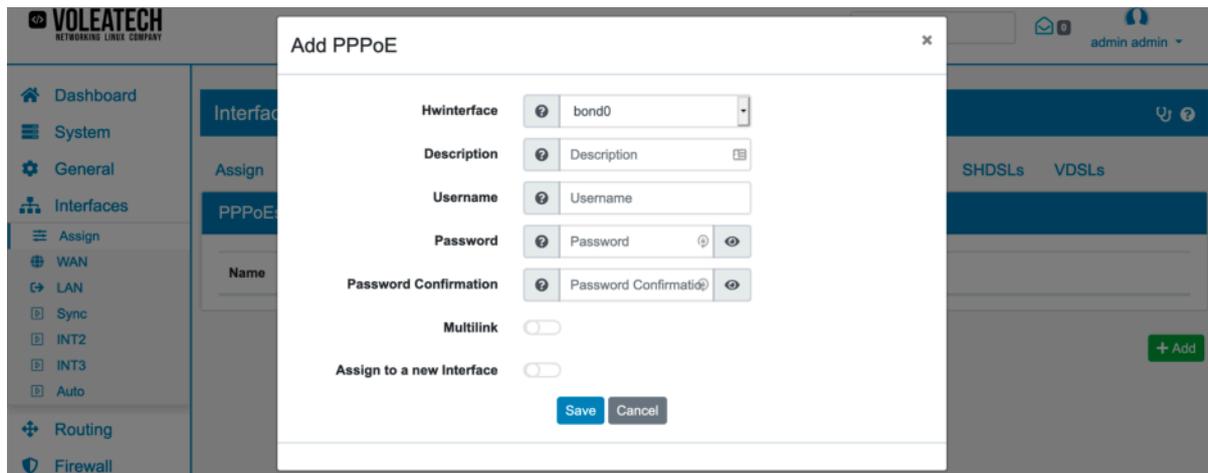
If you are using the High Availability feature of your TBF device you should configure your GRE tunnel in a way that works seamlessly when switching between routers. For this to work you should choose the virtual IP that you configured when setting up your *High Availability* feature as the **Local Public IP**. This ensures that the IP doesn't change when switching routers (as described in *Setup Examples*).

If you have multiple WAN connections you can additionally configure a second GRE tunnel via another Interface, create a second virtual IP address for the second WAN Interface and set the second tunnel as a backup. To do so use the **Grekeepalive backup** feature of your first GRE tunnel as described above.



10.9 PPPoE

You can find the PPPoE Settings at **Interfaces** → **Assign** → **PPPoE**.



PPPoE can only be configured on top of:

- Physical Interfaces
- VLAN Interface

PPPoE is commonly used for DSL dial in connections.

Username is the PPPoE Username.

Password is the PPPoE Password.

Master Only can be enabled or disabled. In case of a HA setup, this PPPoE is only added to the master device. It's disabled by default.

Assign to new Interface is an option shown when you create a new VLAN and it will automatically assign the Interfaces as described in [Assign Interfaces](#).

10.9.1 DSL Connection via PPPoE

We have a Video Tutorial regarding how to create a DSL connection via PPPoE:

10.10 PPP

You can find the PPP Settings at **Interfaces** → **Assign** → **PPP**.

The screenshot shows the 'Add PPP' configuration window in the VOLEATECH web interface. The window is titled 'Add PPP' and has a close button (X) in the top right corner. The form contains the following fields and controls:

- Hwinterface:** A dropdown menu with 'None' selected.
- Modem Port:** A dropdown menu with 'None' selected.
- Modem Data Port:** A dropdown menu with 'None' selected.
- Description:** A text input field with 'Description' as a placeholder.
- Country:** A dropdown menu with 'Custom' selected.
- APN:** A text input field with 'APN' as a placeholder.
- Username:** A text input field with 'Username' as a placeholder.
- Phone Number:** A text input field with '*99#' as a placeholder.
- Init String:** A text input field with 'ATI' as a placeholder.
- SIM PIN:** A text input field with 'SIM PIN' as a placeholder.
- Roaming:** A toggle switch that is currently turned on (blue).

At the bottom of the form, there are two buttons: 'Save' (highlighted in blue) and 'Cancel'.

PPP can only be configured on top of:

- WWAN Physical Interfaces
- Modem Serial Ports

PPP is commonly used for Cellular modem dial in connections.

There are three drop downs: **Country**, **Provider** and **Plan**. Depending on the selection it will prefill several of the following fields with data.

Username is the PPP Username.

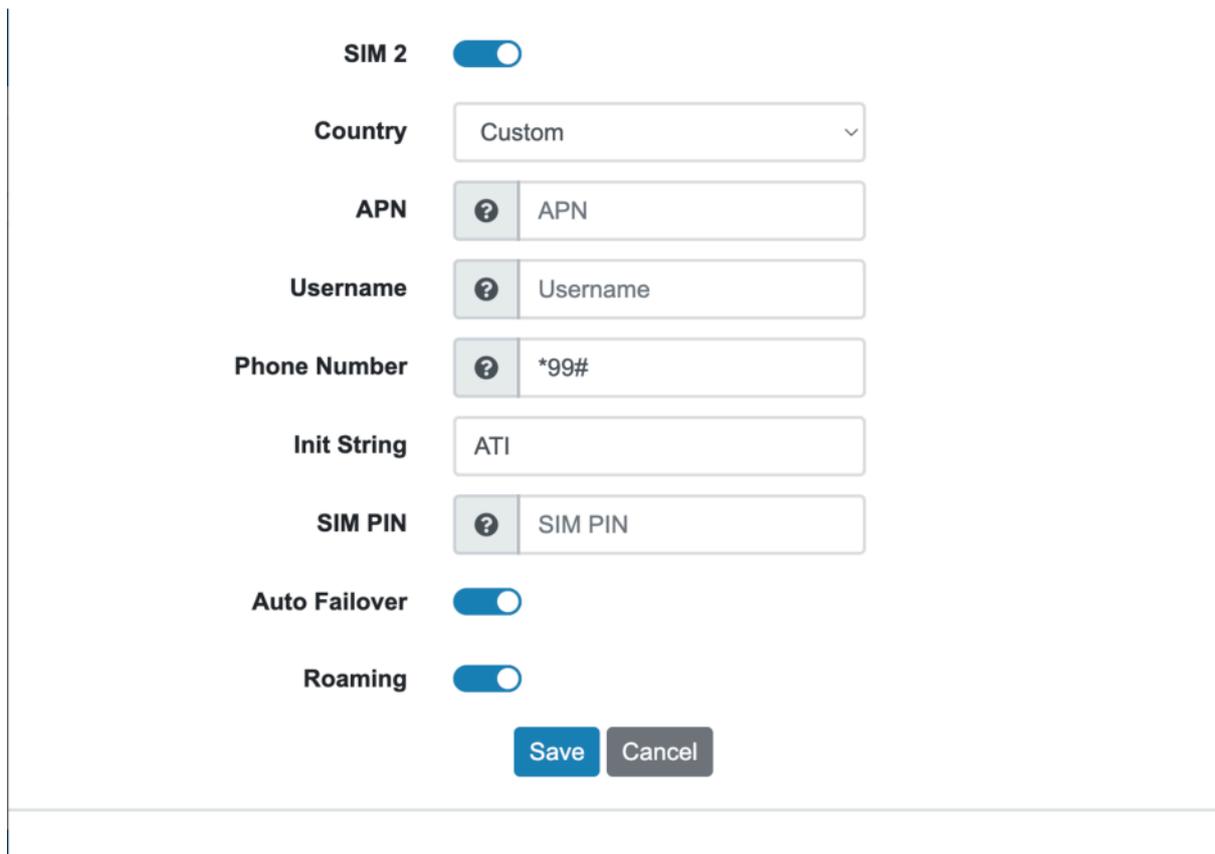
Password is the PPP Password.

APN is the Access Point Name.

Auth Authentication method for the connection, either None, Chap or PPP.

SIM PIN can be configured if necessary.

Dual SIM Card Support if you have a TBF that has two physical SIM card slots, you can utilize the Dual SIM Option. Only one SIM Card can be active at the same time but you can configure an automatic failover in case the **Gateway** of the connection is down. In order for this to work, please configure a monitoring IP and disable the **Gateway** option *Always Up Gateway*.



The screenshot shows a configuration window for SIM 2. The settings are as follows:

- SIM 2**: Enabled (toggle switch)
- Country**: Custom (dropdown menu)
- APN**: APN (input field with a help icon)
- Username**: Username (input field with a help icon)
- Phone Number**: *99# (input field with a help icon)
- Init String**: ATI (input field)
- SIM PIN**: SIM PIN (input field with a help icon)
- Auto Failover**: Enabled (toggle switch)
- Roaming**: Enabled (toggle switch)

Buttons: Save, Cancel

Options all options above are available again for the second SIM card.

Auto Failover enables the failover to the non active SIM card in case the Gateway of the connection goes down.

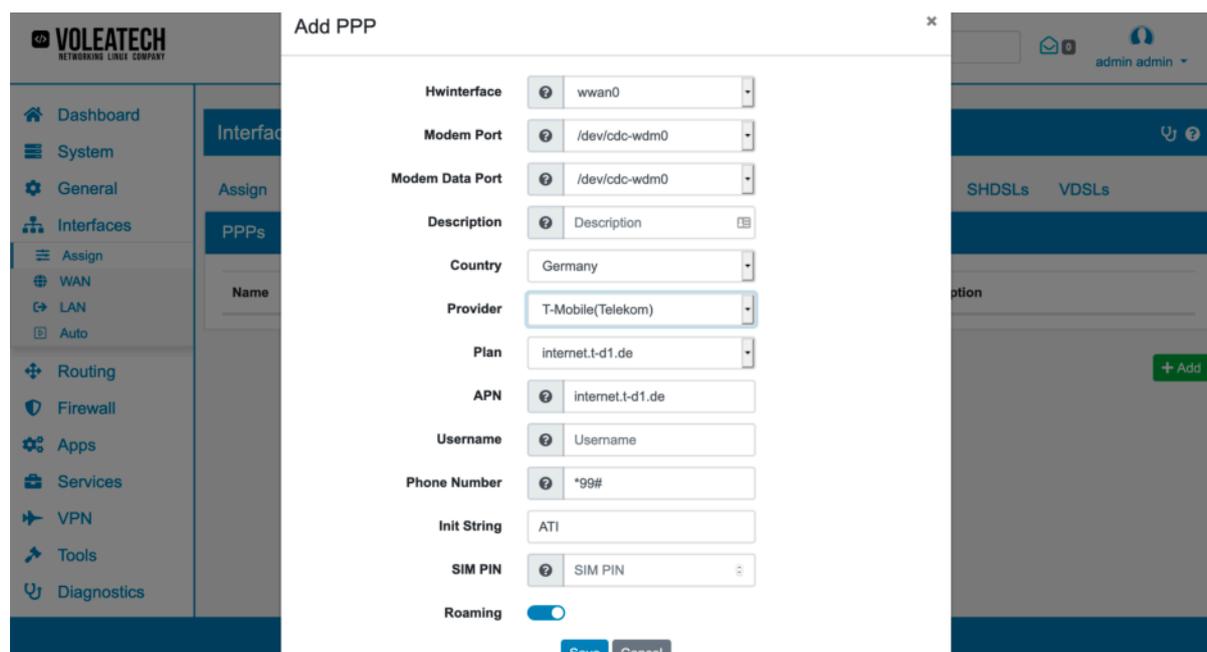
Roaming to allow the modem to use roaming.

10.10.1 LTE/5G

If you bought your TBF with *LTE* or *5G*, you can configure it with the following settings:

HWInterface wwan0 **Port** /dev/cdc-wdm0 **Data Port** /dev/cdc-wdm0

Add the dial in data of your provider and assign the PPP to an interface.



You can now configure your newly created interface for internet or as a backup connection.

We have a Video Tutorial regarding the LTE/5G configuration:

10.10.2 LTE450

LTE 450 is a network that utilizes the 450MHz cellular band to provide robust, long-range connectivity with increased coverage and deeper signal penetration. This frequency is now being used for LTE 450 networks as the industry transitions into the LTE and 5G era. The 450MHz band is well-suited for IoT devices and critical applications, ranging from smart grid and smart meter services to public safety applications. It supports CAT-M and narrowband-IoT (NB-IoT) technologies, making it ideal for large area coverage. This has enabled cellular providers to offer blanket coverage cost-effectively. The 450MHz band is used by 115 operators in 60 countries across the world.

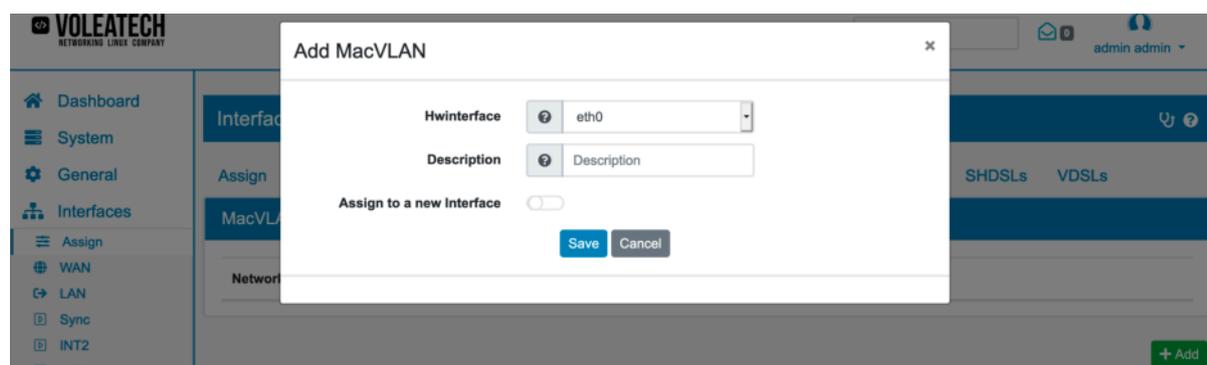
If you bought your TBF with *LTE450*, you can configure it with the following settings:

HWInterface None **Port** '/dev/ttyCELLULAR' **Data Port** '/dev/ttyCELLULAR'

Add the dial in data of your provider and assign the PPP to an interface.

10.11 MacVLAN

You can find the MacVLAN Settings at **Interfaces** → **Assign** → **MacVLAN**.

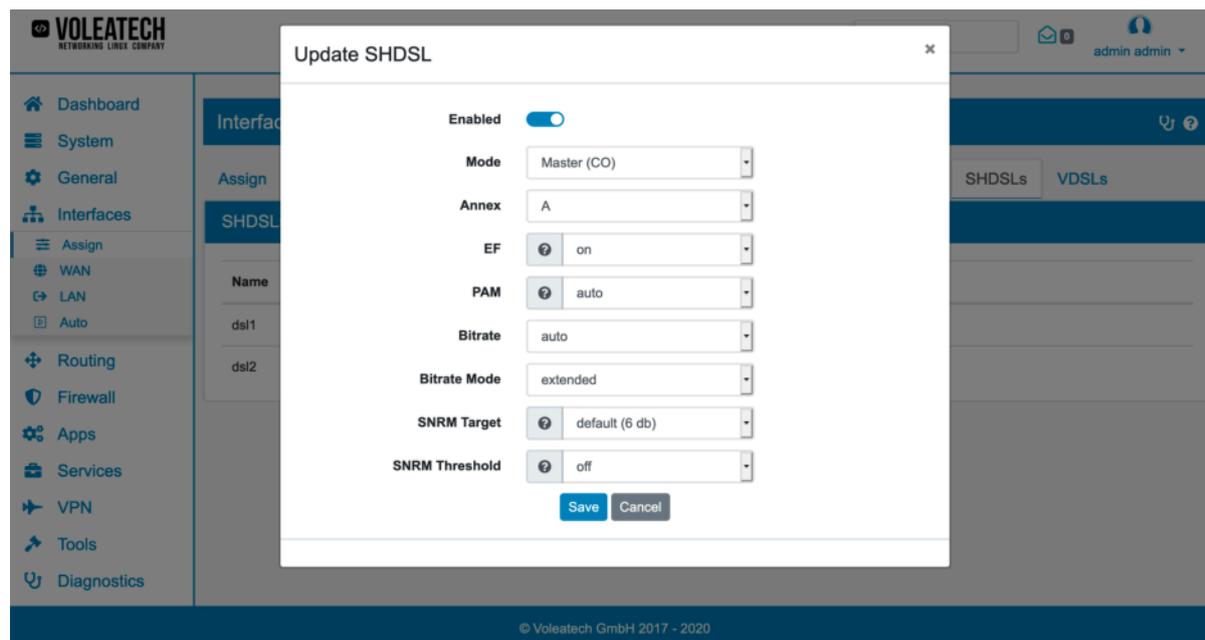


A MacVLAN is an interface on top of another interface. It has its own Mac Address and appears like a normal network interface to the outside world. If you have an ISP that can only assign IP Addresses to MAC Addresses, you can create multiple MacVLANs on your WAN Port to use them all.

Assign to new Interface is an option shown when you create a new MacVLAN and it will automatically assign the Interfaces as described in [Assign Interfaces](#).

10.12 SHDSL

You can find the SHDSL Settings at **Interfaces** → **Assign** → **SHDSLs**.



SHDSL stands for **Symmetric Digital Subscriber Line** and is responsible for the transmission of digital data over the copper wires of the telephone network. The following options can be changed:

Enabled to enable or disable the modem. It is highly recommended to disable the modem if it is not in use. The power consumption is much higher when the modem is searching for a connection.

Mode can be either *Master (CO)* or *Slave (CPE)*.

Annex can be A or B.

EF Emergency Freeze can be on or off and is *on* by default. Emergency Freeze will stop data transmission and freeze the connection in order to prevent connection loss on bad signals.

PAM is the Pulse-amplitude modulation and *auto* by default.

Bitrate is *auto* by default.

Bitrate Mode is *extended* by default.

SNRM Target is the Signal-to-noise ratio Target and *default* by default.

SNRM Threshold is the Signal-to-noise ratio Threshold and *auto* by default.

10.12.1 SHDSL Tuning

The SHDSL modem will try and find the right connection settings. If that takes longer than 5 minutes, you should go ahead and tune the parameters manually.

The *Master (CO)* determines the connection and you should start changing the settings on it.

PAM is influenced by the quality of your DSL cable. Bitrate is influenced by the length of your DSL cable.

Depending on your cable you should start tweaking one or both settings.

SNRM should be between 6 and 9db or for very harsh environments 12db. The SNRM threshold gives an upper bound if the quality of the DSL line is not always the same. Brief fluctuations in signal quality are not necessarily recognized.

To find the optimal speed you need to tune PAM and Bitrate if autodetect does not work. It is a 2 dimensional problem, where the amplitude (PAM) is the y axes and the speed (Bitrate) is the x axes of the wave that is used for the DSL signal.

Speed can be gained by a higher amplitude (PAM) if the cable has a good quality or by speed (Bitrate) if the cable is not too long.

10.12.2 Bitrate Mode

The *Bitrate Modes* can have specific limitations:

g.shdsl.bis needs PAM 16 or PAM 32. PAM 16 does not support a bitrate higher than 4 Mbit/s. PAM 32 does not support a bitrate higher than 6 Mbit/s.

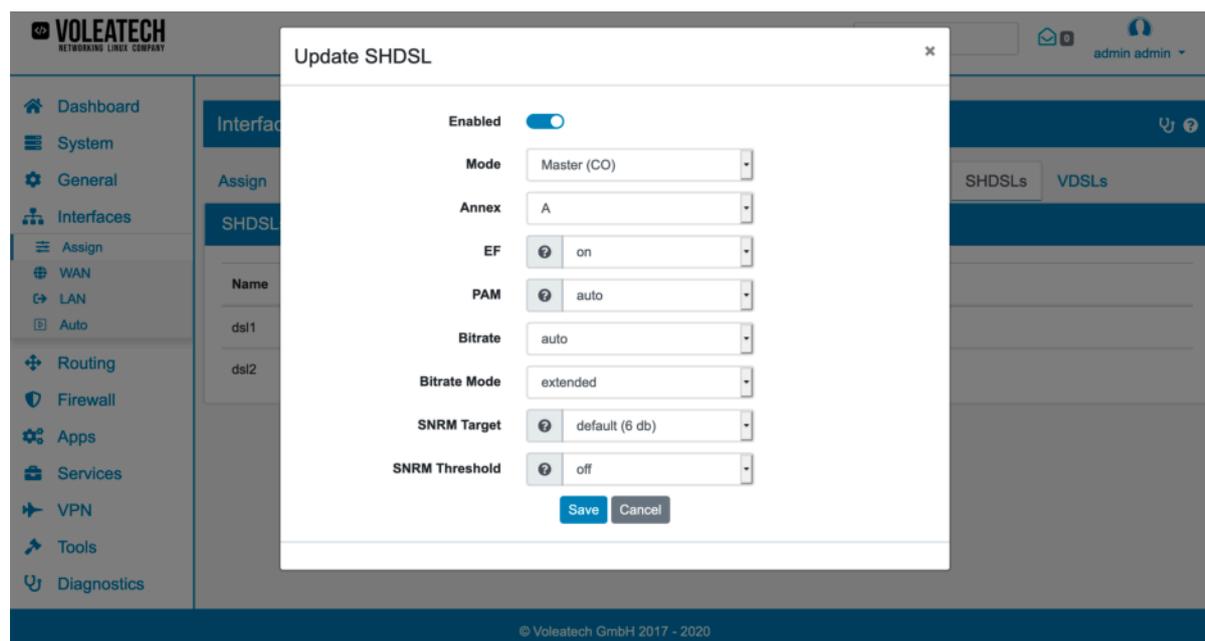
g.shdsl needs PAM 16. It also does not support a bitrate higher than 4 Mbit/s.

extended does not need a specific PAM or bitrate.

10.12.3 SHDSL Configuration

To configure a SHDSL connection on your TBF device follow these steps.

Go to **Interfaces** → **Assign** → **SHDSLs** and click **Edit**.



Depending on your configuration you'll either find one or two SHDSL modems. Each modem can be configured individually. Since SHDSL connections are always point to point connections one device needs to be the *Master (CO)* and one device needs to be the *Slave (CPE)*. The Master device determines all relevant connection parameters.

Start with the configuration of your Master device. You can start with the default settings and improve your connection if necessary. First, set the desired Signal-to-Noise-Ratio (**SNR**). Reliable (but slower) connections have an SNR above 9dB while standard connections have an SNR around 6dB. For high-speed connections the SNR can be as low as 3dB. The Auto-**Bitrate** feature tests the highest available connection speed first and determines whether the SNR is sufficient. If not, it switches to the next lower speed setting and tries to make a connection again. This process can take up to 20min since each speed setting is tested for about a minute. This is also the case for already established connections. Should the signal quality drop, the device would lower the **Bitrate** one step and vice versa.

Should the Auto-**Bitrate** fail to make a connection you can still configure the connection parameters manually. Start with the modulation type (**PAM**). Smaller numbers stand for a less complex and therefore more reliable modulation. You can see the the current Signal-to-Noise-Ratio (SNR) under **Diagnostics** → **SHDSLs**.

You should also change the **Bitrate** setting to a manual speed in this case. Lower numbers stand for a slower connection speed. Find a good value pair of modulation type and bus speed that fits your **SNR** requirements.

Note: The SNRM is only measured for received data. In some cases (e.g. one lead of a cable being worse than the other) the achievable speeds can vary based on the direction you're looking at. Should one direction be faster than the other but you need more speed on the slower cable, try switching the leads.

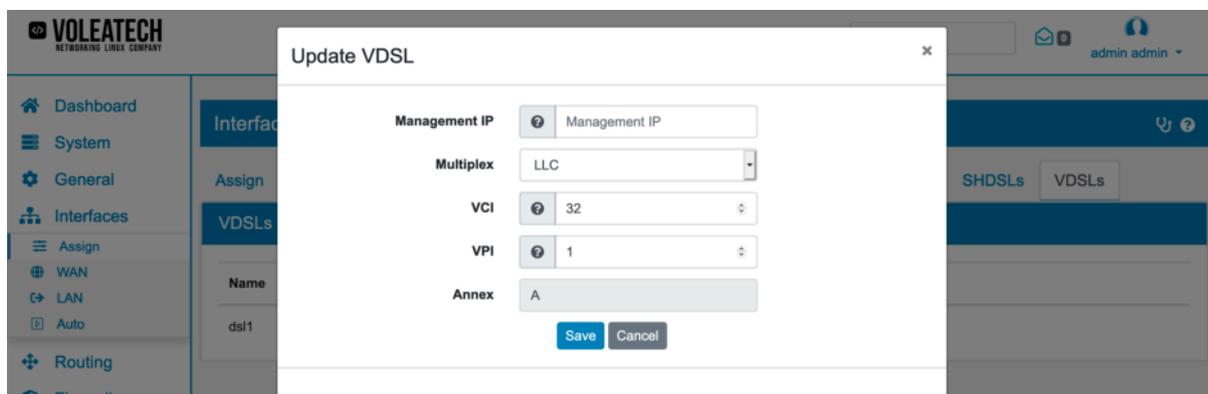
An advantage of setting your connection parameters manually is that you do not get connection outages due to the algorithm automatically changing connection speeds.

The Emergency Freeze (**EF**) feature keeps the current connection settings in case of short connection drops. This can be deactivated. The maximum drop time depends on the configured speed and can range from a few milliseconds to multiple seconds.

After you get a solid connection you can go to **Interfaces** → **Assign** and configure a new Interface based on your SHDSL modem.

10.13 VDSL

You can find the VDSL Settings at **Interfaces** → **Assign** → **VDSLs**.



VDSL stands for **Very High Speed Digital Subscriber Line** and provides data transmission over the telephone network. The following options can be changed:

Management IP of the modem is used internally to read out connection data. You can change the local ip to reach it here in case it collides with your network. It must be an IP in the range of 10.0.0.0/8.

Multiplex can be either *LLC* (Logical Link Control) or *VCMUX* (Virtual Circuit Multiplexing). Default is LLC.

VCI is the Virtual Channel Identifier and 32 by default.

VPI is the Virtual Path Identifier and 1 by default.

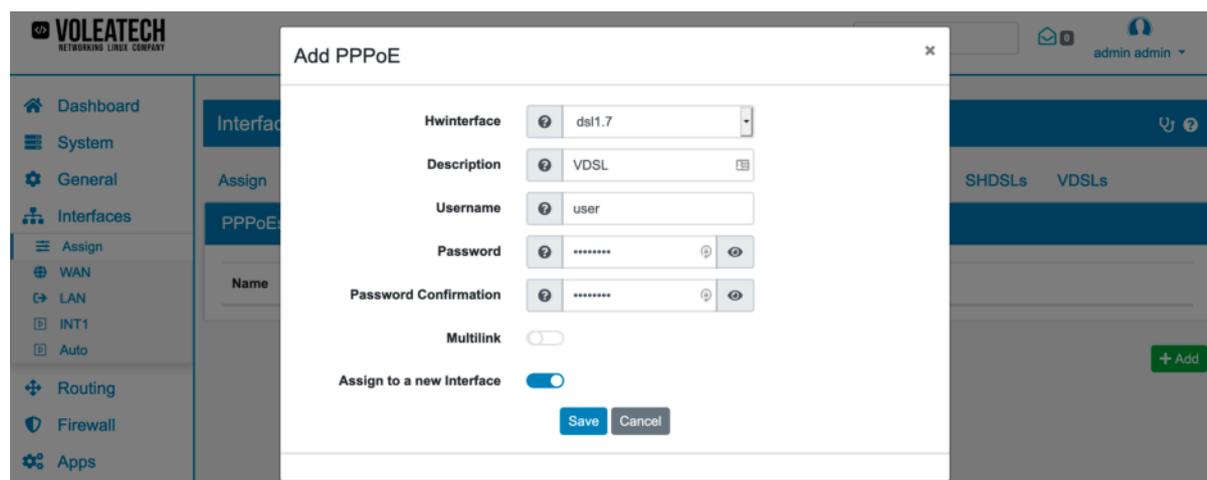
10.13.1 VDSL Configuration

To configure a VDSL connection on your TBF device you need to follow these steps.

The specific requirements for connecting to a VDSL are dependent on your ISP. Check with your ISP to find the specific configuration. In many cases ISPs require you to have a VLAN with a specific ID to connect to their VDSL service. This configuration is assumed in this tutorial.

First go to **Interfaces** → **Assign** → **VLAN**. Create a VDSL with your ISPs specific VLAN ID (e.g. 7) and either your internal VDSL modem hardware interface or your WAN hardware interface (if you have an external modem connected) as the underlying Interface. Do not enable the **Assign to new Interface** option. Click **Save**.

Next, go to **Interfaces** → **Assign** → **PPPoEs** and click **Add**. Select your newly created VLAN Interface as **Hwinterface** and enter the credentials that your ISP should have given you. Also enable the **Assign to new Interface** option and click **Save**.



You should now see a new PPPoE Interface that you can configure. Refer to [Configure Interfaces](#) for more details.

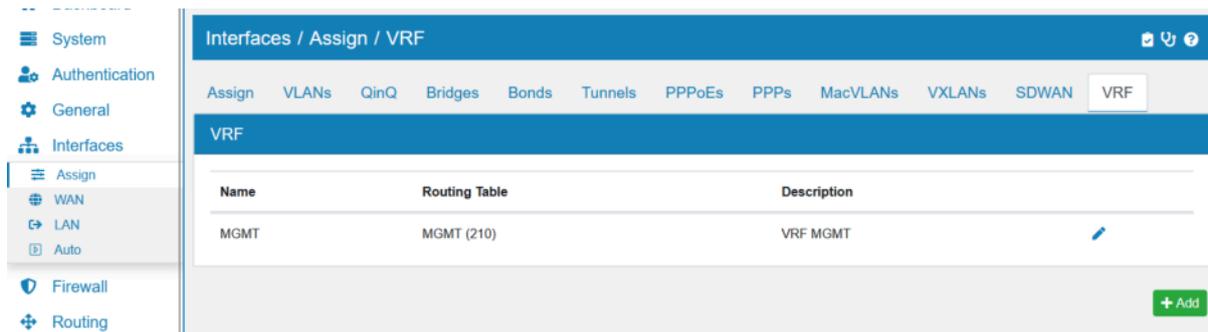
10.14 VRF

Virtual routing and forwarding (VRF) enables the simultaneous co-existence of multiple virtual routers (VRs) as instances or virtual router instances (VRIs) within the same router. It allows for a logical separation of interfaces and routes in VRF units, so they can not see each other directly. It is possible to have the same IP Adresses in different VRFs and also the same routes.

Be aware that not all TBF services are VRF aware and can be used in that case.

You can find the VRF Settings at **Interfaces** → **Assign** → **VRF**.

Virtual Routing and Forwarding (VRF) allows multiple routing table instances to co-exist within the same router at the same time.



Each VRF instance has a unique **Routing Table**. There cannot be multiple VRFs with the same Routing Table.

In the **Firewall Settings** all interfaces assigned to a VRF will show up coming from the VRF as interface. You will not be able to set Firewall Rules on each Interface separately anymore. The VRF groups all Interfaces together for the Firewall.

VRFs also allow you to create an out of band management network. For that purpose the default *MGMT* VRF is already created by default.

VRF also allows the creation of a Layer 3 VPN (**L3VPN**) in combination with our dynamic routing options.

10.15 VXLAN

You can find the VXLAN Settings at **Interfaces** → **Assign** → **VXLAN**.

Virtual Extensible LAN (VXLAN) is a network virtualization technology that attempts to address the scalability problems associated with large cloud computing deployments. It uses a VLAN-like encapsulation technique to encapsulate OSI layer 2 Ethernet frames within layer 4 UDP datagrams. VXLAN endpoints, which terminate VXLAN tunnels and may be either virtual or physical switch ports, are known as VXLAN tunnel endpoints (VTEPs)

VXLANs can only be configured on top of Physical Interfaces.

HWInterface is the underlying interface.

VXLAN ID has to be unique to identify the VXLAN.

Mode Multicast or Head End Replication. Multicast is more efficient but it has to be configured on all VTEPs. The Multicast group must be same. Head End Replication replicates all entries to all VTEPs.

Local Public IP Address that is used as the sender to connect to other VTEPs. If none is provided one will be auto used from the underlying HWInterface.

Port to use to connect to VTEPs and receive connections.

Ageing The vxlan keeps track of ethernet addresses seen. This is the timeout in seconds for members that have not been seen. Between 0 and 4096. Default is 300

Multicast Group v4 Multicast Group IPv4 **Multicast Group v6** Multicast Group IPv6. One of them is enough for a Multicast Setup.

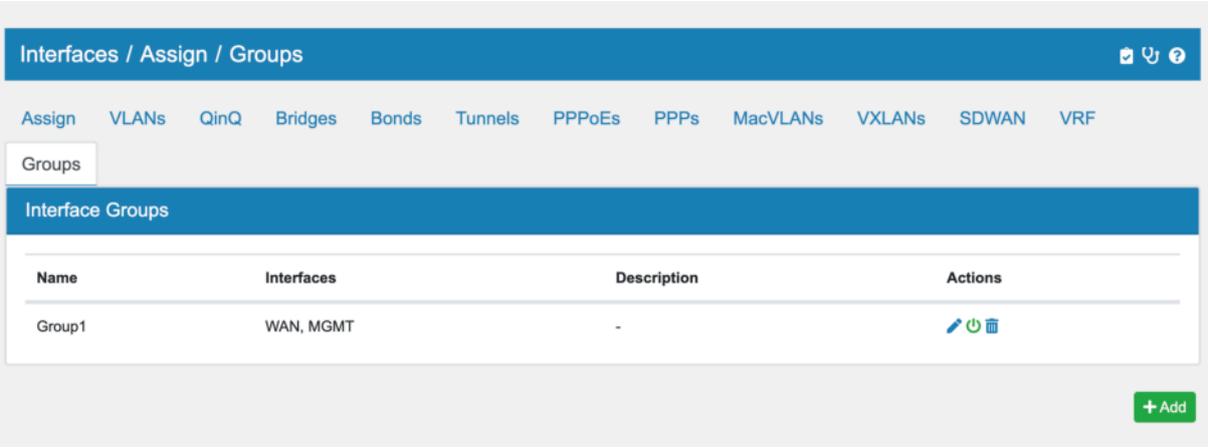
TTL Specifies the TTL value to use in outgoing packets. Between 0 and 255, 0=auto

Remote IPs remote VTEPs to connect to.

VXLANs can also be used in Bridges.

10.16 Interface Groups

You can find the Interface Groups Settings at **Interfaces** → **Assign** → **Groups**.



The screenshot shows a web interface for configuring interface groups. At the top, there is a breadcrumb trail: "Interfaces / Assign / Groups". Below this, a navigation menu includes "Assign", "VLANs", "QinQ", "Bridges", "Bonds", "Tunnels", "PPPoEs", "PPPs", "MacVLANs", "VXLANs", "SDWAN", and "VRF". The "Groups" tab is selected. The main content area is titled "Interface Groups" and contains a table with the following data:

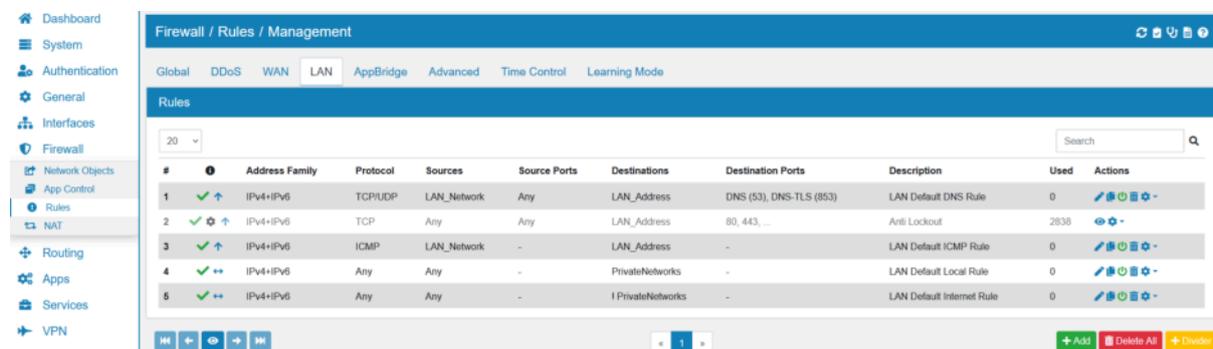
Name	Interfaces	Description	Actions
Group1	WAN, MGMT	-	  

At the bottom right of the interface, there is a green "+ Add" button.

An Interface Group is a group of interfaces. It can be used in NAT Rules that are supposed to be on multiple interfaces.

11.1 Firewall General

You can find the Firewall Rule Settings at **Firewall** → **Rules**.



We have a Video Tutorial regarding the firewall rules:

11.1.1 Stateful vs Stateless

First a small excursion on what kind of firewall TBF is. * |prodname|** is a **stateful firewall**, it keeps track of open connections and also allows them without rechecking the firewall rules.

The definition of a **stateful firewall** is:

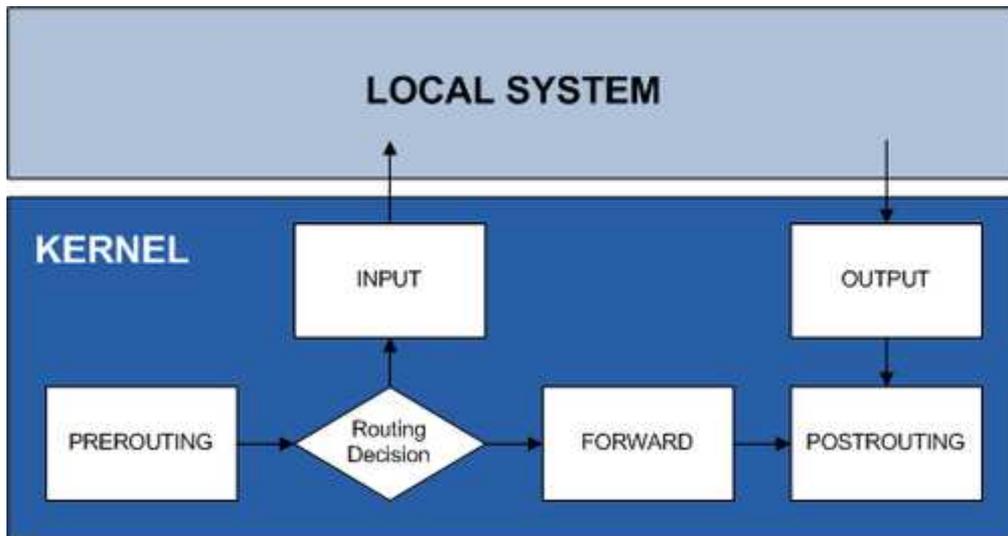
Note: In computing, a stateful firewall is a network firewall that tracks the operating state and characteristics of network connections traversing it. The firewall is configured to distinguish legitimate packets for different types of connections. Only packets matching a known active connection are allowed to pass the firewall. ([Stateful Firewall](#))

The definition of a **stateless firewall** is:

Note: Stateless firewalls watch network traffic, and restrict or block packets based on source and destination addresses or other static values. They are not 'aware' of traffic patterns or data flows. A stateless firewall uses simple rule-sets that do not account for the possibility that a packet might be received by the firewall 'pretending' to be something you asked for. ([Stateful vs Stateless Firewalls](#))

11.1.2 Firewall Flow

To better understand firewall rules it is necessary to have a look at how the system processes the rules



In different stages the following operations are performed

- PREROUTING: DNAT
- FORWARD: Firewall Rules for forwarding traffic between interfaces
- INPUT: Firewall Rules if the destination is the firewall itself (e.g. DNS Server, WebGUI)
- OUTPUT: Firewall Rules if the firewall itself is the source (answer from DNS Server, WebGUI)
- POSTROUTING: SNAT

We will look into each option throughout this chapter.

Note: **OUTPUT** is not filtered in TBF. The firewall itself can always send out everything.

Note: To match **INPUT** rules to the firewall, you need to use the Network Objects *Address* or *Network* of each Interface. It is not enough to type the IP Address of the interface as destination. The destination will be added as a forward rule and not input.

11.1.3 Firewall Processing

In TBF, the Global Firewall Rules are processed before any Interface Rule. First match wins and order matters.

11.1.4 Flowtable Bypass

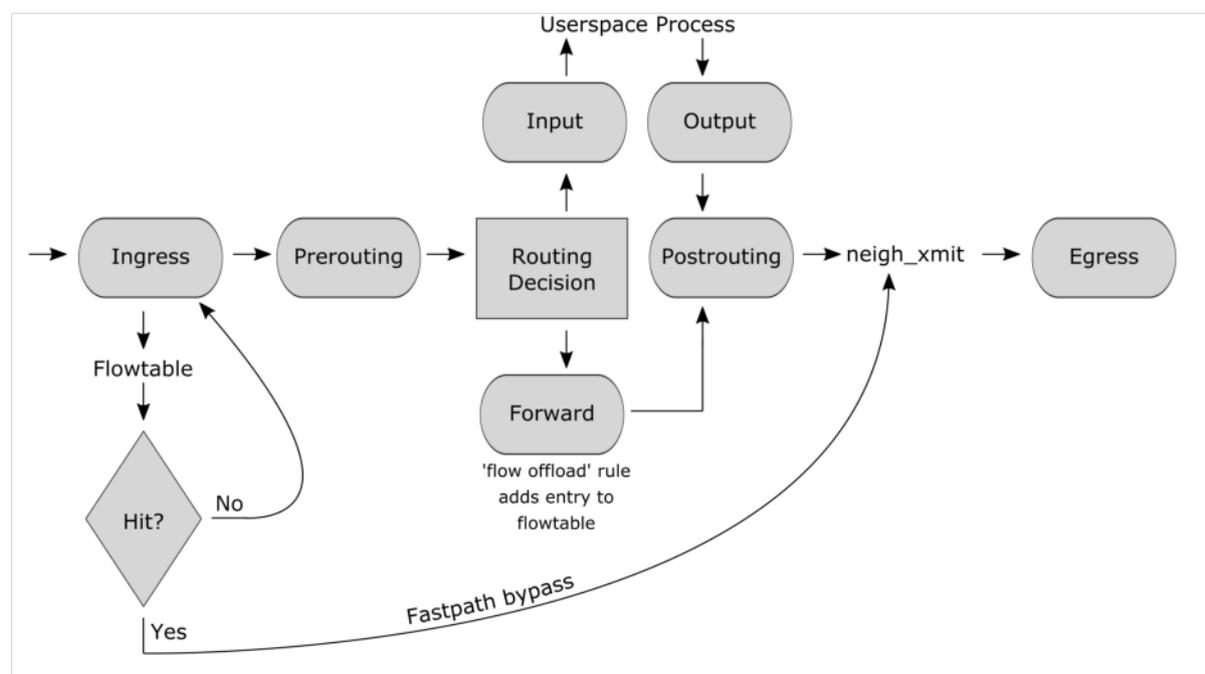


Fig. 1: Netfilter hooks and flowtable interactions

We use a feature called flowtable bypass which speeds up the firewall processing by a factor of 2. It bypasses the network stack for established connections and directly forwards traffic from the input interface to the output interface. It **only** works with stateful connections (TCP/UDP) and is activated after the first package flow is established. If a long lived connection is used flowoffload will only be active for the time actual traffic is seen. The connection will revert to a normal state when there has not been any traffic for a few minutes. The same way it will be turned back to a flowoffload when there is new traffic detected.

It is disabled for firewall rules that have logging or a limiter enabled since those features are not compatible with the flowtable bypass.

11.1.5 eXpress Data Path

Our XDP offload technology enhances the speed of the flowtable bypass by a factor of 2.5X and the normal firewall speed by 5X by utilizing the XDP and eBPF technology. Our offloader allows for established TCP/UDP connections to be forwarded directly from the network driver.

Be aware that QoS does not work when XDP is enabled and this is due to the fact that the speed improvements are only possible by bypassing any QoS logic in the TBF Firewall.

We recommend to enable XDP for the fastest possible firewall experience.

For more information, we recommend to read the manual section regarding the XDP technology [XDP Accelerator](#).

11.2 Network Objects

You can find the Network Objects Settings at **Firewall** → **Network Objects**.

An Network Object can be of one of the following types:

- Hosts (Single IPs or Hostname)
- Hosts (Network Range)
- Ports
- Mac Addresses
- DNS Domain

You can have Network Objects in Network Objects but they have to be from the same type. Adding a Mac Address Network Object to a Port Network Object does not work. You are also not allowed to create cyclic structures like creating 2 Network Objects and add each of them to the other Network Object. This structure creates a loop and is not valid.

For Hosts you can also use **hostnames** (DNS entries) instead of IP Addresses. Be aware though that it is up to the service you use the Network Object in to resolve that hostname. You can change the order of the entries inside a Network Object via drag and drop once you saved them. The order is only cosmetic and has no influence on the Network Object.

Network Objects can be used in different places like firewall rules.

Network Objects for Interface IPs, Networks and Virtual IPs are automatically generated.

11.2.1 Hosts (Single IP)

You can enter Single IPs or other Network Objects with Single IPs. They can be IPv4 or IPv6.

You can also use **hostnames** (DNS entries) instead of IP Addresses.

Builtin Hosts

Name	IPs
OSPF	<ul style="list-style-type: none"> • 224.0.0.5 • FF02::5 • 224.0.0.6 • FF02::6

11.2.2 Hosts (Network Range)

You can enter Network Ranges or other Network Objects with Network Ranges. They can be IPv4 or IPv6.

Dynamic Block Lists

Here you can enable *DBL* and enter an **URL**. The **Update Interval** can be daily or hourly. Once configured a system job will run regularly and updates Network Object Entries with the data it gets from the URL.

Builtin Network Ranges

Name	Network Range
LOOPBACK	127.0.0.0/8
RFC1918_A	10.0.0.0/8
RFC1918_B	172.16.0.0/12
RFC1918_C	192.168.0.0/16
MULTICAST	224.0.0.0/4
RFC4193	fd00::/7
PrivateNetworks	<ul style="list-style-type: none"> • RFC1918_A • RFC1918_B • RFC1918_C • RFC4193

11.2.3 Ports

You can enter Ports or other Network Objects with Ports. You can also add built in ports.

Builtin Ports

Name	Port
BGP	179
CIFS	3020
CITRIX-ICA	1494
DNS	53
DNS-TLS	853
ESP	4500
FTP	21
FTP-DATA	20
HTTP	80
HTTPS	443
IEC104	2404
IMAP	143
IMAPSSL	993
ISAKMP	500
KERBEROS	88
LDAP	389
LDAPS	636
LPD	515
MODBUS	502
NETBIOS-SSN	139
NFS	2049
OPENVPN	1194

continues on next page

Table 1 – continued from previous page

Name	Port
POP3	110
POP3S	995
PPTP	1723
RADIUS	1812
RADIUS-ACCT	1813
RSH	514
RTSP	554
SIP	5060
SIP-TLS	5061
SMTP	25
SMTPTLS	465
SMTPSSL	587
SNMP	161
SNMPTRAP	162
SQLNET	1522
SSH	22
TELNET	23
UUCP	540
WHOIS	43

11.2.4 Mac Addresses

You can also create Mac Address Network Objects. They are only used for source Mac Addresses in Firewall Rules. For Mac Addresses you can also use **Dynamic Block Lists** like described above. Be careful to use those as the source Mac Address is changed by L3 Routers.

11.2.5 DNS Domain

You can also create DNS Domain Network Objects. Three different types are supported:

- Direct Subdomains (*.test.de)
- All Subdomains (**.test.de)
- Exact Match (www.test.de)

It is usually not possible to query all subdomains since most DNS servers do not allow zone transfers and therefore will not allow crawling all subdomains. The TBF Firewall will automatically learn the subdomains by observing the answers in the builtin DNS Server. Direct subdomains will only observe first level subdomains so *www.test.de* will be observed but not *test.www.test.de*. The results are limited to 256 entries at which point the oldest entry will be removed and replaced by a newer one.

It is therefore important, that all clients behind the firewall use the firewalls *DNS* Server and not a third party DNS server. For the same reason, DNS Domain Network Objects can only be used as *Destination* in Global and Interface Firewall Rules.

The DNS Domain allows for dynamic adding of wildcard domains to firewall rules by observing DNS results.

11.3 Firewall Rules (Forward and Input)

Firewall Rules are the core of the TBF Firewall. When you open the Rules site you can see that Firewall Rules are grouped by interface. The interface is the **incoming interface**, meaning the interface the traffic enters the firewall first.

For example if your computer is behind LAN and the internet behind WAN and you are going to visit a website, then the traffic originates from your computer and enters the firewall on the LAN interface first. A firewall rule to allow the traffic has to be defined on LAN. A backwards rule is not necessary, since the firewall will create a state which will keep track of the open connection. The backwards connection from the WAN to LAN is implied and allowed.

There are also *Global Firewall Rules (Forward and Input)* which are more flexible and have the option to set the incoming and outgoing interface or set them to any.

#	Address Family	Input Interfaces	Output Interfaces	Protocol	Sources	Source Ports	Destinations	Destination Ports	Description	Used	Actions
1	IPv4	WAN	All	Any	Any	-	225.0.0.50	-	Contrackd Sync Rule	0	ⓘ ⚙️
2	IPv4+IPv6	Localhost	All	VRRP	Any	-	224.0.0.18, fe02::12	-	VRRP Rule	0	ⓘ ⚙️
3	IPv4+IPv6	All	All	VRRP	Firewall_Addresses	-	224.0.0.18, fe02::12	-	VRRP Self Rule	0	ⓘ ⚙️
4	IPv4	LAN	All	UDP	Any	Any	Any	67	DHCP Server IPv4 Rule	0	ⓘ ⚙️
5	IPv6	Localhost	All	UDP	Any	Any	Any	547	DHCP Server IPv6 Rule	0	ⓘ ⚙️
6	IPv4+IPv6	Localhost	All	OSPF	Any	-	Any	-	OSPF Rule	0	ⓘ ⚙️

On each Firewall Rule page you will see the builtin rules with a gray background. You can not change them or move them. Only user created rules can be changed.

You can export the settings in the top right corner as an Excel spreadsheet.

11.3.1 Move Rules

Rules are grouped by interface and are paged in groups of 20 rules. You can drag and drop user created rules to a different position and you can save that position by pressing save on the bottom navigation. You can also move a rule to the next or previous page or the first or last page if you mark the rule on the left (click on the first cell of the firewall rule) and use the arrows on the bottom left. If you hover over the buttons they will also show you their description.

11.3.2 Delete All

Rules can be deleted per Interface or Selected Tab in the GUI. Press the *Delete All* Button in the lower right corner to delete all rules. Please be careful, the rules can not be recovered after deletion. If you already marked a firewall rule then only that rule can be deleted and not all rules. *Deleted Rules* do not close already active connections. Please go to *States* to close already active connections.

11.3.3 Create and Update Rules

If you click **Add** you will create a new rule on the current interface where you are. You have various options for the rule to set and the rules are structured by the following sections:

- General Settings
- ICMP Settings
- Sources
- Destinations
- Advanced

The screenshot shows the 'Firewall / Rules / Create' page. The left sidebar contains navigation links: Dashboard, System, General, Interfaces, Routing, Firewall, Aliases, Rules (selected), NAT, Apps, Services, VPN, Tools, and Diagnostics. The main content area is titled 'Firewall / Rules / Create' and has a 'General Settings' section. The settings are as follows:

Enabled	<input checked="" type="checkbox"/>
Add Rule To	<input type="radio"/> Top <input checked="" type="radio"/> Bottom
Interface	LAN
Action	Accept
Address Family	IPv4+IPv6
Protocol	Any
Description	Description

Below the 'General Settings' section is a 'Sources' section. At the bottom of the page, there is a copyright notice: © Voleatech GmbH 2017 - 2020.

11.3.4 Used Rules

On every Firewall Rule page you can see how often a Firewall Rule was used. If you hover over the number, you can also see the total amount of states as well as the active ones. It also shows, how many packets were affected by the rule and their size in bytes.

Description	Used	Actions
Test	Total: 2841 Active: 2836 Packets: 1236 Bytes: 3.39 MB	    
LAN Default DNS Rule		    
Anti Lockout	2841	 
LAN Default ICMP Rule	0	    
LAN Default Local Rule	0	    
LAN Default Internet Rule	0	    

General Settings

You can change the following options here:

Enabled Enable or Disable the rule

Interface You can change the Interface of this rule. It will be added to the end of the rule list of that interface if you change it.

Action We have three actions defined here:

- Accept
- Drop (Silently drops the package)
- Reject (Send back a reject ICMP message)

Address Family Is either IPv4, IPv6 or both. Depending on the sources and destinations you define the system might not generate a rule for both if you choose IPv4+IPv6.

Protocol The Layer 2 Protocol of the rule.

ICMP Settings

If you choose ICMP as protocol you can also filter by ICMP Type here.

Sources

The Source setting has options for the **Source IPs**, **Source Mac Addresses** and if applicable **Source Ports**. You can also use **hostnames** (DNS entries) instead of Source IPs. You can add multiple entries of each and also mix IPv4 and IPv6. The system will figure out the rule for you.

Source Mac Addresses and **Source Ports** can be found under **Advanced Source Settings**.

The **Invert IP Match** option will invert IPs and Macs as well as the ports.

Destinations

The Destination setting has options for the **Destination IPs** and if applicable **Destination Ports**. You can also use **hostnames** (DNS entries) instead of Destination IPs. You can add multiple entries of each and also mix IPv4 and IPv6. The system will figure out the rule for you.

Note: To match **INPUT** rules to the firewall, you need to use the Network Objects *Address* or *Network* of each Interface. It is not enough to type the IP Address of the interface as destination. The destination will be added as a forward rule and not input.

The **Invert IP Match** option will invert IPs as well as the ports.

Be aware that due to the structure in *Firewall Flow* you have to explicitly choose the Interface IP Network Object if you want the destination to be the firewall itself. Custom IPs or Network Objects are not recognized.

Advanced

In the Advanced Settings you can configure a couple of extra options.

Logging You can log the rules traffic, it will log the initial packet that is seen when the state is created or the connection started.

Force Input Rule This option will make this rule an Input rule so the firewall is the destination with whatever IP you set in the destination field. Usually TBF will try and figure out if it needs to put the rule into Input or Forward or both. This will override the detection and only put the Rule in Input.

Stateless If set no state is created for this connection. You **must** create a second rule for the return traffic. This is mostly needed for asymmetric routing.

Trace To show packets that match this rule in real time enable the trace option. The trace will make the processing of the rule slower but you can debug problems. Disable the trace after debugging. The matching packets can be seen in *Trace*.

Limit Limit the rule. You can set for how many matches the rule should be active for a given time. It can be a speed (KBit/MBit/Byte/KByte/MByte) or time in packages per second/minute/hours. Please also refer to *QoS* for more explanations.

TCP Flags If the protocol is TCP you can also filter by TCP Flags.

TCP MSS If the protocol is TCP you can also set the MSS. This might be necessary if the MTU is smaller than usual. This setting is also available on a per Interface basis in the Interface Settings.

Routing Table Choose a different Routing Table for matches. The main routing table is used by default. This allows for *Policy Routing*. Matching traffic will use the selected routing table.

Routing Table Reverse Main Use the Main Routing Table for the reverse direction of the connection. This is needed for Policy Routing as the local LAN route is in the main routing table. In that case the reverse direction is WAN to LAN.

Bypass IDS/App Control The matching traffic will not be inspected by the Intrusion Detection/App Detection engine.

QoS Class Input The class used for input shaping on any interface this traffic is passing and that has QoS enabled. Be aware that the directions must be assigned accordingly. If you create a rule on LAN to be shaped on WAN, make sure that QoS is active on WAN and you pick the correct class that you want to have for WAN. Unlike QoS Output, QoS Input can only be configured for non Bridge members.

QoS Class Output The class used for output shaping on any interface this traffic is passing and that has QoS enabled. If you create a rule on LAN to be shaped on WAN, make sure that QoS is active on WAN and you pick the correct class that you want to have for WAN.

DSCP Types Differentiated services code point (DSCP) for QoS in the IP or IP6 Header. You can match the different types with this option. The option is only matched when a new firewall state is created on the first packet of the connection. Afterwards any change of the DSCP Type is not recognized for an open firewall state.

Time Control The firewall rule will only be active during that time. You need to create time objects in the *Advanced Settings* first.

Raw Data The Raw Data will be appended to the generated firewall rule. Please be careful as wrong input will prevent the firewall rules from being loaded. Please refer to the nftables syntax for the format.

Changes

At the bottom of each rule you can see the **Created date**, **Modified date** and the user that last modified the rule **Modified user**.

11.3.5 Hostnames in Rules

We support hostnames in rules as destination or source. Be aware though that they **MUST** be resolvable when the firewall rules are loaded, applied or reapplied. The firewall rules **CAN NOT** be updated, if there is no working DNS. The reload will fail and leave the old ruleset in place.

11.3.6 Search

In the top right corner of the overview page you can search for rules. As search value you can use protocol, source, destination, IP address, port or description.

11.3.7 Convert Firewall Rules

In the actions column on the right side of the overview page you can convert firewall rules. You can convert a *Global Firewall Rule* to an *Interface Firewall Rule* and vice versa. When converting a *Global Firewall Rule* a popup dialog will let you select an interface.

11.3.8 TCPCDump

In the actions column on the right side of the overview page you can start a TCPCDump for a firewall rule. A popup window will appear and show the result in realtime.

11.3.9 Trace

In the actions column on the right side of the overview page you can start a Trace for a firewall rule. A popup window will appear and show the result in realtime. The window will only show data when a packet is matching for the first time, otherwise it will stay empty.

11.4 Global Firewall Rules (Forward and Input)

Firewall Rules are the core of the TBF Firewall. When you open the Rules site you can see that Firewall Rules are grouped by interface. The global firewall rules can be found under **Global**.

#	Address Family	Input Interfaces	Output Interfaces	Protocol	Sources	Source Ports	Destinations	Destination Ports	Description	Used	Actions
1	IPv4	WAN	All	Any	Any	-	225.0.0.50	-	Contrackid Sync Rule	0	ⓘ ⚙
2	IPv4+IPv6	Localhost	All	VRRP	Any	-	224.0.0.18, fe02::12	-	VRRP Rule	0	ⓘ ⚙
3	IPv4+IPv6	All	All	VRRP	Firewall_Addresses	-	224.0.0.18, fe02::12	-	VRRP Self Rule	0	ⓘ ⚙
4	IPv4	LAN	All	UDP	Any	Any	Any	67	DHCP Server IPv4 Rule	0	ⓘ ⚙
5	IPv6	Localhost	All	UDP	Any	Any	Any	547	DHCP Server IPv6 Rule	0	ⓘ ⚙
6	IPv4+IPv6	Localhost	All	OSPF	Any	-	Any	-	OSPF Rule	0	ⓘ ⚙

The main difference between a normal firewall rule and the global firewall rule is that the global firewall rule has no fixed interface. You can configure the input and output interface of the rule.

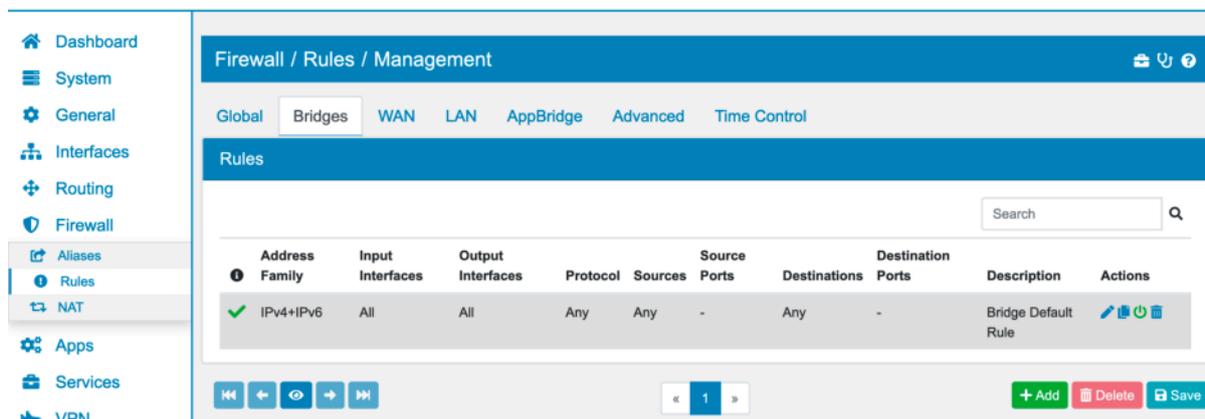
Global firewall rules are processed **before** interface firewall rules. If you have a match here the other rules will not be looked at. The firewall rule flow stops here.

The other settings are equivalent to normal firewall rules. Please have a look at [Firewall Rules \(Forward and Input\)](#) for a detailed explanation.

In the top right corner of the overview page you can **search** for rules. As search value you can use protocol, source, destination, IP address, port or description.

11.5 Bridge Firewall Rules (Forward)

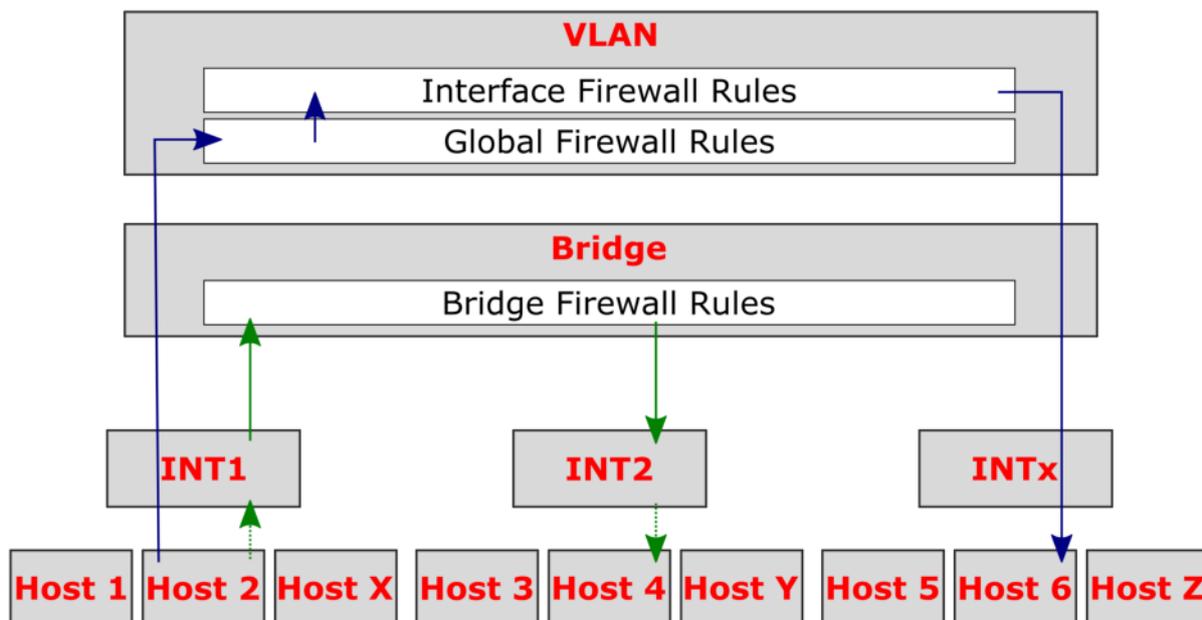
Bridge Firewall Rules are a special case of Firewall Rules. When you create a bridge interface a new **Bridges** Tab will be shown in the Firewall Rules page.



The main difference between a normal firewall rule and the bridge firewall rule is that you filter in the bridge itself. The bridge can have traffic that does not go to the host and is by default simply forwarded (green path in figure below). Bridge forwarding is done in a special path that is not the same as the normal forwarding in TBF. Bridge Firewall Rules only apply to traffic that is being forwarded.

The Global rules do not apply for bridge traffic unless you created a VLAN Interface on top of the bridge (blue path in figure below). A bridge can have multiple VLANs though and with Bridge Firewall Rules you can also match traffic that is not in a VLAN Interface.

You need to either select the bridge interface itself or bridge member interfaces as Input and Output Interface for this rule.



In HA Setups you need to make sure that the interface names are the same on both ends or exclude the rules from hasync or the sync will fail.

The settings are equivalent to normal firewall rules but they do not have advanced settings like limiter or routing table since routing is done in L2. Please have a look at *Firewall Rules (Forward and Input)* for a detailed explanation.

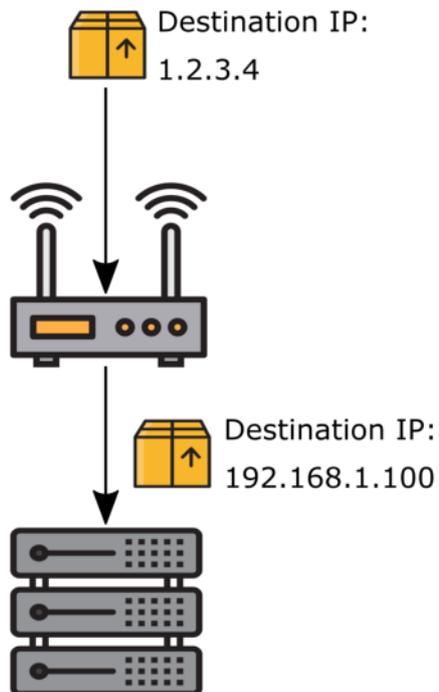
In the top right corner of the overview page you can **search** for rules. As search value you can use protocol, source, destination, IP address, port or description.

11.6 DNAT (Prerouting)

DNAT or Destination NAT is responsible for changing the Destination IP Address of a Network Packet. It is the first rule that is processed in TBF when a new Network Packet arrives at the firewall.

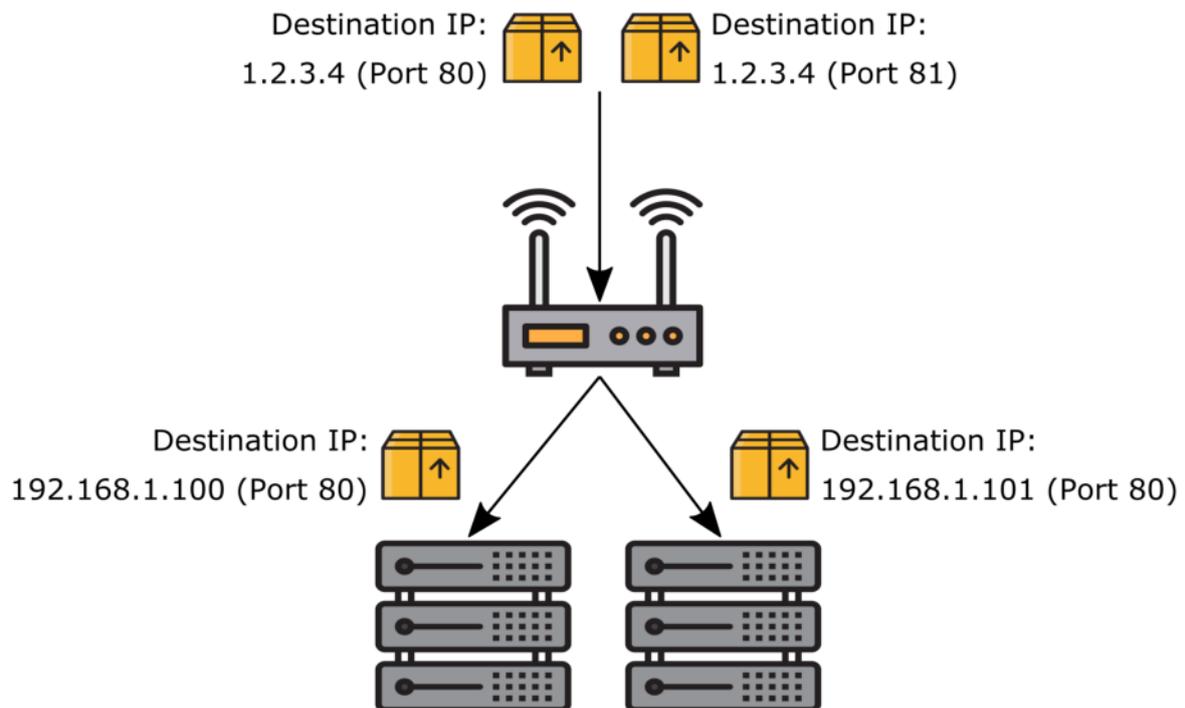
With DNAT you can do Port Forwarding or Host Forwarding. DNAT rewrites the destination of the Network Packet to the host you want it to be forwarded to.

Typical applications include the redirection of traffic from a single public IP address to a single private IP address within the private network. By doing this it becomes possible to connect to a single host from outside your local network that would otherwise be hidden. Other applications include the translation of an IP address range if you have multiple hosts you want to connect to.



This image was created with icons by [srip](#) and [Good Ware](#) from [Flaticon](#).

In a port forwarding scenario it is also possible to expand the mentioned scenarios by specific source and destination ports. That way you can have multiple servers running similar services on a single public IP address (separated by differing public ports) for example.



This image was created with icons by [srip](#) and [Good Ware](#) from [Flaticon](#).

You can find the DNAT Rule Settings at **Firewall** → **NAT**.

You will find 3 Tabs here Inbound (DNAT), Outbound (SNAT) and Both (BiNAT).

Click on DNAT to get to the rules.

11.6.1 Move DNAT Rules

Rules are grouped by interface and are paged in groups of 20 rules. You can drag and drop user created rules to a different position and you can save that position by pressing save on the bottom navigation. You can also move a rule to the next or previous page or the first or last page if you mark the rule on the left (click on the first the cell of the firewall rule) and use the arrows on the bottom left. If you hover over the buttons they will also show you their description.

11.6.2 Create and Update DNAT Rules

If you click **Add** you will create a new dn timer rule on the current interface where you are. You have various options for the rule to set and the rules are structured by the following sections:

- General Settings
- Sources
- Destinations
- NAT Settings
- Advanced

General Settings

You can change the following options here:

Enabled Enable or Disable the rule

Interface You can change the Interface of this rule. It will be added to the end of the rule list of that interface if you change it.

Address Family Is either IPv4, IPv6 or both. Depending on the sources and destinations you define the system might not generate a rule for both if you choose IPv4+IPv6.

Protocol The Layer 2 Protocol of the rule.

Sources

The Source setting has options for the **Source IPs** and if applicable **Source Ports**. You can add multiple entries of each and also mix IPv4 and IPv6. The system will figure out the rule for you.

Source Ports can be found under **Advanced Source Settings**.

The **Invert IP Match** option will invert IPs and Macs as well as the ports.

Destinations

The Destination setting has options for the **Destination IPs** and if applicable **Destination Ports**. You can add multiple entries of each and also mix IPv4 and IPv6. The system will figure out the rule for you.

The **Invert IP Match** option will invert IPs as well as the ports.

Be aware that due to the structure in *Firewall Flow*, you have to explicitly choose the Interface IP Network Object if you want the destination to be the firewall itself. Custom IPs or Network Objects are not recognized.

The destination is the **original** address where the package arrives and not the address where you want it to be forwarded to.

NAT Settings

You can configure the **Redirect IP** and if applicable the **Redirect Port**. This is the destination that the traffic should be forwarded/redirected to. The firewall will change the destination of the Network Packet to this address/port.

Be aware that you also need a firewall rule on the Interface where the traffic originates so it is allowed to go to the **Redirect IP**. The option **Associate Firewall Rule** will create one for you.

If you need a **SNAT Rule** associated with the DNAT Rule, the option **Associate SNAT Rule** will create and update a rule for you.

NAT Reflection is the option so your internal network will also be included in the DNAT. It is advisable to use a NAT Override instead because this will be slower. The traffic has to leave and reenter the firewall with this option instead of going directly to the Redirect IP.

If *NAT Reflection* is enabled you can also choose the Netmask of a Redirect IP in order to generate a NAT Reflection rule that matches the traffic of the same subnet. This is necessary to create a proper SNAT Rule for such traffic or *NAT Reflection* will not work properly.

Advanced

In the Advanced Settings you can configure a couple of extra options.

Logging You can log the rules traffic and also add a prefix so you can find it easier. Be aware that firewall logging is an expensive operation and generates a lot of log entries.

Routing Table Choose a different Routing Table for matches. The main routing table is used by default.

Changes

At the bottom of each rule you can see the **Created date**, **Modified date** and the user that last modified the rule **Modified user**.

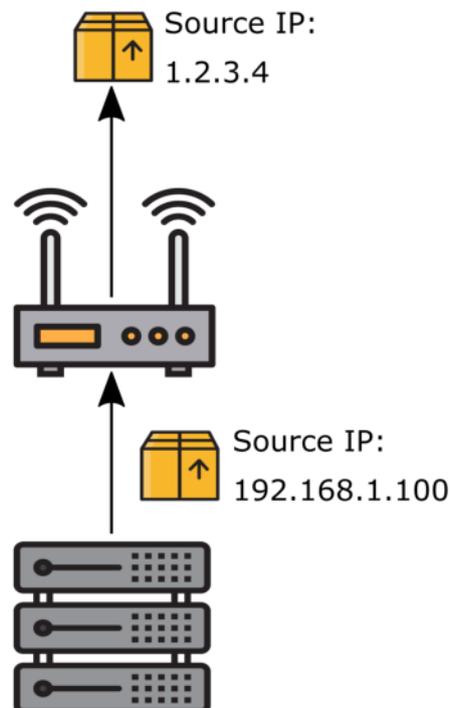
11.6.3 Search

In the top right corner of the overview page you can search for rules. As search value you can use protocol, source, destination, IP address, port or description.

11.7 SNAT (Postrouting)

SNAT or Source NAT is responsible for changing the Source IP Address of a Network Packet. It is the last rule that is processed in TBF when a new Network Packet arrives at the firewall.

With SNAT you can masquerade the sender of the Network Packet. SNAT rewrites the source of the Network Packet to the IP you choose.



This image was created with icons by [srip](#) and [Good Ware](#) from [Flaticon](#).

By default traffic coming from your local network and going to a destination outside of your network will be given a new source IP reflecting your WAN IP. However this is not always the desired behaviour.

In High Availability setups for example a shared virtual WAN address must be used. Refer to [Setup Examples](#) for further details on this.

Interface	Address Family	Protocol	Sources	Source Ports	Destinations	Destination Ports	Translation IP	Translation Port	Description	Actions
WAN	IPv4+IPv6	Any	PrivateNetworks	-	Any	-	WAN_Address	-	SNAT WAN (Private Networks)	

You can find the SNAT Rule Settings at **Firewall** → **NAT**.

You will find 3 Tabs here Inbound (DNAT), Outbound (SNAT) and Both (BiNAT).

Click on SNAT to get to the rules.

11.7.1 Move SNAT Rules

Rules are grouped by interface and are paged in groups of 20 rules. You can drag and drop user created rules to a different position and you can save that position by pressing save on the bottom navigation. You can also move a rule to the next or previous page or the first or last page if you mark the rule on the left (click on the first the cell of the firewall rule) and use the arrows on the bottom left. If you hover over the buttons they will also show you their description.

11.7.2 Create and Update SNAT Rules

If you click **Add** you will create a new dn timer rule on the current interface where you are. You have various options for the rule to set and the rules are structured by the following sections:

- General Settings
- Sources
- Destinations
- NAT Settings
- Advanced

General Settings

You can change the following options here:

Enabled Enable or Disable the rule

Interface You can change the Interface of this rule. It will be added to the end of the rule list of that interface if you change it.

No NAT This will exclude a match of this rule from SNAT. It might be useful for exceptions.

Address Family Is either IPv4, IPv6 or both. Depending on the sources and destinations you define the system might not generate a rule for both if you choose IPv4+IPv6.

Protocol The Layer 2 Protocol of the rule.

Sources

The Source setting has options for the **Source IPs** and if applicable **Source Ports**. You can add multiple entries of each and also mix IPv4 and IPv6. The system will figure out the rule for you.

Source Ports can be found under **Advanced Source Settings**.

The **Invert IP Match** option will invert IPs and Macs as well as the ports.

Destinations

The Destination setting has options for the **Destination IPs** and if applicable **Destination Ports**. You can add multiple entries of each and also mix IPv4 and IPv6. The system will figure out the rule for you.

The **Invert IP Match** option will invert IPs as well as the ports.

NAT Settings

You can configure the **Translation IP** and if applicable the **Translation Port**. This is the address that the traffic will be rewritten to. The firewall will change the source of the Network Packet to this address/port.

By default TBF will select a random port for the traffic. This is not useful in all situations. Some protocols depend on a static port like VOIP. Enable that option to use a static port.

Advanced

In the Advanced Settings you can configure a couple of extra options.

Logging You can log the rules traffic and also add a prefix so you can find it easier. Be aware that firewall logging is an expensive operation and generates a lot of log entries.

Routing Table You can apply this SNAT Rule to traffic using the specified routing table. The traffic must be matched by a firewall rule first that sets the routing table for the connection.

Input Interface You can set the input interface of the packet to match.

Changes

At the bottom of each rule you can see the **Created date**, **Modified date** and the user that last modified the rule **Modified user**.

11.7.3 Search

In the top right corner of the overview page you can search for rules. As search value you can use protocol, source, destination, IP address, port or description.

11.8 BiNAT (Prerouting + Postrouting)

BiNAT is responsible for changing the Source and Destination IP Address of a Network Packet. It is DNAT and SNAT combined.

It will only work for a 1:1 mapping of an host to another IP Address.

You can find the BiNAT Rule Settings at **Firewall** → **NAT**.

You will find 3 Tabs here Inbound (DNAT), Outbound (SNAT) and Both (BiNAT).

Click on BiNAT to get to the rules.

11.8.1 Move BiNAT Rules

Rules are grouped by interface and are paged in groups of 20 rules. You can drag and drop user created rules to a different position and you can save that position by pressing save on the bottom navigation. You can also move a rule to the next or previous page or the first or last page if you mark the rule on the left (click on the first the cell of the firewall rule) and use the arrows on the bottom left. If you hover over the buttons they will also show you their description.

11.8.2 Create and Update BiNAT Rules

If you click **Add** you will create a new dnatt rule on the current interface where you are. You have various options for the rule to set and the rules are structured by the following sections:

- General Settings
- Destinations
- NAT Settings
- Advanced

General Settings

You can change the following options here:

Enabled Enable or Disable the rule

Interface You can change the Interface of this rule. It will be added to the end of the rule list of that interface if you change it.

Address Family Is either IPv4, IPv6 or both. Depending on the sources and destinations you define the system might not generate a rule for both if you choose IPv4+IPv6.

Destinations

The Destination setting has options for the **Destination IPs**. The destination is the IP that the internal host is mapped to. It is usually an IP on the Firewall e.g. a WAN virtual IP.

NAT Settings

You can configure the **Redirect IP** here. This is the address that the traffic will be rewritten/forwarded to. It is the internal IP of a host that is associated with the Destination.

If *NAT Reflection* is enabled you can also choose the Netmask of a Redirect IP in order to generate a NAT Reflection rule that matches the traffic of the same subnet. This is necessary to create a proper SNAT Rule for such traffic or *NAT Reflection* will not work properly.

Advanced

In the Advanced Settings you can configure a couple of extra options.

Logging You can log the rules traffic and also add a prefix so you can find it easier. Be aware that firewall logging is an expensive operation and generates a lot of log entries.

Changes

At the bottom of each rule you can see the **Created date**, **Modified date** and the user that last modified the rule **Modified user**.

11.8.3 Search

In the top right corner of the overview page you can search for rules. As search value you can use protocol, source, destination, IP address, port or description.

11.9 Firewall Rules Advanced

You can find the Advanced Settings at **Firewall** → **Rules** → **Advanced**.

The screenshot displays the 'Firewall / Rules / Advanced' configuration page. The left sidebar lists various system settings, with 'Rules' selected. The main content area shows three rule configurations:

- Geo Blocking:** Enabled (toggle), Update Interval: Weekly (dropdown).
- Office 365:** Enabled (toggle), Update Interval: Weekly (dropdown).
- Amazon Web Services:** Enabled (toggle), Update Interval: Weekly (dropdown).

The footer of the page indicates '© Voletech GmbH 2017 - 2022'.

11.9.1 Geo Blocking

Enabling Geo Blocking will download the Geo IP List (IPv4 + IPv6) and generate Network Objects with IPs for each country and continent that you can use in Firewall Rules. This helps with filtering/blocking IP addresses from specific countries/regions.

Update Interval is set to weekly by default and can be changed to daily or monthly.

This product includes GeoLite2 data created by MaxMind, available from <http://www.maxmind.com>.

11.9.2 Office 365

Enabling Office 365 will download the Office 365 IP List (IPv4 + IPv6) and generate Network Objects with IPs for each service that you can use in Firewall Rules. The available services to choose from are: *All, Exchange, Skype, Sharepoint* and *Common*.

Update Interval is set to weekly by default and can be changed to daily or monthly.

You can find more information about the ipranges at <http://aka.ms/ipurlws>.

11.9.3 Amazon Web Services

Enabling Amazon Web Services will download the Amazon Web Services IP List (IPv4 + IPv6) and generate Network Objects with IPs for each service that you can use in Firewall Rules.

Update Interval is set to weekly by default and can be changed to daily or monthly.

You can find more information about the aws ipranges at <https://docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html>.

11.9.4 Google

Enabling Google will download the Google IP List (IPv4 + IPv6) and generate one Network Object for all Google IPs.

Update Interval is set to weekly by default and can be changed to daily or monthly.

11.9.5 Miscellaneous

Reload Firewall can be enabled or disabled. When enabled it will reload Firewall Rules if a hostname is used that needs to be resolved to an IP.

Reload Firewall Interval is the Reload Firewall Interval in hours. Default is 24.

Rules Default Page defines the default landing page for Firewall > Rules.

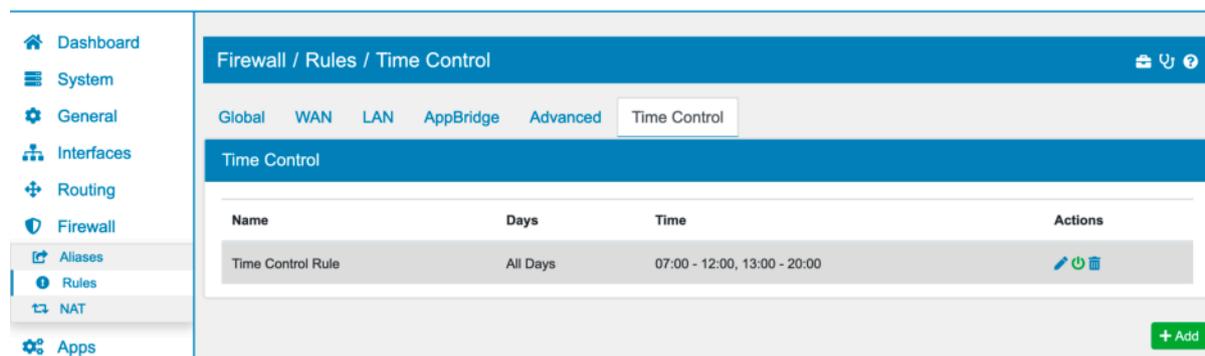
Firewall Default Policy can be either drop or accept. It is drop by default.

11.9.6 Custom Rules

Custom nftables rules can be defined here, one per line. They must match the nftables syntax and they will be imported before any rule of the WebGUI is added. Please be careful as syntax errors will lead to errors on loading the firewall rules and no new rules can be added.

11.10 Firewall Time Control

You can find the Time Control at **Firewall** → **Rules** → **Time Control**.



11.10.1 Time Control

You can create Time Control blocks that can be used in Firewall Rules. Each Time Control block has days and hours associated with it.

You can use them to block or allow traffic in firewall rules, the entire firewall rule will only be evaluated within the time range defined.

Be aware that open states from the firewall rules will not be auto closed outside of the time range. Only new connections are affected by this.

11.11 App Control

You can find the App Control Settings at **Firewall** → **App Control**.

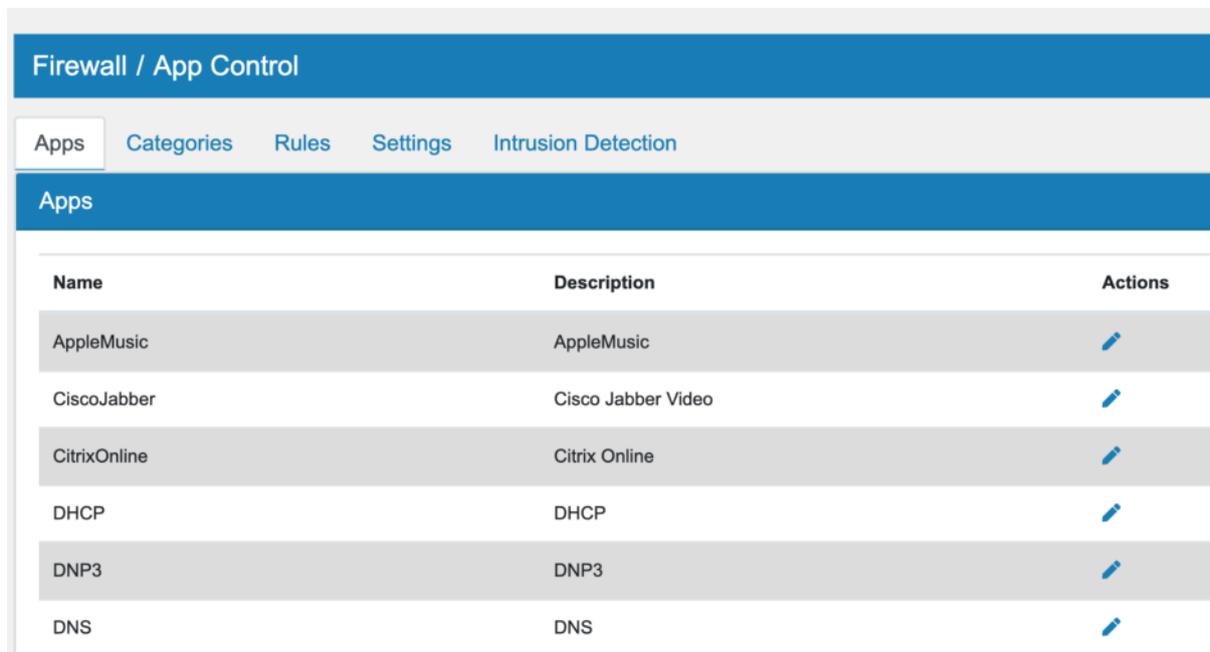
Traditional firewall rules, which only identify ports, protocols and IP addresses, cannot identify and control applications. App Control allows you to define and use Application Definitions and Signatures to define Firewall Rules that are based on Layer 7 attributes.

App Control is based on the Intrusion Detection system. The Intrusion Detection System has to be enabled in order for App Control to work. The Settings of App Control presents some of the same options as the Intrusion Detection Settings. Both change the same settings.

11.11.1 Apps

There are several Apps predefined in the System. You can click on *Edit* to show their definition in the System.

Note: If you are missing an App or have suggestions for Apps, please write us an email. We are happy to add new Apps.



The screenshot shows the 'Firewall / App Control' interface. At the top, there is a blue header with the text 'Firewall / App Control'. Below this, there is a navigation bar with tabs for 'Apps', 'Categories', 'Rules', 'Settings', and 'Intrusion Detection'. The 'Apps' tab is selected. Below the navigation bar, there is a blue header with the text 'Apps'. The main content area displays a table with three columns: 'Name', 'Description', and 'Actions'. The table lists several predefined apps, each with an edit icon in the 'Actions' column.

Name	Description	Actions
AppleMusic	AppleMusic	
CiscoJabber	Cisco Jabber Video	
CitrixOnline	Citrix Online	
DHCP	DHCP	
DNP3	DNP3	
DNS	DNS	

Defining new Apps can be done by adding new Apps. Since most applications are based on HTTP or HTTPS the GUI presents three predefined options. You can always use the custom option to define custom rules that are not covered by the GUI options. We refer to the [Suricata Manual](#) for this case.

Name has to be unique for the applications

Description can be a user defined string

AppType is one of HTTP, SSL/TLS (HTTPS), Web or JA3. *JA3* defines a unique string of the encryption parameters of an SSL/TLS connection. The JA3 is tied to the specific encryption parameters used for a server or client. This is most useful for fixed clients where the options never change. A JA3 hash is also shown for a *flow* in the logfiles for each established connection. *Web* will create a combined HTTP and SSL/TLS field matching the Host and SNI field.

Option for HTTP, SSL/TLS or JA3 shows you different fields that can be searched for inside a connection. For TLS/SSL you can for example match against the SNI or certificate fields of the connection. After the initial connection handshake no further information can be obtained by encrypted connections.

Content for the content to match against.

Offset in order to make the match faster an offset into the selected option field can be set. Otherwise the entire fields content is searched.

Case Insensitive by default content matches are case sensitive. The options changes that.

Data Check opens up more options for additional options to match inside data.

Is Data At checks if there are more data at the given position.

Is Data At Negation makes the *Is Data At* field a NOT *Is Data At* field.

Is Data At Relative makes the match for *Is Data At* relative to the matched content in the *Content* field

Flow Direction can be *To Server* or *To Client*. For HTTP or SSL/TLS connections the flow is usually *To Server*.

Flow Established checks for an established flow. For HTTP or SSL/TLS connections the setting is usually *Established*.

PCRE allows for an additional regex PCRE check. It is also possible to leave the *Content* field empty and only use the *PCRE* match.

PCRE Content should have the *PCRE* match content, for example `/voleatech.com$|voleatech.de$/i`

Flows

For App Control flows are an important concept. A flow is a connection between a server and a client that is identified by its attributes. This is usually the IP addresses, the protocol and the ports.

Data about the *Application* can usually only be obtained when a connection is established between a client and a server. For example for SSL/TLS the TCP connection needs to go through the TCP handshake in order to obtain the certificate and SNI information.

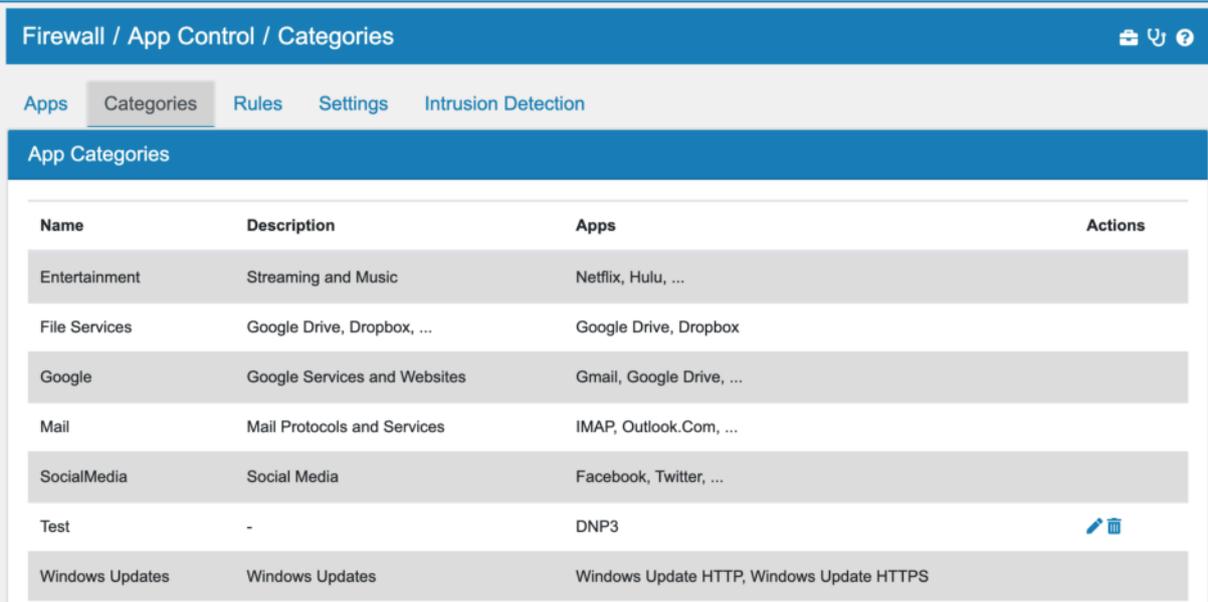
The connection can be blocked or accepted after the initial connection creation with *App Control*.

Warning: This means that a Firewall Rule *Firewall Rules (Forward and Input)* has to be created to allow the connection to be started. App Control is executed **AFTER** the firewall rules.

11.11.2 Categories

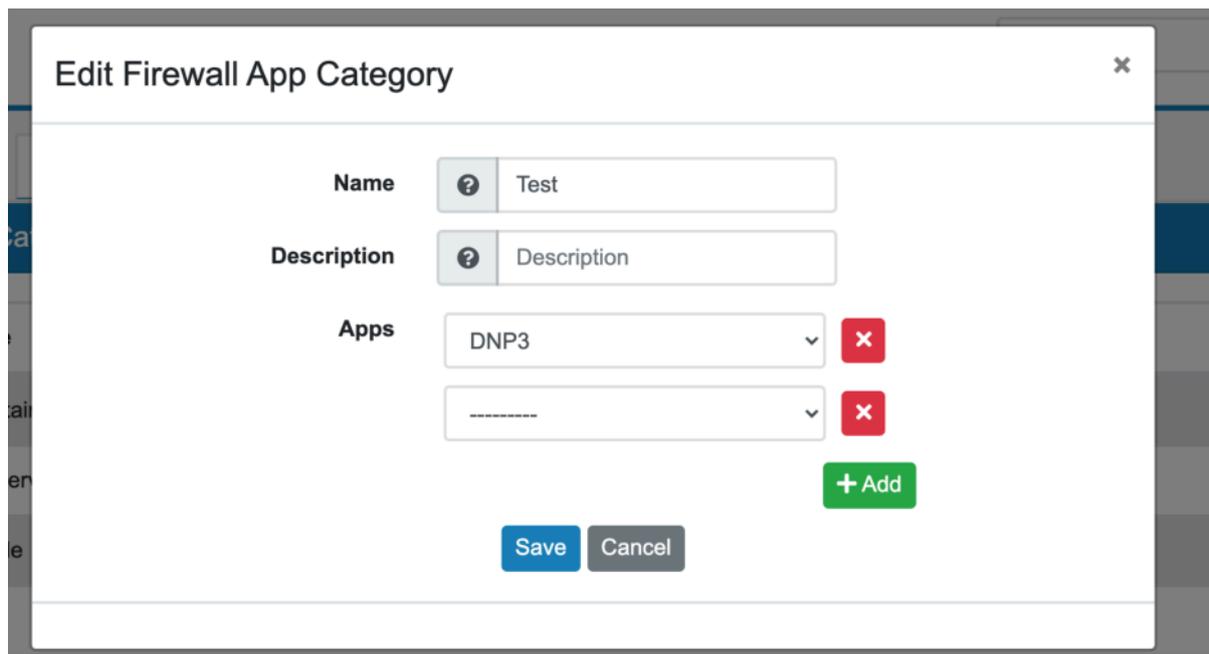
Apps are grouped in Categories. There are default builtin categories that can be used and you have the ability to create your own categories.

Categories are groups of Apps that can be used in App Control Rules.



The screenshot shows the 'App Categories' section of the Firewall configuration interface. The breadcrumb is 'Firewall / App Control / Categories'. There are tabs for 'Apps', 'Categories', 'Rules', 'Settings', and 'Intrusion Detection'. The 'Categories' tab is active. Below the tabs is a table with the following data:

Name	Description	Apps	Actions
Entertainment	Streaming and Music	Netflix, Hulu, ...	
File Services	Google Drive, Dropbox, ...	Google Drive, Dropbox	
Google	Google Services and Websites	Gmail, Google Drive, ...	
Mail	Mail Protocols and Services	IMAP, Outlook.Com, ...	
SocialMedia	Social Media	Facebook, Twitter, ...	
Test	-	DNP3	 
Windows Updates	Windows Updates	Windows Update HTTP, Windows Update HTTPS	



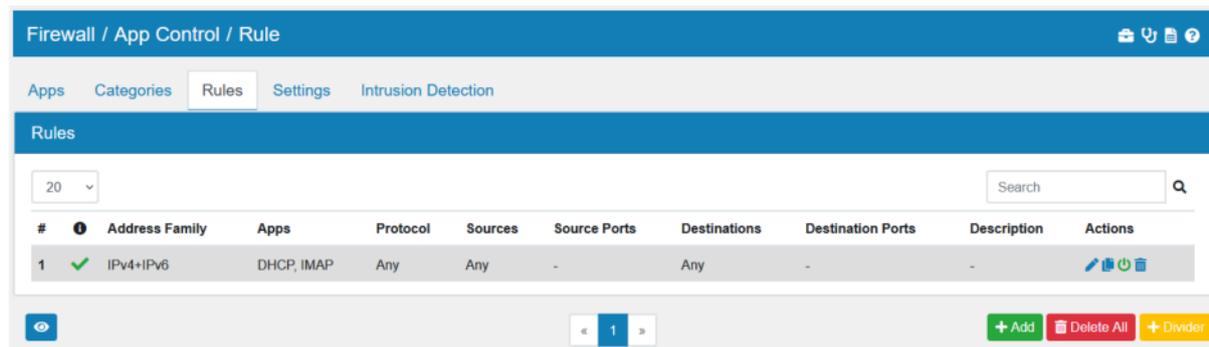
11.11.3 Rules

App Control Rules are similar to firewall rules. You can still narrow down the match to *IP Version*, *Protocol*, *Source IP*, *Source Port*, *Destination IP* and *Destination Port*.

The difference is, that you can also add **Apps** and **App Categories** to a rule.

It is also possible to assign QoS to a matched rule.

Note: App Rules are processed differently than normal firewall rules. The rules are processed in the following order: Pass, Reject, Drop, Match. You can change the order so Pass is processed last in the settings. Therefore App Rules order can not be changed as well.



Firewall / App Control / Rule / Update

General Settings

Enabled

Action ? Accept ▼

Address Family ? IPv4+IPv6 ▼

Protocol ? Any ▼

Description ? Description

Applications

Invert App Match

Applications

Category	File Services	✕
App	DHCP	✕
App	Skype	✕

+ Add

Sources

Invert IP Match

Source IPs Any ? IP Address / 128 ▼

+ Add

Advanced Source Settings

Destinations

Invert IP Match

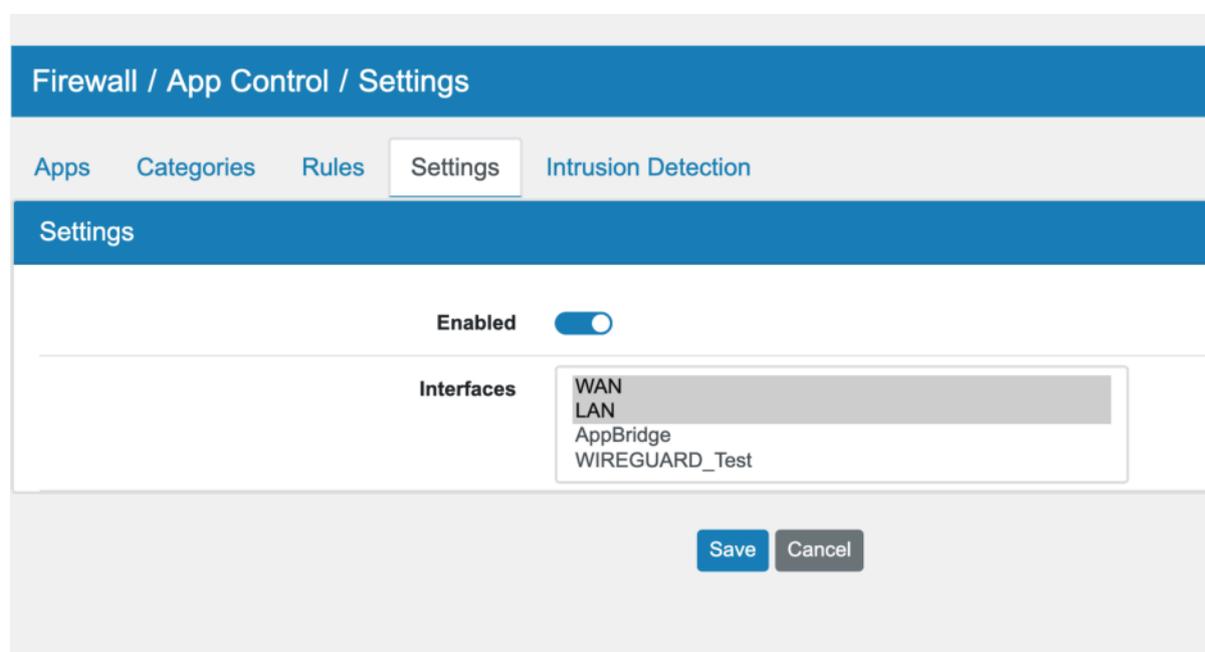
Destination IPs Any ? IP Address / 128 ▼

+ Add

11.11.4 Settings

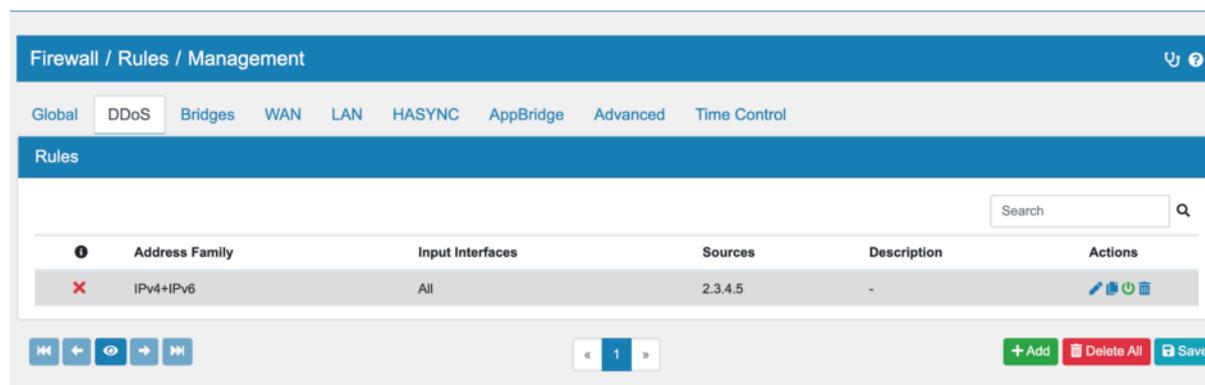
The Settings allow you to turn on and off the App Control. You can also select the interfaces that should get traffic analyzed.

Note: The input and output interface must be enabled for internet traffic for example LAN and WAN



11.12 DDoS Rules

You can find the DDoS Rules at **Firewall** → **Rules** under the tab **DDoS**.



DDoS Rules are early rules that match an IP Address in the destination or source or a packet. The packet is processed very early when it reaches the firewall and therefore has a high drop performance. In case of an active DDoS attack firewall resources are preserved and normal traffic can still be processed.

11.12.1 General Settings

DDoS rules have some of the same options as firewall rules. You can change the following options here:

Enabled Enable or Disable the rule

Input Interface You can change the Input Interface of this rule.

Action Can be *Drop* or *Accept*. It is *Drop* by default. **Accept** will act as a whitelist and all **Accept** rules are processed before **Drop** rules.

IP Address Enter one or more IP Address or IP Network to block.

Log this Rule will log information when the rule is used.

The screenshot shows the 'Firewall / Rules / Create' page. It is divided into three main sections:

- General Settings:** Includes a toggle for 'Enabled' (checked), 'Add Rule To' (radio buttons for 'Top' and 'Bottom', with 'Bottom' selected), 'Input Interfaces' (a searchable dropdown menu), 'Action' (a dropdown menu set to 'Drop'), and 'Description' (a text input field).
- IP Address:** Features a dropdown for 'IP Address' type (set to 'Host'), a text input for the IP address (192.168.10.104), a dropdown for the subnet (128), and a green '+ Add' button.
- Advanced:** Contains a 'Log this Rule' toggle (checked).

At the bottom, there are 'Save' and 'Cancel' buttons.

11.13 Divider

Firewall Divider can be used to structure your firewall rules.

The screenshot shows the 'Firewall / Rules / Management' page. A table lists the firewall rules:

#	Address Family	Protocol	Sources	Source Ports	Destinations	Destination Ports	Description	Used	Actions
1	IPv4+IPv6	Any	PrivateNetworks	-	Any	-	No RFC1918 (Private Networks)	0	[Edit] [Delete]
2	Test Divider								[Edit] [Delete]
3	IPv4+IPv6	Any	WAN_Network	-	WAN_Address	-	HA Rule	0	[Edit] [Delete]

At the bottom right of the table, there are buttons for '+ Add', 'Deletes All', and '+ Divider'.

You can create a divider by clicking on the **+ Divider** button in the bottom right corner on every firewall rules overview page. Each divider needs a **Description** and a **Color**.

You can drag and drop dividers to a different position and you can save that position by pressing save on the bottom navigation. Dividers will also be synchronized in a HA setup.

11.14 Learning Mode

You can find the Learning Mode at **Firewall** → **Rules** → **Learning Mode**.

Time	Action	Interface	Source	Destination	Protocol	Actions
2024-06-22 17:40	drop	eth0	79.124.62.86.54831	37.24.174.42.65169	TCP	✎
2024-06-22 17:40	drop	eth0	37.79.252.130.61706	37.24.174.42.445	TCP	✎
2024-06-22 17:40	drop	eth0	92.63.196.228.54701	37.24.174.42.8127	TCP	✎
2024-06-22 17:50	drop	eth0	92.63.196.228.54701	37.24.174.42.8841	TCP	✎
2024-06-22 17:50	drop	eth0	37.79.252.130.61706	37.24.174.42.445	TCP	✎

11.14.1 Learning Mode

The learning mode lets you see the traffic to the TBF and create rules from those logs.

When you **Enable** the learning mode, all traffic to the TBF will be allowed and logged, with the exception of other firewall rules that are already in place and have logging disabled.

Data Retention Days are the maximum days to store for analysis. More days requires more disk storage and for small systems it is necessary to keep the entries relatively low.

You can see and search traffic in a list of **Event Logs**. In the *Actions* column you can create a firewall rule from each entry.

When learning mode is enabled, a green icon is displayed at the top right of the TBF navigation interface.

12.1 Enforcer General

The Enforcer allows for Deep Packet Inspection (DPI) of OT Protocols. The Enforcer is based on the Tofino Technology and support the following protocols:

- AMP
- DNP3
- IEC104
- Goose
- Modbus
- OPC Classic

The DPI function lets you monitor and filter data packets. The function supports you in protecting the network from undesirable content. The DPI function inspects data packets for undesirable characteristics and protocol violations. The protocol inspects the header and the payload of the data packets. This dialog lets you specify the DPI settings. The device blocks the data packets that violate the specified profiles. If an error is detected, then the device terminates the data connection upon user request.

12.2 AMP

The ASCII Message Protocol (AMP) is a communication protocol widely used in the automation industry for Supervisory Control and Data Acquisition (SCADA) and system integration. The ASCII Message Protocol (AMP) is designed to help ensure reliable communication between industrial equipment. The ASCII Message Protocol (AMP) is used to monitor and control industrial automation equipment such as Programmable Logic Controllers (PLCs), sensors, and meters.

The device uses the Deep Packet Inspection (DPI) function to discard data packets that violate one of the specified profiles. The AMP Enforcer function supports Common ASCII Message Protocol (CAMP) and Non-Intelligent Terminal Protocol (NITP) using TCP. The device uses the AMP Enforcer function to perform the DPI function on the CAMP and NITP data stream. The device performs the DPI function based on the Program and mode protect function and the specified profiles.

When the AMP Enforcer profile is active, the device applies the profiles to the data stream.

The device permits only data packets that contain the values specified in the following fields depending on the status of the Program and mode protect function:

- Protocol
- Message type
- Address class
- Device class

- Memory address
- Data word
- Task code
- Task code data
- Block check characters
- Error check characters
- Sanity check

The menu contains the following dialogs:

- AMP Global
- AMP Profile

You can find the AMP enforcer at **Firewall** → **Enforcer** → **AMP**.

12.2.1 AMP Settings

Name Name of the AMP enforcer.

Possible values:

- **Character string** with 0..100 characters

Description Description of the AMP enforcer.

Possible values:

- **Character string** with 0..250 characters

Enabled Whether the AMP enforcer is active or not.

Possible values:

- **Enabled**
- **Disabled** (default setting)

Protocol

Specifies the TCP payload protocol type of the data packets to which the device applies the profile. The device applies the profile only to data packets that contain the specified value in the Protocol field.

Possible values:

- **camp**
Common ASCII Message Protocol

- **nitp**
Non-Intelligent Terminal Protocol

- **any (default setting)**
The device applies the profile to every data packet without evaluating the protocol.

Task code The prerequisite is that in the *Protocol* field one of the following values is specified:

- *nitp*
- *camp*: Additionally, in the *Message type* field, a hexadecimal value in the range 00..03 or the hexadecimal value FF is specified.
- *any*: Additionally, in the *Message type* field, the value *any* is specified.

Possible values:

- 01-9A

Task code data Specifies the task code data for the Task code.

The prerequisite is that in the *Protocol* field one of the following values is specified:

- **camp**
Additionally, in the *Message type* field, a hexadecimal value in the range 00..03 or the hexadecimal value FF, and in the *Task code* field a single hexadecimal value are specified.

- **nitp**
Additionally, in the *Task code* field, a single hexadecimal value is specified.

Possible values:

- **0..F**
The device applies the profile only to data packet that contains the specified task code data. The maximum length is 72 bytes.

Message types Specifies if the message is of the type command or response. The prerequisite is that in the *Protocol* field the value *camp* is specified.

Possible values:

- 00-FF

Address Classes Specifies the particular type of the memory to be accessed on the equipment.

Prerequisites:

- In the *Protocol* field, the value *camp* is specified.
- In the *Message type* field, a hexadecimal value in the range 00..03 or the hexadecimal value FF is specified.

Possible values:

- **any (default setting)**
The device applies the profile to every data packet without evaluating the address class.
- **0000..FFFF**
The device applies the profile only to data packets that contain the specified address class.

Device class Specifies the type of device class (vendor specific device) to be accessed.

Prerequisites:

- In the *Protocol* field, the value *camp* is specified.

- In the *Message type* field, a hexadecimal value in the range 00..03 or the hexadecimal value FF is specified.

Possible values:

- **any** (default setting)

The device applies the profile to every data packet without evaluating the device class.

- **0000..FFFF**

The device applies the profile only to data packets that contain the specified device class.

Memory address Specifies the starting address of the memory to be read or written.

Prerequisites:

- In the *Protocol* field, the value *camp* is specified.
- In the *Message type* field, a hexadecimal value in the range 00..01 or 04..09 or the hexadecimal value FF is specified.

Possible values:

- **any** (default setting)

The device applies the profile to every data packet without evaluating the memory address.

- **0000..FFFF**

The device applies the profile only to data packets that contain the specified memory address.

Data word Specifies the starting address that the equipment uses to read data from the packet.

Prerequisites:

- In the *Protocol* field, the value *camp* is specified.
- In the *Message type* field, a hexadecimal value in the range 00..01 or 08..09 or the hexadecimal value FF is specified.

Possible values:

- **any** (default setting)

The device applies the profile to every data packet without evaluating the data word.

- **0000..FFFF**

The device applies the profile only to data packets that contain the specified data word.

Sanity check Activates/deactivates the plausibility check for the data packets.

Possible values:

- **enabled** (default setting)

The plausibility check is active.

The device checks the plausibility of the data packets regarding format and specification.

The device blocks the data packets that violate the specified profiles.

- **disabled**

The plausibility check is inactive.

TCP Reset Activates/deactivates the resetting of the TCP connection in case of a protocol violation or if the plausibility check detects an error.

Possible values:

- **enabled** (default setting)

The resetting of the TCP connection is active.

If the device identifies a protocol violation or detects a plausibility check error, then the device terminates the TCP connection. The device establishes the TCP connection again on receiving a new connection request.

- **disabled**

The resetting of the TCP connection is inactive.

Debug Activates/deactivates the debugging of the profiles.

Possible values:

- **enabled**

Debugging is active.

The device sends the reset packet along with the information related to the termination of TCP connection. The prerequisite is that in the TCP reset field the checkbox is marked.

- **disabled** (default setting)

Debugging is inactive.

12.2.2 Task Codes

Enabled Whether the AMP enforcer is active or not.

Possible values:

- **Enabled**
- **Disabled** (default setting)

Description Description of the AMP enforcer.

Possible values:

- **Character string** with 0..250 characters

Task code Possible values:

- 01-9A

Mode Specifies the mode applicable for the Task code.

Possible values:

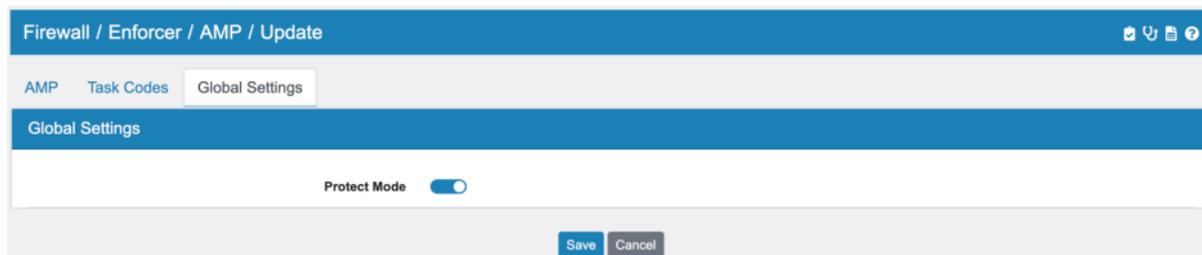
- **config**

Specifies commands associated with the modification of the controller settings, the application program or the operational mode.

- **non-config**

Specifies read/write commands, excluding the commands associated with modification of the controller settings, application program or operational mode.

12.2.3 AMP Global Settings



Protect mode

Activates/deactivates the inspection of the data packets that contain the Task codes with the value config in the Mode field.

Possible values:

- **enabled** (default setting)

The inspection is active.

The device forwards only the data packets that match the parameters specified in the profiles. The device discards data packets that contain the value config in the Mode field for the Task codes specified in the profiles.

- **disabled**

The device forwards the data packets that match the parameters specified in the profiles, including the data packets that contain Task codes with the value config in the Mode field.

12.2.4 Task Code

#	Meaning
01	Read Word Memory Random
02	Write Word Memory Area Random
30	Read Operational Status
32	Program to Run Mode
33	Go to Program Mode
34	Execute Power-up
35	Execute Complete (Warm) Start
36	Execute Partial (Hot) Start
50	Read User Word Area Block
51	Write User Word Area Starting at Address
58	Set Controller Time of Day Clock
59	Write Discrete I/O Status or Force via Data Element Type
5A	Write Block
6B	Read Discrete I/O Status or Force via Data Element Type
71	Read Controller Time of Day Clock
7D	Read SF/Loop Processor Mode
7E	Read Random
7F	Read Block
88	Select Number of SF Module Task Codes Per Scan
89	Read Number of SF Module Task Codes Per Scan
99	Write VME Memory Area Block/Random
9A	Read VME Memory Area Block/Random

12.2.5 AMP Message types

#	Meaning
00	Module General Query Command
01	Module General Response Command
02	Packet T/C Command
03	Packed T/C Response
04	Read data Command
05	Read data Response
06	Write data Command
07	Write data Response
08	Mem Exch Command
09	Mem Exch Response
FF	Protocol Error

12.3 DNP3

The DNP3 protocol is designed to help ensure reliable communication between components in process automation systems. The protocol provides multiplexing, error checking, link control, prioritization, and layer 2 addressing services for user data. The DNP3 Enforcer function activates the Deep Packet Inspection (DPI) firewall capabilities for the DNP3 data stream. The device blocks the data packets that violate the specified settings. Upon user request, the device verifies the data packets for their lausibility and their fragment characteristics. The device verifies and monitors DNP3 data connections and helps protect against invalid or falsified data packets.

When the DNP3 Enforcer settings are enabled, the device applies the settings to the data stream.

- The device permits data packets containing only the function codes specified in the Function code list field.
- The device rejects the data packets containing any other function codes that are not specified in the Function code list field.

12.3.1 DNP3 Settings

Enabled Whether the DNP3 enforcer is active or not.

Possible values:

- **Enabled**
- **Disabled** (default setting)

Name Name of the DNP3 enforcer.

Possible values:

- **Character string** with 0..100 characters

Description Description of the DNP3 enforcer.

Possible values:

- **Character string** with 0..250 characters

Function Codes Displays the function codes for the DNP3 Enforcer. The device permits data packets with the specified properties.

The device lets you specify multiple function codes.

Possible values:

- **0..255**

CRC Check Activates/deactivates the CRC check for the data packets to validate the checksum contained in the DNP3 data packets.

Possible values:

- **Enabled** (default setting)

The CRC check is active.

The device calculates the checksum and compares it with the checksum field in the DNP3 data packets.

- **Disabled**

The CRC check is inactive.

Sanity Check Activates/deactivates the plausibility check for the data packets.

Possible values:

- **Enabled** (default setting)

The plausibility check is active.

The device checks the plausibility of the data packets regarding format and specification.

The device blocks the data packets that violate the specified settings.

- **Disabled**

The plausibility check is inactive.

Check Outstation Traffic

Activates/deactivates the checking of the data packets that originate at an outstation.

Possible values:

- **Enabled** (default setting)

The checking of data packets from an outstation is active.

- **Disabled**

The checking of data packets from an outstation is inactive.

TCP Reset Activates/deactivates the resetting of the TCP connection in case of a protocol violation or if the plausibility check detects an error.

Possible values:

- **Enabled** (default setting)

The resetting of the TCP connection is active.

If the device identifies a protocol violation or detects a plausibility check error, then the device terminates the TCP connection. The device establishes the TCP connection again on receiving a new request.

- **Disabled**

The resetting of the TCP connection is inactive.

Preset Preset of default DNP3 objects.

Possible values:

- **All** (default setting)

Assigns all default objects.

- **Custom**

Lets you specify user-defined objects.

12.3.2 DNP3 Objects

Index Number	Function Code	Type	Group Number	Variation	Length	Description	Actions
-	2 Write	request	2	34	single_bit_packed	test	  

[+ Add Default Object](#)
[+ Create Object](#)

Enabled Whether the DNP3 object is active or not.

Possible values:

- **Enabled**
- **Disabled** (default setting)

Description Description of the DNP3 object.

Possible values:

- **Character string** with 0..250 characters

Type Specifies the type of the message.

Possible values:

- **Request**
Creates a request message object in the object list.
- **Response**
Creates a response message object in the object list.

Group Number Specifies a means of classifying the type or the types of data packets in a message. The prerequisite is that in the Type field a valid value is specified.

Possible values:

- **0..255**

Each group number shares a common point type and method of data packet creation. The point type defines the machine in an outstation.

Variation Specifies the variation number. The prerequisite is that in the Group no. field a valid value is specified. The device applies the DNP3 Enforcer profile only to data packets containing the specified value.

The DNP3 function provides the choice of encoding formats for the type of data packets known as variation number. Every value in the Group no. field has a set of variation numbers.

Possible values:

- **0..255**

The field lets you specify the following options:

- You specify a single variation number with a single numerical value, for example 1.
- You specify a range with numerical values connected by a dash, for example 0-55.

Function Code The function code identifies the purpose of the message. The prerequisite is that in the Variation field a valid value is specified. The device applies the DNP3 Enforcer profile only to data packets containing the specified value.

Possible values:

- **0..128**

Request messages from masters. Specify a single numerical value, for example 1.

- **129..255**

Response messages from outstations. Specify a single numerical value, for example 254.

Qualifier Specifies the qualifier code for a pair of each Group no., Variation, and Function fields. The qualifier code is an 8-bit value that defines the prefix code and the range specifier code for the object in a DNP3 message.

The prerequisite is that in the Function field a valid value is specified. The device applies the DNP3 Enforcer profile only to data packets containing the specified value.

Possible values:

- **0x00..0xff**

You specify multiple individual qualifier codes using hexadecimal values separated by a comma for a set of each Group no., Variation, and Function fields.

Length Specifies the optional length for the object. The prerequisite is that in the Function field a valid value is specified. The device applies the DNP3 Enforcer profile only to data packets containing the specified value.

Possible values:

- **0..255**

Specify a single numerical value, for example 1.

- **byte_2**

The second byte of the object data contains the length of the remaining portion of the data.

- **single_bit_packed**

If the count of bit values is not a multiple of 8, then the device pads the packed single-bit values up to the next byte boundary.

- **double_bit_packed**

If the count of double bit values is not a multiple of 4, then the device pads the packed doublebit values up to the next byte boundary.

- **variation**

Encodes the length of the object.

12.3.3 DNP3 Function Codes

#	Meaning
0	Confirm
1	Read
2	Write
3	Select
4	Operate
5	Direct Operate
6	Direct Operate-No Response Required
7	Freeze
8	Freeze-No Response Required
9	Freeze Clear
10	Freeze Clear-No Response Required
11	Freeze at Time
12	Freeze at Time-No Response Required
13	Cold Restart
14	Warm Restart
15	Initialize Data
16	Initialize Application
17	Start Application
18	Stop Application
19	Save Configuration
20	Enable Unsolicited Messages
21	Disable Unsolicited Messages
22	Assign Class
23	Delay Measurement
24	Record Current Time

continues on next page

Table 1 – continued from previous page

#	Meaning
25	Open File
26	Close File
27	Delete File
28	Get File Information
29	Authenticate File
30	Abort File Transfer
31	Active Configuration
32	Authentication Request
33	Authenticate Request-No Acknowledgment
129	Response
130	Unsolicited Response
131	Authentication Response

12.3.4 DNP3 Default Object List

Table 2: Table 1: Request messages

Index	Group no.	Variation	Function	Function name	Length	Qualifier
1	0	209-239	1	Read	undefined	0x00
2	0	240	1	Read	undefined	0x00
3	0	240	2	Write	byte_2	0x00
4	0	241-243	1	Read	undefined	0x00
5	0	245-247	1	Read	undefined	0x00
6	0	245-247	2	Write	byte_2	0x00
7	0	248-250	1	Read	undefined	0x00
8	0	252	1	Read	undefined	0x00
9	0	254	1	Read	undefined	0x00,0x06
10	0	255	1	Read	undefined	0x00,0x06
11	1	0-2	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
12	1	0	22	Assign Class	undefined	0x00,0x01,0x06,0x17,0x28
13	2	0-3	1	Read	undefined	0x06,0x07,0x08
14	3	0-2	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
15	3	0	22	Assign Class	undefined	0x00,0x01,0x06,0x17,0x28
16	4	0-3	1	Read	undefined	0x06,0x07,0x08
17	10	0	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
18	10	0	22	Assign Class	undefined	0x00,0x01,0x06,0x17,0x28
19	10	1	2	Write	single_bit_packed	0x01
20	10	2	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
21	11	0-2	1	Read	undefined	0x06,0x07,0x08
22	12	0	22	Assign Class	undefined	0x00,0x01,0x06,0x17,0x28
23	12	1	3	Select	11	0x00,0x01,0x17,0x28
24	12	1	4	Operate	11	0x00,0x01,0x17,0x28
25	12	1	5	Direct Operate	11	0x00,0x01,0x17,0x28
26	12	1	6	Direct Operate-No Response Required	11	0x00,0x01,0x17,0x28
27	12	2	3	Select	11	0x07,0x08

continues on next page

Table 2 – continued from previous page

Index	Group no.	Variation	Function	Function name	Length	Qualifier
28	12	2	4	Operate	11	0x07,0x08
29	12	2	5	Direct Operate	11	0x07,0x08
30	12	2	6	Direct Operate-No Response Required	11	0x07,0x08
31	12	3	3	Select	single_bit_packed	0x00,0x01
32	12	3	4	Operate	single_bit_packed	0x00,0x01
33	12	3	5	Direct Operate	single_bit_packed	0x00,0x01
34	12	3	6	Direct Operate-No Response Required	single_bit_packed	0x00,0x01
35	13	0-2	1	Read	undefined	0x06,0x07,0x08
36	20	0-2	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
37	20	5-6	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
38	20	0	7	Freeze	undefined	0x00,0x01,0x06,0x17,0x28
39	20	0	8	Freeze-No Response Required	undefined	0x00,0x01,0x06,0x17,0x28
40	20	0	9	Freeze Clear	undefined	0x00,0x01,0x06,0x17,0x28
41	20	0	10	Freeze Clear-No Response Required	undefined	0x00,0x01,0x06,0x17,0x28
42	20	0	11	Freeze at Time	undefined	0x00,0x01,0x06,0x17,0x28
43	20	0	12	Freeze at Time-No Response Required	undefined	0x00,0x01,0x06,0x17,0x28
44	20	0	22	Assign Class	undefined	0x00,0x01,0x06,0x17,0x28
45	21	0-2	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
46	21	5-6	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
47	21	9-10	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
48	21	0	22	Assign Class	undefined	0x00,0x01,0x06,0x17,0x28
49	22	0-2	1	Read	undefined	0x06,0x07,0x08
50	22	5-6	1	Read	undefined	0x06,0x07,0x08
51	23	0-2	1	Read	undefined	0x06,0x07,0x08
52	23	5-6	1	Read	undefined	0x06,0x07,0x08
53	30	0-6	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
54	30	0	7	Freeze	undefined	0x00,0x01,0x06,0x17,0x28
55	30	0	8	Freeze-No Response Required	undefined	0x00,0x01,0x06,0x17,0x28
56	30	0	11	Freeze at Time	undefined	0x00,0x01,0x06,0x17,0x28
57	30	0	12	Freeze at Time-No Response Required	undefined	0x00,0x01,0x06,0x17,0x28
58	30	0	22	Assign Class	undefined	0x00,0x01,0x06,0x17,0x28
59	31	0-8	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
60	31	0	22	Assign Class	undefined	0x00,0x01,0x06,0x17,0x28
61	32	0-8	1	Read	undefined	0x06,0x07,0x08
62	33	0-8	1	Read	undefined	0x06,0x07,0x08
63	34	0-3	1	Read	undefined	0x00,0x01,0x06
64	34	1	2	Write	2	0x00,0x01,0x17,0x28
65	34	2	2	Write	4	0x00,0x01,0x17,0x28
66	34	3	2	Write	4	0x00,0x01,0x17,0x28
67	40	0	1	Read	undefined	0x00,0x01,0x06
68	40	0	22	Assign Class	undefined	0x00,0x01,0x06,0x17,0x28
69	40	1-4	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
70	41	0	22	Assign Class	undefined	0x00,0x01,0x06,0x17,0x28
71	41	1	3	Select	5	0x00,0x01,0x17,0x28
72	41	2	3	Select	3	0x00,0x01,0x17,0x28
73	41	3	3	Select	5	0x00,0x01,0x17,0x28

continues on next page

Table 2 – continued from previous page

Index	Group no.	Variation	Function	Function name	Length	Qualifier
74	41	1	4	Operate	5	0x00,0x01,0x17,0x28
75	41	2	4	Operate	3	0x00,0x01,0x17,0x28
76	41	3	4	Operate	5	0x00,0x01,0x17,0x28
77	41	1	5	Direct Operate	5	0x00,0x01,0x17,0x28
78	41	2	5	Direct Operate	3	0x00,0x01,0x17,0x28
79	41	3	5	Direct Operate	5	0x00,0x01,0x17,0x28
80	41	1	6	Direct Operate-No Response Required	5	0x00,0x01,0x17,0x28
81	41	2	6	Direct Operate-No Response Required	3	0x00,0x01,0x17,0x28
82	41	3	6	Direct Operate-No Response Required	5	0x00,0x01,0x17,0x28
83	42	0-8	1	Read	undefined	0x06,0x07,0x08
84	43	0-8	1	Read	undefined	0x06,0x07,0x08
85	50	1	1	Read	undefined	0x07
86	50	1	2	Write	6	0x07
87	50	2	11	Freeze at Time	10	0x07
88	50	2	12	Freeze at Time-No Response Required	10	0x07
89	50	3	2	Write	10	0x07
90	50	4	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
91	50	4	2	Write	11	0x00,0x01,0x17,0x28
92	60	1	1	Read	undefined	0x06
93	60	2-4	1	Read	undefined	0x06,0x07,0x08
94	60	1-4	22	Assign Class	undefined	0x06
95	60	2-4	20	Enable Unsolicited Messages	undefined	0x06
96	60	2-4	21	Disable Unsolicited Messages	undefined	0x06
97	70	2	29	Authenticate File	QC_5B	0x5B
98	70	3	25	Open File	QC_5B	0x5B
99	70	3	27	Delete File	QC_5B	0x5B
100	70	4	26	Close File	QC_5B	0x5B
101	70	4	30	Abort File Transfer	QC_5B	0x5B
102	70	5-6	1	Read	QC_5B	0x5B
103	70	5	2	Write	QC_5B	0x5B
104	70	7	28	Get File Information	QC_5B	0x5B
105	70	8	31	Active Configuration	QC_5B	0x5B
106	80	1	1	Read	undefined	0x00,0x01
107	80	1	2	Write	single_bit	0x01
108	81	1	1	Read	undefined	0x00,0x01
109	82	1	1	Read	undefined	0x00,0x01
110	83	1	1	Read	undefined	0x00,0x01
111	85	0	1	Read	undefined	0x06
112	85	1	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
113	85	1	2	Write	QC_5B	0x5B
114	86	0	22	Assign Class	undefined	0x00,0x01,0x06,0x17,0x28
115	86	1-3	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
116	86	1	2	Write	QC_5B	0x5B
117	86	3	2	Write	QC_5B	0x5B
118	87	0	1	Read	undefined	0x06
119	87	1	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
120	87	1	2	Write	QC_5B	0x5B

continues on next page

Table 2 – continued from previous page

Index	Group no.	Variation	Function	Function name	Length	Qualifier
121	87	1	3	Select	QC_5B	0x5B
122	87	1	4	Operate	QC_5B	0x5B
123	87	1	5	Direct Operate	QC_5B	0x5B
124	87	1	6	Direct Operate-No Response Required	QC_5B	0x5B
125	88	0-1	1	Read	undefined	0x06,0x07,0x08
126	90	1	16	Initialize Application	QC_5B	0x5B
127	90	1	17	Start Application	QC_5B	0x5B
128	90	1	18	Stop Application	QC_5B	0x5B
129	101	1-3	1	Read	undefined	0x00,0x01,0x06,0x17,0x28
130	102	1	1	Read	undefined	0x00,0x01,0x03,0x04,0x05,0x06,0x17,0x28
131	102	1	2	Write	1	0x00,0x01,0x03,0x04,0x05,0x17,0x28
132	110	128	1	Read	undefined	0x00,0x01,0x03,0x04,0x05,0x06,0x17,0x28
133	110	128	2	Write	variation	0x00,0x01,0x03,0x04,0x05,0x17,0x28
134	110	128	31	Active Configuration	variation	0x5B
135	111	128	1	Read	undefined	0x06
136	112	128	2	Write	variation	0x00,0x01,0x17,0x28
137	113	0	1	Read	undefined	0x00,0x01,0x17,0x28
138	113	0	22	Assign Class	undefined	0x00,0x01,0x06,0x17,0x28

Table 3: Table 2: Response messages

Index	Group no.	Variation	Function	Function name	Length	Qualifier
139	0	209-239	129	Response	byte_2	0x00,0x17
140	0	240	129	Response	byte_2	0x00,0x17
141	0	241-243	129	Response	byte_2	0x00,0x17
142	0	245-247	129	Response	byte_2	0x00,0x17
143	0	248-250	129	Response	byte_2	0x00,0x17
144	0	252	129	Response	byte_2	0x00,0x17
145	0	255	129	Response	byte_2	0x00,0x17
146	1	1	129	Response	single_bit	0x00,0x01,0x17,0x28
147	1	2	129	Response	1	0x00,0x01,0x17,0x28
148	2	1	129	Response	1	0x17,0x28
149	2	2	129	Response	7	0x17,0x28
150	2	3	129	Response	3	0x17,0x28
151	2	1	130	Unsolicited Response	1	0x17,0x28
152	2	2	130	Unsolicited Response	7	0x17,0x28
153	2	3	130	Unsolicited Response	3	0x17,0x28
154	3	1	129	Response	double_bit	0x00,0x01,0x17,0x28
155	3	2	129	Response	1	0x00,0x01,0x17,0x28
156	4	1	129	Response	1	0x17,0x28
157	4	2	129	Response	7	0x17,0x28
158	4	3	129	Response	3	0x17,0x28
159	4	1	130	Unsolicited Response	1	0x17,0x28
160	4	2	130	Unsolicited Response	7	0x17,0x28
161	4	3	130	Unsolicited Response	3	0x17,0x28
162	10	2	129	Response	1	0x00,0x01,0x17,0x28

continues on next page

Table 3 – continued from previous page

Index	Group no.	Variation	Function	Function name	Length	Qualifier
163	11	1	129	Response	1	0x17,0x28
164	11	2	129	Response	7	0x17,0x28
165	11	1	130	Unsolicited Response	1	0x17,0x28
166	11	2	130	Unsolicited Response	7	0x17,0x28
167	12	1	129	Response	11	0x00,0x01,0x17,0x28
168	12	2	129	Response	11	0x07,0x08
169	12	3	129	Response	single_bit_packed	0x00,0x01
170	13	1	129	Response	1	0x17,0x28
171	13	2	129	Response	7	0x17,0x28
172	13	1	130	Unsolicited Response	1	0x17,0x28
173	13	2	130	Unsolicited Response	7	0x17,0x28
174	20	1	129	Response	5	0x00,0x01,0x17,0x28
175	20	2	129	Response	3	0x00,0x01,0x17,0x28
176	20	5	129	Response	4	0x00,0x01,0x17,0x28
177	20	6	129	Response	2	0x00,0x01,0x17,0x28
178	21	1	129	Response	5	0x00,0x01,0x17,0x28
179	21	2	129	Response	3	0x00,0x01,0x17,0x28
180	21	5	129	Response	4	0x00,0x01,0x17,0x28
181	21	6	129	Response	2	0x00,0x01,0x17,0x28
182	21	9	129	Response	4	0x00,0x01,0x17,0x28
183	21	10	129	Response	2	0x00,0x01,0x17,0x28
184	22	1	129	Response	5	0x17,0x28
185	22	2	129	Response	3	0x17,0x28
186	22	1	130	Unsolicited Response	5	0x17,0x28
187	22	2	130	Unsolicited Response	3	0x17,0x28
188	22	5	129	Response	11	0x17,0x28
189	22	6	129	Response	9	0x17,0x28
190	22	5	130	Unsolicited Response	11	0x17,0x28
191	22	6	130	Unsolicited Response	9	0x17,0x28
192	23	1	129	Response	5	0x17,0x28
193	23	2	129	Response	3	0x17,0x28
194	23	1	130	Unsolicited Response	5	0x17,0x28
195	23	2	130	Unsolicited Response	3	0x17,0x28
196	23	5	129	Response	11	0x17,0x28
197	23	6	129	Response	9	0x17,0x28
198	23	5	130	Unsolicited Response	11	0x17,0x28
199	23	6	130	Unsolicited Response	9	0x17,0x28
200	30	1	129	Response	5	0x00,0x01,0x17,0x28
201	30	2	129	Response	3	0x00,0x01,0x17,0x28
202	30	3	129	Response	4	0x00,0x01,0x17,0x28
203	30	4	129	Response	2	0x00,0x01,0x17,0x28
204	30	5	129	Response	5	0x00,0x01,0x17,0x28
205	30	6	129	Response	9	0x00,0x01,0x17,0x28
206	31	1	129	Response	5	0x00,0x01,0x17,0x28
207	31	2	129	Response	3	0x00,0x01,0x17,0x28
208	31	3	129	Response	11	0x00,0x01,0x17,0x28
209	31	4	129	Response	9	0x00,0x01,0x17,0x28
210	31	5	129	Response	4	0x00,0x01,0x17,0x28
211	31	6	129	Response	2	0x00,0x01,0x17,0x28
212	31	7	129	Response	5	0x00,0x01,0x17,0x28
213	31	8	129	Response	9	0x00,0x01,0x17,0x28
214	32	1	129	Response	5	0x17,0x28

continues on next page

Table 3 – continued from previous page

Index	Group no.	Variation	Function	Function name	Length	Qualifier
215	32	2	129	Response	3	0x17,0x28
216	32	3	129	Response	11	0x17,0x28
217	32	4	129	Response	9	0x17,0x28
218	32	5	129	Response	5	0x17,0x28
219	32	6	129	Response	9	0x17,0x28
220	32	7	129	Response	11	0x17,0x28
221	32	8	129	Response	15	0x17,0x28
222	32	1	130	Unsolicited Response	5	0x17,0x28
223	32	2	130	Unsolicited Response	3	0x17,0x28
224	32	3	130	Unsolicited Response	11	0x17,0x28
225	32	4	130	Unsolicited Response	9	0x17,0x28
226	32	5	130	Unsolicited Response	5	0x17,0x28
227	32	6	130	Unsolicited Response	9	0x17,0x28
228	32	7	130	Unsolicited Response	11	0x17,0x28
229	32	8	130	Unsolicited Response	15	0x17,0x28
230	33	1	129	Response	5	0x17,0x18
231	33	2	129	Response	3	0x17,0x28
232	33	3	129	Response	11	0x17,0x28
233	33	4	129	Response	9	0x17,0x28
234	33	5	129	Response	5	0x17,0x28
235	33	6	129	Response	9	0x17,0x28
236	33	7	129	Response	11	0x17,0x28
237	33	8	129	Response	15	0x17,0x28
238	33	1	130	Unsolicited Response	5	0x17,0x28
239	33	2	130	Unsolicited Response	3	0x17,0x28
240	33	3	130	Unsolicited Response	11	0x17,0x28
241	33	4	130	Unsolicited Response	9	0x17,0x28
242	33	5	130	Unsolicited Response	5	0x17,0x28
243	33	6	130	Unsolicited Response	9	0x17,0x28
244	33	7	130	Unsolicited Response	11	0x17,0x28
245	33	8	130	Unsolicited Response	15	0x17,0x28
246	34	1	129	Response	2	0x00,0x01
247	34	2-3	129	Response	4	0x00,0x01
248	40	1	129	Response	5	0x00,0x01,0x17,0x28
249	40	2	129	Response	3	0x00,0x01,0x17,0x28
250	40	3	129	Response	5	0x00,0x01,0x17,0x28
251	40	4	129	Response	9	0x00,0x01,0x17,0x28
252	41	1	129	Response	5	0x00,0x01,0x17,0x28
253	41	2	129	Response	3	0x00,0x01,0x17,0x28
254	41	3	129	Response	5	0x00,0x01,0x17,0x28
255	42	1	129	Response	5	0x17,0x28
256	42	2	129	Response	3	0x17,0x28
257	42	3	129	Response	11	0x17,0x28
258	42	4	129	Response	9	0x17,0x28
259	42	5	129	Response	5	0x17,0x28
260	42	6	129	Response	9	0x17,0x28
261	42	7	129	Response	11	0x17,0x28
262	42	8	129	Response	15	0x17,0x28
263	42	1	130	Unsolicited Response	5	0x17,0x28
264	42	2	130	Unsolicited Response	3	0x17,0x28
265	42	3	130	Unsolicited Response	11	0x17,0x28
266	42	4	130	Unsolicited Response	9	0x17,0x28

continues on next page

Table 3 – continued from previous page

Index	Group no.	Variation	Function	Function name	Length	Qualifier
267	42	5	130	Unsolicited Response	5	0x17,0x28
268	42	6	130	Unsolicited Response	9	0x17,0x28
269	42	7	130	Unsolicited Response	11	0x17,0x28
270	42	8	130	Unsolicited Response	15	0x17,0x28
271	43	1	129	Response	5	0x17,0x28
272	43	2	129	Response	3	0x17,0x28
273	43	3	129	Response	11	0x17,0x28
274	43	4	129	Response	9	0x17,0x28
275	43	5	129	Response	5	0x17,0x28
276	43	6	129	Response	9	0x17,0x28
277	43	7	129	Response	11	0x17,0x28
278	43	8	129	Response	15	0x17,0x28
279	43	1	130	Unsolicited Response	5	0x17,0x28
280	43	2	130	Unsolicited Response	3	0x17,0x28
281	43	3	130	Unsolicited Response	11	0x17,0x28
282	43	4	130	Unsolicited Response	9	0x17,0x28
283	43	5	130	Unsolicited Response	5	0x17,0x28
284	43	6	130	Unsolicited Response	9	0x17,0x28
285	43	7	130	Unsolicited Response	11	0x17,0x28
286	43	8	130	Unsolicited Response	15	0x17,0x28
287	50	1	129	Response	6	0x07
288	50	4	129	Response	11	0x00,0x01,0x17,0x28
289	51	1-2	129	Response	6	0x07
290	51	1-2	130	Unsolicited Response	6	0x07
291	52	1-2	129	Response	2	0x07
292	70	2	129	Response	QC_5B_c0x5B1	0x5B
293	70	4-7	129	Response	QC_5B_c0x5B1	0x5B
294	70	4-7	130	Unsolicited Response	QC_5B_c0x5B1	0x5B
295	80	1	129	Response	2	0x00,0x01
296	81	1	129	Response	3	0x07
297	82	1	129	Response	QC_5B_c0x5B1	0x5B
298	82	1	130	Unsolicited Response	QC_5B_c0x5B1	0x5B
299	83	1-2	129	Response	QC_5B	0x5B
300	83	1	130	Unsolicited Response	QC_5B	0x5B
301	85	1	129	Response	QC_5B	0x5B
302	86	1	129	Response	QC_5B	0x5B
303	86	2	129	Response	1	0x00,0x01,0x17,0x28
304	86	3	129	Response	QC_5B	0x5B
305	87	1	129	Response	QC_5B	0x5B
306	88	1	129	Response	QC_5B	0x5B
307	88	1	130	Unsolicited Response	QC_5B	0x5B
308	91	1	129	Response	QC_5B	0x5B
309	101	1	129	Response	2	0x00,0x01,0x17,0x28
310	101	2	129	Response	4	0x00,0x01,0x17,0x28
311	101	3	129	Response	8	0x00,0x01,0x17,0x28
312	102	1	129	Response	1	0x00,0x01,0x03,0x04,0x05,0x17,0x28
313	110	128	129	Response	variation	0x00,0x01,0x03,0x04,0x05,0x17,0x28
314	111	128	129	Response	variation	0x00,0x01,0x03,0x04,0x05,0x17,0x28
315	111	128	130	Unsolicited Response	variation	0x00,0x01,0x17,0x28
316	113	128	129	Response	variation	0x00,0x01,0x17,0x28
317	113	128	130	Unsolicited Response	variation	0x00,0x01,0x17,0x28

12.4 ENIP

The Ethernet Industrial Protocol (ENIP) is part of the Common Industrial Protocol (CIP). The Common Industrial Protocol (CIP) defines the object structure and specifies the message transfer. The ENIP Enforcer function applies the Deep Packet Inspection (DPI) function to the ENIP and CIP data stream. The Ethernet Industrial Protocol (ENIP) is used to monitor and control industrial automation equipment such as PLCs (Programmable Logic Controllers), sensors, and meters.

The device uses the ENIP Enforcer function to perform the DPI function on the data stream. The device performs the DPI function based on the values defined in the specified profiles. The device blocks the data packets that violate the specified profiles.

Note: The ENIP Enforcer function performs the DPI function only on packets that contain an explicit request, and drops packets that contain an implicit request. An explicit request contains CIP message over TCP. An implicit request contains CIP message over UDP.

When the ENIP Enforcer profile is active, the device applies the profile to the data stream.

The device permits only data packets containing the values specified in the following fields:

- Function type
- Sanity check
- Default object list
- Wildcard service codes
- Allow embedded PCCC (Programmable Controller Communication Commands)

The menu contains the following dialogs:

- ENIP Profile
- ENIP Object

You can find the ENIP enforcer at **Firewall** → **Enforcer** → **ENIP**.

Firewall / Enforcer / ENIP / Create

ENIP

Enabled

Name

Description

Sanity Check

TCP Reset

Debug

Allow embedded PCCC

Preset Read Only Read Write Any Custom

Save Cancel

12.4.1 ENIP Settings

Enabled Whether the ENIP enforcer is active or not.

Possible values:

- **Enabled**
- **Disabled** (default setting)

Name Name of the ENIP enforcer.

Possible values:

- **Character string** with 0..100 characters

Description Description of the ENIP enforcer.

Possible values:

- **Character string** with 0..250 characters

Sanity Check Activates/deactivates the plausibility check for the data packets.

Possible values:

- **enabled** (default setting)

The plausibility check is active.

The device checks the plausibility of the data packets regarding format and specification.

The device blocks the data packets that violate the specified profiles.

- **disabled**

The plausibility check is inactive.

TCP Reset Activates/deactivates the resetting of the TCP connection in case of a protocol violation or if the plausibility check detects an error.

Possible values:

- **enabled** (default setting)

The resetting of the TCP connection is active.

If the device identifies a protocol violation or detects a plausibility check error, then the device terminates the TCP connection. The device establishes the TCP connection again on receiving a new connection request.

- **disabled**

The resetting of the TCP connection is inactive.

Debug Activates/deactivates the debugging of the profiles.

Possible values:

- **enabled**

Debugging is active.

The device sends the reset packet along with the information related to the termination of TCP connection. The prerequisite is that in the TCP reset field the checkbox is marked.

- **disabled** (default setting)

Debugging is inactive.

Allow embedded PCCC Activates/deactivates DPI for PCCC messages encapsulated in data packets. PCCC messages are embedded within the Ethernet Industrial Protocol (ENIP). Activating this setting is useful when securing network traffic to and from PLC-5 and MicroLogix controllers.

Possible values:

- **enabled**
DPI for PCCC messages is active.
- **disabled** (default setting)
DPI for PCCC messages is inactive.

Preset Preset of class IDs and service codes

Possible values:

- **Read Only**
Assigns the class IDs for the read function.
- **Read Write**
Assigns the class IDs for the read/write functions.
- **Any** (default setting)
Assigns the class IDs for every function.
The device does not permit any subsequent changes in the *Advanced Class IDs* list.
- **Advanced**
Lets you specify user-defined class IDs.

12.4.2 ENIP Class IDs for different function types

Table 4: Table 1: Class IDs for function type **readonly**

Class ID	Service codes
0x01 = Identity	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x11 = Find Next Object Instance 0x18 = Get Member
0x02 = Message Router	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x54
0x04 = Assembly	0x0E = Get Attribute Single 0x18 = Get Member
0x05 = Connection	0x08 = Create 0x0E = Get Attribute Single 0x11 = Find Next Object Instance 0x4C

continues on next page

Table 4 – continued from previous page

Class ID	Service codes
0x06 = Off-Link Connection Manager	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x4C 0x4E 0x52 0x54 0x56 0x57 0x59 0x5A 0x5B
0x07 = Register	0x0E = Get Attribute Single
0x08 = Discrete Input Point	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x09 = Discrete Output Point	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x0A = Analog Input Point	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x0B = Analog Output Point	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x0E = Presence Sensing	0x0E = Get Attribute Single
0x0F = Parameter	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x18 = Get Member 0x4B
0x10 = Parameter Group	0x01 = Get Attributes All 0x0E = Get Attribute Single

continues on next page

Table 4 – continued from previous page

Class ID	Service codes
0x12 = Group	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x1D = Discrete Input Group	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x1E = Discrete Output Group	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x1F = Discrete Group	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x20 = Analog Input Group	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x21 = Analog Output Group	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x22 = Analog Group	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x23 = Position Sensor Object	0x0E = Get Attribute Single 0x18 = Get Member
0x24 = Position Controller Supervisor Object	0x0E = Get Attribute Single
0x25 = Position Controller Object	0x0E = Get Attribute Single
0x26 = Block Sequencer Object	0x0E = Get Attribute Single
0x27 = Command Block Object	0x0E = Get Attribute Single

continues on next page

Table 4 – continued from previous page

Class ID	Service codes
0x28 = Motor Data Object	0x0E = Get Attribute Single
0x29 = Control Supervisor Object	0x0E = Get Attribute Single
0x2A = AC/DC Drive Object	0x0E = Get Attribute Single
0x2B = Acknowledge Handler Object	0x0E = Get Attribute Single
0x2C = Overload Object	0x0E = Get Attribute Single
0x2D = Softstart Object	0x0E = Get Attribute Single
0x2E = Selection Object	0x0E = Get Attribute Single 0x18 = Get Member
0x30 = S-Device Supervisor Object	0x0E = Get Attribute Single
0x31 = S-Analog Sensor Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x32 = S-Analog Actuator Object	0x0E = Get Attribute Single
0x33 = S-Single Stage Controller Object	0x0E = Get Attribute Single
0x34 = S-Gas Calibration Object	0x0E = Get Attribute Single 0x4B
0x35 = Trip Point Object	0x0E = Get Attribute Single

continues on next page

Table 4 – continued from previous page

Class ID	Service codes
0x37 = File Object	0x0E = Get Attribute Single 0x18 = Get Member 0x4B 0x4D 0x4F
0x38 = S-Partial Pressure Object	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x4C 0x4D 0x4E
0x40 = S-Sensor Calibration Object	0x0E = Get Attribute Single 0x4B
0x41 = Event Log Object	0x0E = Get Attribute Single 0x18 = Get Member
0x42 = Motion Device Axis Object	0x03 = Get Attribute List 0x0E = Get Attribute Single 0x4B 0x50 0x52 0x54
0x43 = Time Sync Object	0x01 = Get Attributes All 0x03 = Get Attribute List 0x0E = Get Attribute Single
0x44 = Modbus Object	0x0E = Get Attribute Single 0x4B 0x4C 0x4D 0x4E
0x45 = Originator Connection List Object	0x4C

continues on next page

Table 4 – continued from previous page

Class ID	Service codes
0x46 = Modbus Serial Link Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x47 = Device Level Ring (DLR) Object	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x18 = Get Member
0x48 = QoS Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x4D = Target Connection List Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x4E = Base Energy Object	0x01 = Get Attributes All 0x03 = Get Attribute List 0x0E = Get Attribute Single 0x18 = Get Member
0x4F = Electrical Energy Object	0x01 = Get Attributes All 0x03 = Get Attribute List 0x0E = Get Attribute Single
0x50 = Non-Electrical Energy Object	0x01 = Get Attributes All 0x03 = Get Attribute List 0x0E = Get Attribute Single
0x51 = Base Switch Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x52 = SNMP Object	0x01 = Get Attributes All 0x0E = Get Attribute Single

continues on next page

Table 4 – continued from previous page

Class ID	Service codes
0x53 = Power Management Object	0x01 = Get Attributes All 0x03 = Get Attribute List 0x0E = Get Attribute Single 0x18 = Get Member
0x54 = RSTP Bridge Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x55 = RSTP Port Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x91 = ANSI Extended Symbol Segment	0x03 = Get Attribute List 0x55
0x6C	0x01 = Get Attributes All
0xAC	0x01 = Get Attributes All 0x4C
0xB2	0x08 = Create 0x4E 0x4F
0xF3 = Connection Configuration Object	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x4C 0x4D 0x4E 0x50
0xF4 = Port Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0xF5 = TCP/IP Interface Object	0x01 = Get Attributes All 0x0E = Get Attribute Single

continues on next page

Table 4 – continued from previous page

Class ID	Service codes
0xF6 = EtherNet Link Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x300 = Module Diagnostics	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x301 = InputIOCnx	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x302 = Local Slaves	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x400 = Service Port Control Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x401 = Dynamic IO Control Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x402 = Router Diagnostics Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x403 = Router Routing Table Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x404 = SMTP	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x405 = SNTP	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x406 = HSBY	0x01 = Get Attributes All 0x0E = Get Attribute Single

Table 5: Table 2: Class IDs for function type **readwrite**

Class ID	Service codes
0x01 = Identity	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x11 = Find Next Object Instance 0x18 = Get Member
0x02 = Message Router	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x4B 0x54
0x04 = Assembly	0x08 = Create 0x09 = Delete 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x18 = Get Member 0x19 = Set Member 0x1A = Insert Member 0x1B = Remove Member 0x4B 0x4C
0x05 = Connection	0x05 = Reset
0x06 = Off-Link Connection Manager	0x01 = Get Attributes All 0x02 = Set Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x4C 0x4E 0x52 0x54 0x56 0x57 0x59 0x5A 0x5B
0x07 = Register	0x0E = Get Attribute Single 0x10 = Set Attribute Single

continues on next page

Table 5 – continued from previous page

Class ID	Service codes
0x08 = Discrete Input Point	0x01 = Get Attributes All 0x02 = Set Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x09 = Discrete Output Point	0x01 = Get Attributes All 0x02 = Set Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x0A = Analog Input Point	0x01 = Get Attributes All 0x02 = Set Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x0B = Analog Output Point	0x01 = Get Attributes All 0x02 = Set Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x0E = Presence Sensing	0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x0F = Parameter	0x01 = Get Attributes All 0x05 = Reset 0x0D = Apply Attributes 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x15 = Restore 0x16 = Save 0x18 = Get Member 0x4B
0x10 = Parameter Group	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single

continues on next page

Table 5 – continued from previous page

Class ID	Service codes
0x12 = Group	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x1D = Discrete Input Group	0x01 = Get Attributes All 0x02 = Set Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x1E = Discrete Output Group	0x01 = Get Attributes All 0x02 = Set Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x1F = Discrete Group	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x20 = Analog Input Group	0x01 = Get Attributes All 0x02 = Set Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x21 = Analog Output Group	0x01 = Get Attributes All 0x02 = Set Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x22 = Analog Group	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x23 = Position Sensor Object	0x05 = Reset 0x0D = Apply Attributes 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x15 = Restore 0x16 = Save 0x18 = Get Member 0x19 = Set Member

continues on next page

Table 5 – continued from previous page

Class ID	Service codes
0x24 = Position Controller Supervisor Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x25 = Position Controller Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x26 = Block Sequencer Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x27 = Command Block Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x28 = Motor Data Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x15 = Restore 0x16 = Save
0x29 = Control Supervisor Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x05 = Reset
0x2A = AC/DC Drive Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x15 = Restore 0x16 = Save
0x2B = Acknowledge Handler Object	0x08 = Create 0x09 = Delete 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x4B 0x4C

continues on next page

Table 5 – continued from previous page

Class ID	Service codes
0x2C = Overload Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x15 = Restore 0x16 = Save
0x2D = Softstart Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x15 = Restore 0x16 = Save
0x2E = Selection Object	0x05 = Reset 0x06 = Start 0x07 = Stop 0x08 = Create 0x09 = Delete 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x18 = Get Member 0x19 = Set Member 0x1A = Insert Member 0x1B = Remove Member
0x30 = S-Device Supervisor Object	0x05 = Reset 0x06 = Start 0x07 = Stop 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x4B 0x4C 0x4E
0x31 = S-Analog Sensor Object	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x4B 0x4C
0x32 = S-Analog Actuator Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single

continues on next page

Table 5 – continued from previous page

Class ID	Service codes
0x33 = S-Single Stage Controller Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x63
0x34 = S-Gas Calibration Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x4B
0x35 = Trip Point Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x37 = File Object	0x06 = Start 0x07 = Stop 0x08 = Create 0x09 = Delete 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x15 = Restore 0x16 = Save 0x18 = Get Member 0x4B 0x4C 0x4D 0x4E 0x4F 0x50 0x51
0x38 = S-Partial Pressure Object	0x01 = Get Attributes All 0x08 = Create 0x09 = Delete 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x4B 0x4C 0x4D 0x4E 0x4F

continues on next page

Table 5 – continued from previous page

Class ID	Service codes
0x40 = S-Sensor Calibration Object	0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x4B
0x41 = Event Log Object	0x05 = Reset 0x06 = Start 0x07 = Stop 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x18 = Get Member 0x19 = Set Member 0x1A = Insert Member 0x1B = Remove Member
0x42 = Motion Device Axis Object	0x03 = Get Attribute List 0x04 = Set Attribute List 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x1C = Group Sync 0x4B 0x4C 0x4D 0x4E 0x4F 0x50 0x51 0x52 0x53 0x54
0x43 = Time Sync Object	0x01 = Get Attributes All 0x03 = Get Attribute List 0x04 = Set Attribute List 0x0E = Get Attribute Single 0x10 = Set Attribute Single

continues on next page

Table 5 – continued from previous page

Class ID	Service codes
0x44 = Modbus Object	0x0E = Get Attribute Single 0x4B 0x4C 0x4D 0x4E 0x4F 0x50 0x51
0x45 = Originator Connection List Object	0x08 = Create 0x09 = Delete 0x4C
0x46 = Modbus Serial Link Object	0x01 = Get Attributes All 0x05 = Reset 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x4B
0x47 = Device Level Ring (DLR) Object	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x18 = Get Member 0x4B 0x4C 0x4D 0x4E
0x48 = QoS Object	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x4D = Target Connection List Object	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x4C

continues on next page

Table 5 – continued from previous page

Class ID	Service codes
0x4E = Base Energy Object	0x01 = Get Attributes All 0x03 = Get Attribute List 0x04 = Set Attribute List 0x05 = Reset 0x08 = Create 0x09 = Delete 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x18 = Get Member 0x19 = Set Member 0x1A = Insert Member 0x1B = Remove Member 0x4B 0x4C
0x4F = Electrical Energy Object	0x01 = Get Attributes All 0x03 = Get Attribute List 0x0E = Get Attribute Single
0x50 = Non-Electrical Energy Object	0x01 = Get Attributes All 0x03 = Get Attribute List 0x0E = Get Attribute Single
0x51 = Base Switch Object	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x52 = SNMP Object	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single

continues on next page

Table 5 – continued from previous page

Class ID	Service codes
0x53 = Power Management Object	0x01 = Get Attributes All 0x03 = Get Attribute List 0x04 = Set Attribute List 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x18 = Get Member 0x19 = Set Member 0x4D 0x4E 0x4F
0x54 = RSTP Bridge Object	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x55 = RSTP Port Object	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0x91 = ANSI Extended Symbol Segment	0x03 = Get Attribute List 0x55
0x6B	0x55
0x6C	0x01 = Get Attributes All
0xAC	0x01 = Get Attributes All 0x4C
0xB2	0x08 = Create 0x4E 0x4F

continues on next page

Table 5 – continued from previous page

Class ID	Service codes
0xF3 = Connection Configuration Object	0x01 = Get Attributes All 0x02 = Set Attributes All 0x08 = Create 0x09 = Delete 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x15 = Restore 0x4B 0x4C 0x4D 0x4E 0x4F 0x50 0x51 0x52
0xF4 = Port Object	0x01 = Get Attributes All 0x05 = Reset 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0xF5 = TCP/IP Interface Object	0x01 = Get Attributes All 0x02 = Set Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single
0xF6 = EtherNet Link Object	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x10 = Set Attribute Single 0x4C
0x300 = Module Diagnostics	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x301 = InputIOCnx	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x302 = Local Slaves	0x01 = Get Attributes All 0x0E = Get Attribute Single

continues on next page

Table 5 – continued from previous page

Class ID	Service codes
0x400 = Service Port Control Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x401 = Dynamic IO Control Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x402 = Router Diagnostics Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x403 = Router Routing Table Object	0x01 = Get Attributes All 0x0E = Get Attribute Single
0x404 = SMTP	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x32
0x405 = SNTP	0x01 = Get Attributes All 0x0E = Get Attribute Single 0x32
0x406 = HSBY	0x01 = Get Attributes All 0x0E = Get Attribute Single

12.5 GOOSE

The GOOSE (Generic Object Oriented Substation Event) Loadable Security Module (LSM) which enables Deep Pack Inspection (DPI) firewall capabilities for GOOSE traffic.

The GOOSE traffic is one of the mapped standards of IEC 61850 protocol and is engineered for configuration of Intelligent Electronic Devices for electrical substation automation systems to be able to communicate with each other.

You can find the GOOSE protocol at **Firewall** → **Enforcer** → **GOOSE**.

The screenshot shows a web interface for creating a GOOSE enforcer. The breadcrumb trail is 'Firewall / Enforcer / GOOSE / Create'. The main heading is 'GOOSE'. Below it, there are several settings:

- Enabled:** A red toggle switch is turned on.
- Name:** A text input field containing the word 'Name'.
- Description:** A text input field containing the word 'Description'.
- Sanity Check:** A blue toggle switch is turned on.
- State and Sequence Check:** A blue toggle switch is turned on.

At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

12.5.1 GOOSE Settings

Enabled Whether the GOOSE enforcer is active or not.

Possible values:

- **Enabled**
- **Disabled** (default setting)

Name Name of the GOOSE enforcer.

Possible values:

- **Character string** with 0..100 characters

Description Description of the GOOSE enforcer.

Possible values:

- **Character string** with 0..250 characters

Sanity Check Activates/deactivates the plausibility check for the data packets.

Possible values:

- **Enabled** (default setting)
The plausibility check is active.
The device checks the plausibility of the data packets regarding format and specification.
The device blocks the data packets that violate the specified profiles.
- **Disabled**
The plausibility check is inactive.

State and Sequence Check Activates/deactivates the State and Sequence Check.

Possible values:

- **Enabled** (default setting)
- **Disabled**

12.6 IEC104

The IEC104 protocol is a communication protocol used in the automation sector.

The IEC104 protocol helps to transfer the IEC104 data packets between a control station (client) and a substation (server) using a TCP/IP network. The IEC104 Enforcer function activates the Deep Packet Inspection (DPI) firewall capabilities for the IEC104 data stream. The type IDs in the IEC104 protocol specify the purpose of the data transfer. The device blocks the data packets that violate the specified profiles.

When the IEC104 Enforcer profile is active, the device applies the profile to the data stream.

The device permits only data packets containing the values specified in the following fields:

- Function type
- Advanced type ID list
- Originator address list
- Common address list

You can find the IEC104 enforcer at **Firewall** → **Enforcer** → **IEC104**.

The screenshot displays the configuration page for the IEC104 enforcer. The page title is "Firewall / Enforcer / IEC104 / Create". The main content area is titled "IEC104".

Key configuration elements visible include:

- Enabled:** A red toggle switch is turned on.
- Name:** A text input field with a placeholder "Name".
- Description:** A text input field with a placeholder "Description".
- Preset:** A dropdown menu set to "Any".
- Type IDs:** A list of 9 items, each with a radio button and a text label:
 - 1 Single point information M_SP_NA_1
 - 2 Single point information with time tag M_SP_TA_1
 - 3 Double point information M_DP_NA_1
 - 4 Double point information with time tag M_DP_TA_1
 - 5 Step position information M_ST_NA_1
 - 6 Step position information with time tag M_ST_TA_1
 - 7 Bit string of 32 bit M_BO_NA_1
 - 8 Bit string of 32 bit with time tag M_BO_TA_1
 - 9 Measured value, normalized value M_ME_NA_1
- Allow IEC_60870_5_101:** A red toggle switch is turned on.
- Originator Address List:** An empty text input field.
- Common Address List:** An empty text input field.
- Sanity Check:** A blue toggle switch is turned on.
- TCP Reset:** A blue toggle switch is turned on.
- Debug:** A red toggle switch is turned on.
- Cause of transmission size:** A dropdown menu set to "2".
- Common address size:** A dropdown menu set to "2".
- IO Address Size:** A dropdown menu set to "3".

At the bottom of the form, there are "Save" and "Cancel" buttons.

12.6.1 IEC104 Settings

Enabled Whether the IEC104 enforcer is active or not.

Possible values:

- **Enabled**
- **Disabled** (default setting)

Name Name of the IEC104 enforcer.

Possible values:

- **Character string** with 0..100 characters

Description Description of the IEC104 enforcer.

Possible values:

- **Character string** with 0..250 characters

Preset Preset of Type IDs

Possible values:

- **Read Only**

Assigns the type IDs for the read function.

1,3,5,7,9,11,13,15,20,21,30-40,70,100-102

- **Read Write**

Assigns the type IDs for the read/write functions.

1,3,5,7,9,11,13,15,20,21,30-40,45-51,58-64,70,100-102

- **Common**

Assigns the type IDs for the common functions.

1,3,5,7,9,11,13,15,20,21,30-40,45-51,58-64,70,100-102,110-113,120-127

- **Any** (default setting)

Assigns the type IDs for every function.

1,2,...,254,255

The device does not permit any subsequent changes in the *Advanced Type IDs* list.

- **Advanced**

Lets you specify user-defined values in the *Type IDs* list.

Type IDs Gets prefilled depending on the preset selection.

If the preset is *advanced* you can select your own type ids here.

Allow IEC_60870_5_101 Activates/deactivates the type IDs defined in the IEC101 specification.

Possible values:

- **Enabled**

The type IDs defined in the IEC101 specification are active.

The device permits the type ID values 2,4,6,8,10,12,14,16,17,18,19,103,104,105,106 along with the type IDs based on the values specified in the Function type field or Advanced type ID list field.

- **Disabled** (default setting)

The type IDs defined in the IEC101 specification are inactive.

The device permits only the type ID values based on the values specified in the Function type or Advanced type ID list field.

Originator address list Specifies the addresses from which data packets originated. The prerequisite is that in the Cause of transmission size field the value 2 is specified.

Possible values:

- **<empty>** (default setting)

The device permits data packets from any originator address.

- **0..255**

The device permits data packets with the specified originator address.

Common address list Specifies the addresses to which the device forwards the IEC104 data packets.

Possible values:

- **0..255**

The device permits data packets with the specified common address. The prerequisite is that in the Common address size field the value 1 is specified.

- **0..65535** (2¹⁷-1)

The device permits data packets with the specified common address. The prerequisite is that in the Common address size field the value 2 is specified.

Sanity Check Activates/deactivates the plausibility check for the data packets.

Possible values:

- **Enabled** (default setting)

The plausibility check is active.

The device checks the plausibility of the data packets regarding format and specification.

The device blocks the data packets that violate the specified profiles.

- **Disabled**

The plausibility check is inactive.

TCP Reset Activates/deactivates the resetting of the TCP connection in case of a protocol violation or if the plausibility check detects an error.

Possible values:

- **Enabled** (default setting)

The resetting of the TCP connection is active.

If the device identifies a protocol violation or detects a plausibility check error, then the device terminates the TCP connection. The device establishes the TCP connection again on receiving a new request.

- **Disabled**

The resetting of the TCP connection is inactive.

Debug Activates/deactivates the debugging of the profiles.

Possible values:

- **Enabled**

Debugging is active.

The device sends the reset packet along with the information related to the termination of TCP connection. The prerequisite is that the TCP reset checkbox is marked.

- **Disabled** (default setting)

Debugging is inactive.

Cause of transmission size Specifies the size in octets that defines the variation of the respective fields in the data packets.

The device performs the DPI function based on these settings.

Possible values:

- **1**

The data packets do not contain an originator address.

- 2 (default setting)

The data packets contain an originator address.

Common address size Specifies the size in octets of the common address to which the device forwards the IEC104 data packets. This setting affects the setting in the Common address list field.

Possible values:

- 1
- 2 (default setting)

IO Address Size Specifies the size in octets of the information object address.

Possible values:

- 1
- 2
- 3 (default setting)

12.6.2 IEC104 Meaning of the Type ID list values

#	Meaning
1	Single point information M_SP_NA_1
2	Single point information with time tag M_SP_TA_1
3	Double point information M_DP_NA_1
4	Double point information with time tag M_DP_TA_1
5	Step position information M_ST_NA_1
6	Step position information with time tag M_ST_TA_1
7	Bit string of 32 bit M_BO_NA_1
8	Bit string of 32 bit with time tag M_BO_TA_1
9	Measured value, normalized value M_ME_NA_1
10	Measured value, normalized value with time tag M_ME_TA_1
11	Measured value, scaled value M_ME_NB_1
12	Measured value, scaled value with time tag M_ME_TB_1
13	Measured value, short floating point value M_ME_NC_1
14	Measured value, short floating point value with time tag M_ME_TC_1
15	Integrated totals M_IT_NA_1
16	Integrated totals with time tag M_IT_TA_1
17	Event of protection equipment with time tag M_EP_TA_1
18	Packed start events of protection equipment with time tag M_EP_TB_1
19	Packed output circuit information of protection equipment with time tag M_EP_TC_1
20	Packed single-point information with status change detection M_PS_NA_1
21	Measured value, normalized value without quality descriptor M_ME_ND_1
30	Single point information with time tag CP56Time2a M_SP_TB_1
31	Double point information with time tag CP56Time2a M_DP_TB_1
32	Step position information with time tag CP56Time2a M_ST_TB_1
33	Bit string of 32 bit with time tag CP56Time2a M_BO_TB_1
34	Measured value, normalized value with time tag CP56Time2a M_ME_TD_1
35	Measured value, scaled value with time tag CP56Time2a M_ME_TE_1
36	Measured value, short floating point value with time tag CP56Time2a M_ME_TF_1
37	Integrated totals with time tag CP56Time2a M_IT_TB_1
38	Event of protection equipment with time tag CP56Time2a M_EP_TD_1
39	Packed start events of protection equipment with time tag CP56time2a M_EP_TE_1
40	Packed output circuit information of protection equipment with time tag CP56Time2a M_EP_TF_1

continues on next page

Table 6 – continued from previous page

#	Meaning
45	Single command C_SC_NA_1
46	Double command C_DC_NA_1
47	Regulating step command C_RC_NA_1
48	Setpoint command, normalized value C_SE_NA_1
49	Setpoint command, scaled value C_SE_NB_1
50	Setpoint command, short floating point value C_SE_NC_1e
51	Bit string 32 bit C_BO_NA_1
58	Single command with time tag CP56Time2a C_SC_TA_1
59	Double command with time tag CP56Time2a C_DC_TA_1
60	Regulating step command with time tag CP56Time2a C_RC_TA_1
61	Setpoint command, normalized value with time tag CP56Time2a C_SE_TA_1
62	Setpoint command, scaled value with time tag CP56Time2a C_SE_TB_1
63	Setpoint command, short floating point value with time tag CP56Time2a C_SE_TC_1
64	Bit string 32 bit with time tag CP56Time2a C_BO_TA_1
70	End of initialization M_EI_NA_1
100	(General-) Interrogation command C_IC_NA_1
101	Counter interrogation command C_CI_NA_1
102	Read command C_RD_NA_1
103	Clock synchronization command C_CS_NA_1
104	(IEC 101) Test command C_TS_NB_1
105	Reset process command C_RP_NC_1
106	(IEC 101) Delay acquisition command C_CD_NA_1
107	Test command with time tag CP56Time2a C_TS_TA_1
110	Parameter of measured value, normalized value P_ME_NA_1
111	Parameter of measured value, scaled value P_ME_NB_1
112	Parameter of measured value, short floating point value P_ME_NC_1
113	Parameter activation P_AC_NA_1
120	File ready F_FR_NA_1
121	Section ready F_SR_NA_1
122	Call directory, select file, call file, call section F_SC_NA_1
123	Last section, last segment F_LS_NA_1
124	Ack file, Ack section F_AF_NA_1
125	Segment F_SG_NA_1
126	F_DR_TA_1
127	QueryLog - Request archive file F_SC_NB_1

12.7 Modbus

Modbus is a communications protocol designed by Modicon Incorporated for use with its PLCs.

The profiles specify function codes and register or coil addresses. The function code in the protocol Modbus TCP specifies the purpose of the data transfer. The device blocks the data packets that violate the specified profiles. If an error is detected, then the device terminates the data connection upon user request. The predefined function code lists and the function code generator support you when specifying the function codes.

When the Modbus Enforcer profile is active (enabled checkbox is marked), the device applies the profiles to the data stream.

- The device permits data packets containing only the function codes specified in the Function code field.
- The device rejects the data packets containing any other function codes that are not specified in the Function code field.

You can find the Modbus protocol at **Firewall** → **Enforcer** → **Modbus**.

12.7.1 Modbus Settings

Enabled Whether the Modbus enforcer is active or not.

Possible values:

- **Enabled**
- **Disabled** (default setting)

Name Name of the Modbus enforcer.

Possible values:

- **Character string** with 0..100 characters

Description Description of the Modbus enforcer.

Possible values:

- **Character string** with 0..250 characters

Unit identifier Specifies the Modbus TCP identification unit for the Modbus Enforcer profile.

Possible values:

- **<empty>** (default setting)

The device permits data packets without an identification unit.

- **0..255**

The device permits data packets with the specified identification unit.

The field lets you specify the following options:

- A single Modbus TCP identification unit with a single numerical value, for example 1.
- Multiple Modbus TCP identification units with numerical values separated by a comma, for example 1,2,3.

TCP Reset Activates/deactivates the resetting of the TCP connection in case of a protocol violation or if the plausibility check detects an error.

Possible values:

- **enabled** (default setting)

The resetting of the TCP connection is active.

If the device identifies a protocol violation or detects a plausibility check error, then the device terminates the TCP connection. The device establishes the TCP connection again on receiving a new request.

- **disabled**

The resetting of the TCP connection is inactive.

Sanity Check Activates/deactivates the plausibility check for the data packets.

Possible values:

- **enabled** (default setting)

The plausibility check is active.

The device checks the plausibility of the data packets regarding format and specification.

The device blocks the data packets that violate the specified profiles.

- **disabled**

The plausibility check is inactive.

Exception Activates/deactivates the sending of an exception response in case of a protocol violation or if the plausibility check identifies errors.

Possible values:

- **enabled*** (default setting)

The sending of an exception response is active.

If the device identifies a protocol violation or a plausibility check error, then the device sends an exception response to the end points and terminates the Modbus TCP connection.

- **disabled**

The sending of an exception response is inactive. The Modbus TCP connection remains established.

Preset Preset of Modbus rules.

Possible values:

- **Read Only** (default setting)

Assigns the function codes for the read function of the Modbus TCP protocol.

1,2,3,4,7,11,12,17,20,24

- **Read Write**

Assigns the function codes for the read/write functions of the Modbus TCP protocol.

1,2,3,4,5,6,7,11,12,15,16,17,20,21,22,23,24

- **Programming**

Assigns the function codes for the programming functions of the Modbus TCP protocol.

1,2,3,4,5,6,7,11,12,15,16,17,20,21,22,23,24,40,42,90,125,126

- **All**

Assigns the function codes for every function of the Modbus TCP protocol.

1,2,...,254,255

- **Custom**

Lets you specify user-defined values in the Function code field.

12.7.2 Modbus Rules

Name	Description	Function Codes	Read Address	Write Address	Actions
Read Coils	Read Only	1 (Read Coils)	0 - 49999	-	  
Read Discrete Inputs	Read Only	2 (Read Discrete Inputs)	0 - 49999	-	  
Read Multiple Holding Registers	Read Only	3 (Read Multiple Holding Registers)	0 - 49999	-	  
Read Input Registers	Read Only	4 (Read Input Registers)	0 - 49999	-	  
Read Exception Status	Read Only	7 (Read Exception Status)	0 - 49999	-	  
Get Comm Event Counter	Read Only	11 (Get Comm Event Counter)	0 - 49999	-	  
Get Comm Event Log	Read Only	12 (Get Comm Event Log)	0 - 49999	-	  
Report Slave ID	Read Only	17 (Report Slave ID)	0 - 49999	-	  
Read File Record	Read Only	20 (Read File Record)	0 - 49999	-	  
Read FIFO Queue	Read Only	24 (Read FIFO Queue)	0 - 49999	-	  

[+ Create Rule](#)

Name Name of the Modbus rule.

Possible values:

- **Character string** with 0..100 characters

Description Description of the Modbus rule.

Possible values:

- **Character string** with 0..250 characters

Description Description of the Modbus rule.

Possible values:

- **Character string** with 0..250 characters

Function code Possible values:

- **0..255**

Read Address Start Default is 0.

Possible values:

- **0..65535** ($2^{16}-1$)

Read Address Length Default is 1.

Possible values:

- **0..65535** ($2^{16}-1$)

Write Address Start Default is 0.

Possible values:

- **0..65535** ($2^{16}-1$)

Write Address Length Default is 1.

Possible values:

- **0..65535** ($2^{16}-1$)

12.7.3 Modbus Function Codes

#	Meaning	Address range (read)	Address range (write)
1	Read Coils	<0..65535>	-
2	Read Discrete Inputs	<0..65535>	-
3	Read Holding Registers	<0..65535>	-
4	Read Input Registers	<0..65535>	-
5	Write Single Coil	-	<0..65535>
6	Write Single Register	-	<0..65535>
7	Read Exception Status	-	-
8	Diagnostic	-	-
11	Get Comm Event Counter	-	-
12	Get Comm Event Log	-	-
13	Program (584/984)	-	-
14	Poll (584/984)	-	-
15	Write Multiple Coils	-	<0..65535>
16	Write Multiple Registers	-	<0..65535>
17	Report Slave ID	-	-
20	Read File Record	-	-
21	Write File Record	-	-
22	Mask Write Register	-	<0..65535>
23	Read/Write Multiple Registers	<0..65535>	<0..65535>
24	Read FIFO Queue	<0..65535>	-
40	Program (Concept)	-	-
42	Concept Symbol Table	-	-
43	Encapsulated Interface Transport	-	-
48	Advantech Co. Ltd. - Management Functions	-	-
66	Scan Data Inc. - Expanded Read Holding Registers	-	-
67	Scan Data Inc. - Expanded Write Holding Registers	-	-
90	Unity Programming/OFS	-	-
100	Scattered Register Read	-	-
125	Schneider Electric - Firmware	-	-

12.8 OPC

OPC stands for OLE for Process Control. A standard based on OLE, COM and DCOM for accessing process control information on Microsoft Windows systems.

The OPC is an integration protocol for industrial environments. The OPC Enforcer is a function that supports the network security. The device blocks the data packets that violate the specified profiles. Upon user request, the device verifies the data packets for their plausibility and their fragment characteristics. The device verifies and observes OPC data connections and helps protect against invalid or fake data packets. The function dynamically activates TCP ports for each data connection. When requested by an OPC server, the device sets up the data connection only between the OPC server and the related OPC client.

The prerequisite is that authentication level 5 or lower is set up in your end device to perform the Deep Packet Inspection (DPI). The end device can be a computer or any other equipment capable of sending OPC data packets. The authentication level defines the type of authentication required for an OPC client to connect with an OPC server.

The device removes the state information from the packet filter on the following events:

- When applying the profiles saved in the device to the data stream.

- When activating/deactivating the Routing function on a router interface.

This includes potential DCE RPC information of the OPC Enforcer. In the process, the device interrupts open communication connections.

You can find the OPC protocol at **Firewall** → **Enforcer** → **OPC**.

12.8.1 OPC Settings

Enabled Whether the OPC enforcer is active or not.

Possible values:

- **Enabled**
- **Disabled** (default setting)

Name Name of the OPC enforcer.

Possible values:

- **Character string** with 0..100 characters

Description Description of the OPC enforcer.

Possible values:

- **Character string** with 0..250 characters

Sanity Check Activates/deactivates the plausibility check for the data packets.

Possible values:

- **Enabled** (default setting)

The plausibility check is active.

The device checks the plausibility of the data packets regarding format and specification.

The device blocks the data packets that violate the specified profiles.

- **Disabled**

The plausibility check is inactive.

Fragment Check Activates/deactivates the fragment check for the data packets.

Possible values:

- **Enabled** (default setting)

The fragment check is active.

The device checks the data packets for fragment characteristics.

- **Disabled**

The fragment check is inactive.

Timeout Connect Specifies the time in seconds after which the device removes the dynamic TCP ports, if there is no longer an active OPC data connection on the dynamic TCP ports.

Possible values:

- **1..300** (default setting: 5)
- **0**

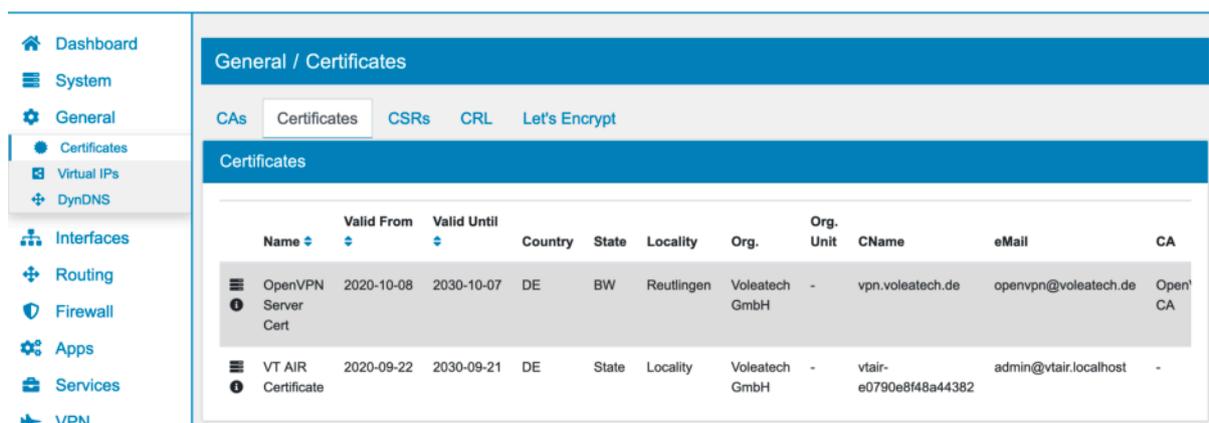
The value 0 deactivates the function.

The OPC data connection remains set up without a time limit.

CERTIFICATES

13.1 Certificate

You can find the Certificate Settings at **General** → **Certificates** → **Certificate**.



A **Certificate** verifies ones digital identity in the network.

On the certificates screen you can export the certificate and its private key in X.509 PEM format. Please be very careful with the private key. If it compromised the Certificate needs to be suspended.

The certificate name has to be a unique name, which means that it's not used by another certificate in the system. A certificate has a **type** which is either *server* or *user*. The type can not be changed later on and special attributes are added to the certificate depending on the **type** that might affect its usage.

There are three different **methods** to create a certificate.

- Create Certificate
- Import Certificate
- Import P12

Country	The country where the company is registered
State or Province	The state or province where the company is located
City	The city where the company is located
Organization	The company name
Organizational Unit	The department of the company
Common Name	Usually the domain name, host name or URL of the company
Email Address	An email address to contact the company

13.2 CA

You can find the CA Settings at **General** → **Certificates** → **CAs**.

The **Certificates Authority** is the entity that issues certificates to verify ones digital identity in the network.

On the CAs screen you can edit CAs and export their certificate and private key in X.509 PEM format. Please be very careful with the private key. If the key is compromised the CA needs to be suspended.

When you want to create a CA you have to give it a unique name, which is not yet used by another CA in the system. There are three different **methods** to create a CA.

- Create Certificate Authority
- Create intermediate Certificate Authority
- Import Certificate Authority

When you edit a certificate authority you can define the **Next Serial Number**. This value will be used if you create a certificate with this certificate authority.

Country	The country where the company is registered
State or Province	The state or province where the company is located
City	The city where the company is located
Organization	The company name
Organizational Unit	The department of the company
Common Name	Usually the domain name, host name or URL of the company
Email Address	An email address to contact the company

13.3 CSR

You can find the CSR Settings at **General** → **Certificates** → **CSR**.

The **Certificate Signing Request** is an unsigned certificate which needs to be sent to a CA to apply for a digital identity certificate.

There are two different **methods** to create a CSR.

- Create CSR
- Import CSR

Country	The country where the company is registered
State or Province	The state or province where the company is located
City	The city where the company is located
Organization	The company name
Organizational Unit	The department of the company
Common Name	Usually the domain name, host name or URL of the company
Email Address	An email address to contact the company

When importing a CSR you need to copy the entire CSR as text into the field and save it.

13.3.1 Sign with Certificate Authority

To sign a CSR with a Certificate Authority you need to create a Certificate Authority and CSR and save it. When you edit the CSR, you can choose **Sign With** and select a Certificate Authority.

The screenshot shows a configuration window for a CSR. On the left, there is a sidebar with a 'Country' field set to 'DE'. The main area contains the following fields:

- Private key:** A text area containing a long alphanumeric string starting with '-----BEGIN PRIVATE KEY-----' and ending with '-----END PRIVATE KEY-----'.
- Sign With:** A dropdown menu set to 'Certificate Authority'.
- Certificate Authority:** A dropdown menu set to 'OpenVPN CA'.
- Type:** A dropdown menu set to 'Server'.
- Valid Days:** A numeric input field set to '3650'.

At the bottom of the main area are 'Save' and 'Cancel' buttons. On the right side of the window, there is a sidebar with an 'eMail' field set to 's@s.de'.

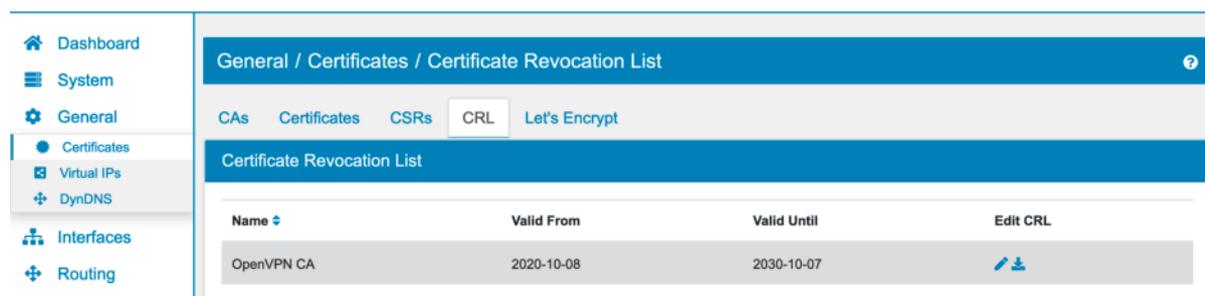
Type can be either *Server* or *User*.

You can also change **Valid Days**, which is 3650 by default.

After those settings are saved you can click on the **Sign via Certificate Authority** icon in the actions column on the CSR overview page. This will create a new certificate object and also copy the created certificate into the CSR certificate field.

13.4 CRL

You can find the CRL Settings at **General** → **Certificates** → **CRL**.



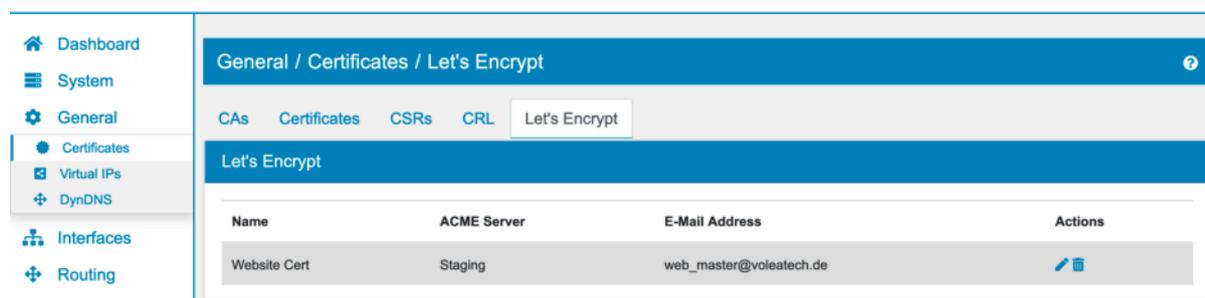
The **Certificate Revocation List** is a list of certificates of a certificate authority that should no longer be trusted.

When a certificate gets revoked the current datetime is saved. There are several revocation reasons available to choose from:

- Unspecified
- CA compromised
- Key compromised
- Affiliation changed
- Superseded
- Cessation of operation
- On Hold

13.5 Let's Encrypt

You can find the Let's Encrypt Settings at **General** → **Certificates** → **Let's Encrypt**.



Let's Encrypt is a non-profit certificate authority that provides free certificates for domain owners.

13.5.1 Create Let's Encrypt Account

First you need to create a new *Let's Encrypt* account entry. The account is used to create certificates and the certificates are registered under this account. An account is free and only used to organize your certificates with *Let's Encrypt*. Be aware that you need the account to revoke an issued certificate.

Name so you can identify it.

ACME Server can be either *Staging (ACME v2)* for testing purposes, *Production (ACME v2)* or *Custom*.

Custom Server can be set up if *Custom* was selected for the *ACME Server*. This might be useful if you have a local certificate server that supports the ACME protocol.

Private Key will be generated automatically if none is provided.

E-Mail Address for contact purposes.

Auto Firewall Rule will create a temporary firewall rule to allow for the signing of the certificate. Otherwise port 80 has to be opened manually on the current WAN interface.

13.5.2 DNS Acme Handle

If you plan on using the DNS Authentication instead of web authentication you can create a DNS Acme Handle here. The handle will create a DNS entry that can be set dynamically by TBF and be used as CNAME entry for the actual domain that is being validated.

For example the DNS Handle looks like this:

```
177c0dc6-4d2e-486b-932e-db248b2dd123.auth.acme-dns.io
```

and can be added to the actual domain like this:

```
_acme-challenge.your-domain CNAME 177c0dc6-4d2e-486b-932e-db248b2dd123.auth.acme-dns.io.
```

TBF can not update the acme handle on certificate signing requests.

13.5.3 Sign Let's Encrypt Certificate

To sign a certificate you need to create a **CSR** and save it. When you edit it, you can select an existing *Let's Encrypt Account* as well as the authentication method. You can choose between *Web Authentication*, *DNS Authentication* and *Custom Script*.

On *Web Authentication* the Let's Encrypt Server will look for a file that is served by the domain's web-server. TBF will take care of that part as long as the domain's DNS entry is pointing to TBF.

Warning: Web Authentication requires the Web Interface of TBF to be listening on Port 80/443 on All Interfaces. If that is not the case, please use the DNS Authentication.

On *DNS Authentication* the Let's Encrypt Server will look for a DNS entry in the domain's DNS Entry. You need to choose an Acme Handle and create a CNAME entry for validation on the domain in question. TBF will take care of the authentication of the certificate.

On *Custom Script* there will be a textfield for you to save your own script.

On the *CSR overview page* there will be a *Sign* action button on the right side where you can sign the certificate. The new certificate will be created and can be found on the *Certificate overview page*.

In order for the signing process to work Port 80 on WAN must be open. The DNS entry for the certificate entry must also point to TBF so it is reachable during signing. The *Let's Encrypt* server will contact the TBF in order to check the validity of the DNS entry.

13.5.4 Renew Let's Encrypt Certificate

When a signed *Let's Encrypt* certificate is about to expire, you can renew it. If the certificate will be only 30 days or less valid, there is a *Renew* action button on the right side of the *Certificate overview page* for each signed certificate.

Also once per week a cron job will automatically renew all *Let's Encrypt* certificates which are about to expire.

13.5.5 Revoke Let's Encrypt Certificate

On the *Certificate* overview page there is a *Revoke* action button for each signed certificate. *Revoke* will revoke the certificate with letsencrypt. You can sign a new certificate for this domain afterwards.

VIRTUAL IPS

14.1 VRRP

You can find the VRRP Settings at **General** → **Virtual IPs**.



A VRRP IP is an IP that can also be shared with different machines. The master always holds the address, one or more secondary machines will be on standby and get the address if the Master is not online anymore.

All VRRP enabled machines communicate over multicast on the interface they are defined on. If a machine is not receiving multicasts from its neighbors it will assume the master role in order of their configured priority.

A VRRP IP can only be added on top of another IP on the same interface. It is highly recommended to use VRRP only with static IPs, DHCP IPs will work too but not receiving a DHCP IP will trigger an automatic failover.

VRRP uses the following destination IPs:

Note:

- IPv4: 224.0.0.18
 - IPv6: fe02::12
-

You can configure the Priority on the screen. The highest available number is always the Master.

A password must also be configured. It must match on all machines that share the address.

Default Active is either Primary or Secondary. This options allows for an Active/Active Cluster where part of the VRRP IPs are on the Primary firewall and part are on the Secondary firewall. Clients in the network need to have the different VRRPs as gateway. In a failover case one Firewall will hold all IPs.

Track Interface might be used to override the trackable interface for this VRRP IP. This is useful if you have a VRRP on top of a Bridge interface. The bridge itself only goes offline when all the interfaces are offline. This allows you to pin the failover event to a specific interface. By default it is always pinned to the underlying interface of the settings.

A disk failure will result in a VRRP service failover.

14.2 IP Alias

You can find the Virtual IP Settings at **General** → **Virtual IPs**.

An IP Alias is an additional IP on one of the interfaces.

You can define any IP you like. Please make sure to use the correct netmask for your use case. A netmask other than /32 will automatically create an interface route for the network as well.

14.3 Custom VRRP Scripts

You can add custom scripts to trigger a failover for the VRRP IPs. Scripts need to be executable and in the directory */etc/keepalived/scripts.d*. The exit code of the script is important, 0 means success and not 0 means failure. If one of the scripts in the folder fails, the entire VRRP daemon changes it's status to failed.

For example to failover if the bgp default route is not present anymore, you can use the following script.

```
#!/bin/bash  
  
ip r s | grep default | grep bgp
```

15.1 DynDNS

You can find the DynDNS Settings at **General** → **DynDNS**.

DynDNS can be used to have a DNS name for a dynamic IP. We currently support the following **Service Types**:

Note:

- DynDNS
 - Gandi
 - dnsHome
 - Strato
 - Custom Script
-

IP Type choose either IPv4 or IPv6

Connection can be an Interface and the according Interface IP, a Routing Table or Periodic Check. The Periodic Check runs every 2 minutes and checks if the IP address changed and the DynDNS will be executed. On Routing Table the current default gateway will be used as the IP. If the routing table has multiple gateways with the same ip, the active one that was created first is used.

Hostname including the domain (test.voleatech.com) that the IP should be assigned to.

Username if applicable to authenticate at the Service.

Password if applicable to authenticate at the Service.

Custom Script if you choose custom script as Service Type. This will be run with minimum user rights and should not access any system resources. There are environment variables that can be used in the script from the GUI values:

Note:

- USERNAME
 - PASSWORD
 - HOSTNAME
 - IPADDRESS
 - IP_TYPE
-

16.1 Routes

You can find the Route Settings at **Routing** → **Routes**.



A route is a static route that can be defined in the system.

You can **Enable** or disable a route. It will be automatically added and removed, according to the settings. This will be done on each route check.

You have to define a **Destination** which is a Network the route is pointing to. You can either have a **Gateway**, **Interface** or **Multipath** route.

Metric a route can have a metric. You can create multiple routes with the same destination as long as they have different metrics. A metric is like a priority for the route, the lowest metric route is always active in the system.

Source in the Advanced Settings you can choose to set a route source. This might be useful if the firewall itself needs to use the route and it has multiple IPs on the Interface the route is defined on.

Routing Table in the Advanced Settings you can select one or multiple routing tables. By default, each new route is automatically assigned the *Main* routing table (ID: 254).

Gateway Status Remove the route when the gateway status changes to down and add it when it changes to up. It is enabled by default. Disabling the option keeps the route even if the gateway is down from the monitoring check.

To change the routing tables see the documentation at [Routing Tables](#).

16.1.1 Gateway Route

Choose a Gateway that was previously created under [Gateway](#) or create a Gateway with the **ADD** button. The route will use the IP Address in the Gateway as destination. This is usually another Router.

16.1.2 Interface Route

Choose an Interface for the route. The route will be defined on that Interface. Please be aware that any Client in the destination network must be in the same L2 Network to be reachable.

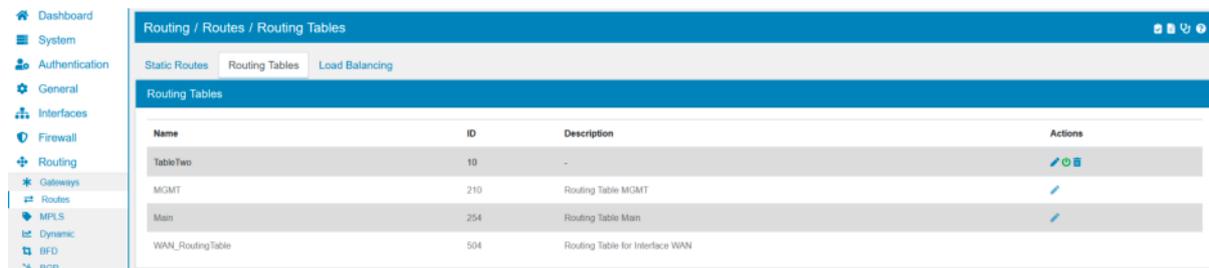
16.1.3 Multipath Route

Choose multiple Gateways and their metric to be used by the route. The Gateway check will be taken into account if the Gateway is up or down.

To change your BGP setup please go to **Routing** → **BGP** and refer to the documentation at [BGP](#).

16.2 Routing Tables

You can find the Routing Tables at **Routing** → **Routes** in the tab **Routing Tables**.



Name	ID	Description	Actions
TableTwo	10	-	Edit Delete Refresh
MGMT	210	Routing Table MGMT	Edit
Main	254	Routing Table Main	Edit
WAN_RoutingTable	504	Routing Table for Interface WAN	

The *Main* table with the ID 254 is a built in route and can not be deleted. Each new routing table needs a unique name and ID.

You can assign static routes to one or multiple routing tables when creating and editing static routes. See the documentation at [Routes](#).

Routing Tables are **additive** to the main routing table. They are queried before the main routing table if no match is found the main routing table is queried.

You can assign clients to a Routing Table through an Option in a Firewall Rule [Firewall Rules \(Forward and Input\)](#). Go to Advanced Settings and choose the Routing Table the matched clients should use.

When you created a routing table and edit it, you can link v4 and v6 gateways to the routing table. Each linked gateway has a priority between 1 and 100, where the lower the number the higher the priority.

The gateway with the highest priority will be created as default gateway in the system. If several gateways have the highest priority, they are treated as a multipath route and create a load balanced Internet connection. Be aware that the routing decision will only be made at the connection start and an open connection will never switch to a different Gateway. Please also check the [DNS Troubleshooting](#) for multipath Gateway scenarios.

You can change the weight of the multipath routes in the Gateway itself at [Gateway](#). For ECMP (Equal Cost Multipath Routing) you can set the weight equal for all gateways.

At the end of the edit screen the static routes which are linked to the selected routing table are listed.

Routing Tables can be used for *Policy Routing* in Firewall Rules.

16.3 Load Balancing

You can find the Load Balancing at **Routing** → **Routes** in the tab **Load Balancing**.

Load Balancing allows you to use multiple routing tables at the same time. This might be necessary to load balance over multiple Gateways.

Name so you can identify it.

Description is a description of the Load Balancing.

Policy can be either *Random*, *IP Source Address* or *IP Source Address + IP Destination Address*. It is *Random* by default. The policy decides on how each state is pinned to one *Routing Table*. A decision is made on state creation and the chosen *Routing Table* will stay the same for a connection for its lifetime.

Be aware that this can lead to problems with servers that require multiple open connections, as the source IP might not be the same for all connections when load balanced.

Multiple **Routing Tables** can be added with a **Priority** of 1 to 99.

Create Load Balancing ✕

Enabled

Name

Description

Policy

16.4 Gateway

You can find the Gateway Settings at **Routing** → **Gateways**.

Routing / Gateways					
Gateways					
Name	Interface	Gateway	Monitor IP	Description	Actions
OVPN_Site2Site_IPv4_DHCP	OVPN_Site2Site	DHCP	-	OVPN_Site2Site DHCP IPv4 Gateway	
SecondaryWANGateway	WAN	192.168.100.1	8.8.8.8	-	
WAN_IPv4_DHCP (Default)	WAN	192.168.10.1 (DHCP)	8.8.4.4	WAN DHCP IPv4 Gateway	
WAN_IPv6_DHCP (Default)	WAN	DHCP	-	WAN DHCP IPv6 Gateway	

A Gateway can be created here for either IPv4 or IPv6. By default interfaces with **DHCP**, **PPP** and **OpenVPN** will automatically get a Gateway created.

Each Gateway needs a unique **Name** for the **Interface** it can be found on and the **IP Address** of the Gateway. If you choose to make the Gateway your **Default Gateway**, please make sure that it is reachable by the Interface it is assigned on.

You need to have an IP Address on the Interface so it can be used. The system can only have one **Default Gateway** for IPv4 and IPv6 and any other default gateway will automatically be downgraded if you save a new **Default Gateway**.

You can also **Monitor** a Gateway. By default the **Gateway IP Address** will be pinged for the monitoring. You can choose to set an alternative IP under **Monitoring IP Address**. A Gateway that is down will be removed from all routes in the system.

Routing / Gateways / Create

General

Enabled

Name

Interface

Gateway IP

Default Gateway

Description

Monitoring

Force Gateway down

Always Up

Disable Monitoring

Monitoring IP Address

Advanced Settings

With the option **Force Gateway down** you can force the Gateway to be down.

If you want to keep the Gateway up, you can set **Always Up**. This will keep the Gateway check enabled.

If you **Disable Monitoring** the Gateway will also be always up and the Gateway Monitoring will be disabled as well.

Under **Advanced Settings** in Monitoring you can also configure the monitoring parameter.

The screenshot displays the 'Advanced Settings' section of a Gateway configuration page. At the top, there is a toggle switch for 'Advanced Settings' which is turned on. Below this, there are four input fields for monitoring parameters: 'Test Interval' (value: 1), 'Average Interval' (value: 60), 'Latency threshold' (value: 250), and 'Packet Loss threshold' (value: 25). Each input field has a help icon (question mark) to its left. Below these fields is a blue bar labeled 'Advanced'. Underneath the bar, there is an 'LB Weight' input field (value: 1) and a 'Master HASync No Overwrite' toggle switch which is turned off. At the bottom right of the configuration area, there are 'Save' and 'Cancel' buttons.

Test Interval how often a ping is send to the Monitoring IP in seconds.

Average Interval is used to determine if a Gateway is down. The average of the tests above in that timeframe will determine the state.

Latency treshold in the average interval determines if the Latency to the Monitoring IP is too long.

Packet Loss threshold determines if the Gateway is down if that amount of packages are lost in the average interval.

You can check up on the Gateway Status on either the Dashboard Widget or under **Diagnostics -> Gateways**.

16.4.1 Advanced

Metric if the Gateway is a default Gateway you can set the default routes metric here. If you are using BGP or OSPF and want to have a static kernel backup default route it is necessary to change the metric here. In that case change the metric to **4278198272** since the dynamic routing daemon (FRR) interprets kernel metrics as a combined admin distance (upper byte) and priority (lower 3 bytes). Thus the metric 4278198272 translates to [255/8192].

LB Weight for Gateway Load Balancing in a Routing Table. The weight will be used to determine how many packets in relation to another Gateway should be send. If there are two Gateways GW1 with *LB weight* 1 and GW2 with *LB weight* 2 then two packets will be send to GW2 and 1 packet to GW1. Be aware that this determination will only be used when a state is created and not during the flow of a state.

Master HASync No Overwrite to not sync any data to the Slave TBF. The Gateway will be created initially but not updated. This is useful if you need the Gateway but have a different IP or settings.

We have a Video Tutorial regarding the Gateway configuration:

16.5 MPLS

You can find the MPLS Settings at **Routing** → **MPLS**.

A MPLS route is a static MPLS route that can be defined in the system.

There are three types of MPLS routes:

- Encapsulation
- Label Switch
- Decapsulation

You can **Enable** or disable a MPLS route. It will be automatically added and removed, according to the settings. This will be done on each route check.

16.5.1 Encapsulate

The screenshot shows the configuration page for an MPLS route with the following settings:

- Enabled:** A toggle switch is turned on.
- Operation:** A dropdown menu is set to 'Encapsulate'.
- Destination Network:** A text input contains '1.2.3.0' and a dropdown menu is set to '32'.
- Gateways:** A dropdown menu is set to 'WAN DHCP IPv4 Gateway' and a numeric input is set to '1'.
- Encapsulation Labels:** A text input contains '100'. There is a red 'X' icon to the right and a green '+ Add' button below the input.
- Metric:** A numeric input is set to '10'.
- Routing Table:** A dropdown menu is set to 'Main'.
- Description:** A text input contains 'Description'.

Encapsulate pushes an MPLS label on a network route and sends it to a gateway.

You have to define a **Destination** which is a network the route is using. **Gateways** lets you select a gateway. You can only configure one gateway at the moment.

Encapsulation Label is the label that will be pushed on the packets before forwarding. You can define more than one label and they will be pushed in order they are defined.

Metric a route can have a metric. You can create multiple routes with the same destination as long as they have different metrics. A metric is like a priority for the route, the lowest metric route is always active in the system.

Routing Table in the Advanced Settings you can select one or multiple routing tables. By default, each new route is automatically assigned the *Main* routing table (ID: 254).

To change the routing tables see the documentation at [Routing Tables](#).

Encapsulate routes are added to the normal Routing Tables.

16.5.2 Label Switch

The screenshot shows the configuration page for a Label Switch. The breadcrumb is 'Routing / MPLS / Update'. The page title is 'General'. The configuration includes:

- Enabled:** A red toggle switch is turned on.
- Operation:** A dropdown menu is set to 'Label Switch'.
- Gateways:** A dropdown menu is set to 'WAN DHCP IPv4 Gateway' with a count of '1'.
- Decapsulation Label:** A dropdown menu is set to '100'.
- Encapsulation Labels:** A dropdown menu is set to 'Label' with a red 'X' icon to the right and a green '+ Add' button below it.
- Description:** A text input field contains the word 'Description'.

Switches one label to one or more other labels and forwards the packets to a Gateway.

You need to define one **Gateway**, you can only configure one gateway at the moment.

Decapsulation Label is the label that will be popped from the packets before encapsulation.

Encapsulation Label is the label that will be pushed on the packets before forwarding. You can define more than one label and they will be pushed in order they are defined.

Label Switch routes are added to the MPLS Routing Tables.

16.5.3 Decapsulation

The screenshot shows the configuration page for Decapsulation. The breadcrumb is 'Routing / MPLS / Update'. The page title is 'General'. The configuration includes:

- Enabled:** A red toggle switch is turned on.
- Operation:** A dropdown menu is set to 'Decapsulate'.
- Type:** Radio buttons are present for 'Gateway' (selected) and 'Interface'.
- Gateways:** A dropdown menu is set to 'WAN DHCP IPv4 Gateway' with a count of '1'.
- Decapsulation Label:** A dropdown menu is set to '100'.
- Description:** A text input field contains the word 'Description'.

Removes a label from a packet and forwards it to an **Interface** or **Gateway**.

You can only configure one gateway at the moment.

Decapsulation Label is the label that will be popped from the packets before forwarding.

Decapsulation routes are added to the MPLS Routing Tables.

16.5.4 LDP

The **Label Distribution Protocol** allows routers of Multiprotocol Label Switching (MPLS) to exchange label mapping information dynamically.

On the page the LDP can be enabled or disabled.

Router ID will be set automatically if empty.

Interfaces can be specified.

Discovery Transport Address is the Discovery Transport Address and can be selected as Network Object.

Address Family can be *IPv4* or *IPv6*. It is *IPv4* be default.

You can create multiple **LDP Neighbors**. They have an **IP Address** and a **Password**.

16.6 Dynamic

You can configure Dynamic Routing settings in TBF. We use **FRR** to configure the settings in the background.

Please feel free to also look at the extended fr documentation [FRR User Guide](#).

We support *BGP*, *OSPF*, *OSPFv6*, *ISIS* and *BFD*.

16.6.1 General Settings

Please always set a console password. You will usually not need it but leaving the console without password leaves you open for security risks.

In order to connect to FRR from the console or bash, you can always use the **vtys** command without any password.

You can also set **Custom Options** under the advanced settings. They will be copied into the config file on the highest level.

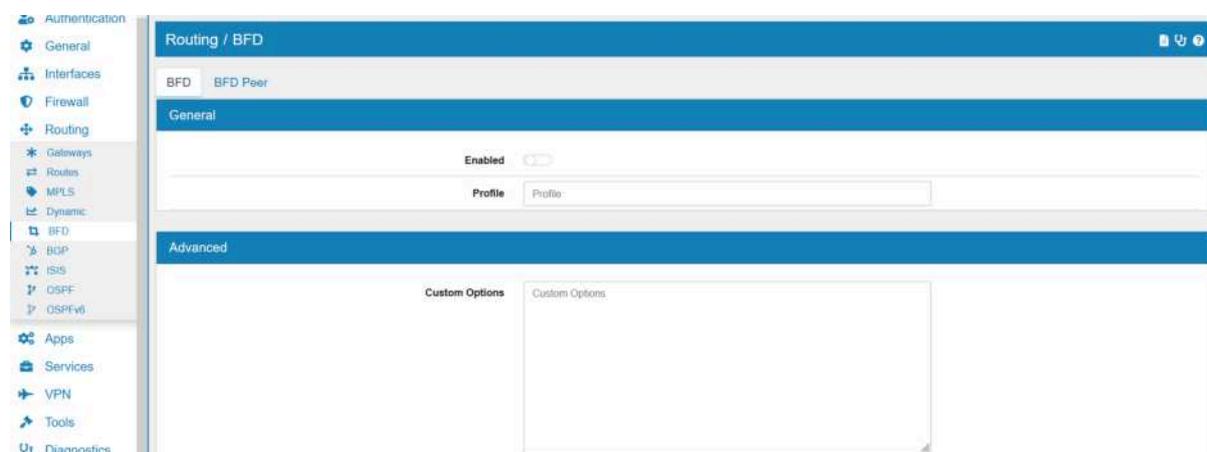
16.6.2 Administrative Distance

Administrative distance allows the dynamic routing daemon (FRR) to make decisions about what routes should be installed in the rib based upon the originating protocol. The lowest Admin Distance is the route selected. This is purely a subjective decision about ordering and care has been taken to choose the same distances that other routing suites have chosen.

Protocol	Distance
System	0
Kernel	0
Static	1
EBGP	20
OSPF	110
ISIS	115
IBGP	200

Routes are added based on their admin distance and if having the same admin distance the metric decides the route. Routes are always added to the TBF main routing table with a metric of 20, the internal metric kept in the dynamic routing daemon is not used to create the route. The internal metric is only for bookkeeping purposes and to redistribute routes to other peers.

16.7 BFD



BGP stands for Bidirectional Forwarding Detection and is a network protocol that is used to detect faults between two routers.

You can find the BFD Settings at **Routing** → **BFD**.

Profile can be set.

Custom Options can be used for custom configuration parameters for the config.

16.7.1 BFD Peer

A BFD Peer can be defined under **Routing** → **BFD** → **BFD Peer**.

IP Address of the Peer.

Profile if different from Default BFP Profile.

Multihop option.

16.8 BGP

BGP stands for a Border Gateway Protocol. The latest BGP version is 4. It is referred to as BGP-4. BGP-4 is one of the Exterior Gateway Protocols and de-facto standard of Inter Domain routing protocol. BGP-4 is described in RFC 1771.

You can find the BGP Settings at **Routing** → **BGP**.

You can set a **Router ID** that is advertised or let the system configure one automatically.

AS Number is an identification of autonomous system and must be unique within your AS.

Redistribute Kernel Routes lets BGP automatically distribute Kernel Routes.

Redistribute Static Routes lets BGP automatically distribute Static Routes.

Redistribute Connected Routes lets BGP automatically distribute Connected Routes.

Custom Options can be used for custom configuration parameters for the config.

Please be aware that TBF static routes are classified as kernel routes.

Networks let you advertise additional networks. You can advertise as many extra networks as you like.

16.8.1 BGP Neighbor

Each BGP Instance that you want to communicate with needs to be created as a Neighbor under **Routing** → **BGP** → **BGP Neighbor**.

Neighbor is the IP Address of the neighbor.

AS Number is the AS number of the neighbor.

IP Type the neighbor should should advertise with us. It is either IPv4, IPv6 or both.

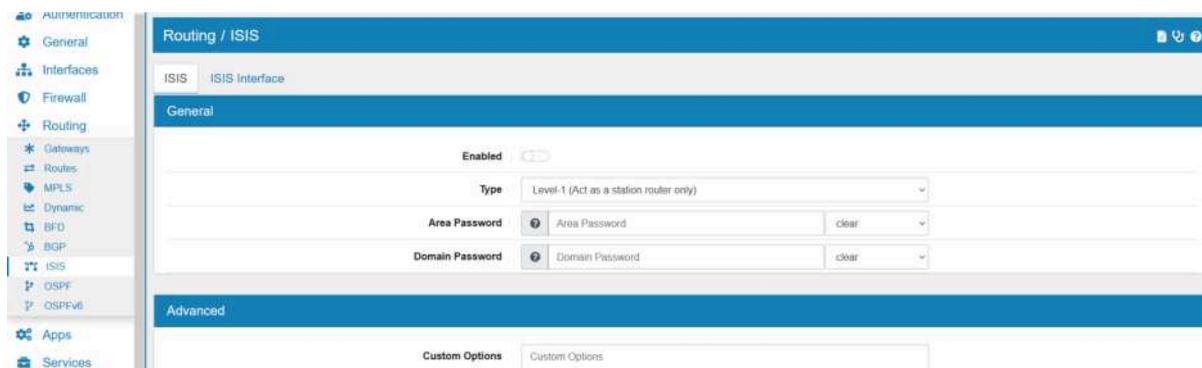
Advanced Settings have a lot of options to customize the neighbor relationship. Please refer to the FRR manual for a detailed explanation [FRR BGP](#).

Input Filter allows you to set an [Access List](#), [Prefix List](#) or [Route Map](#) as a filter for incoming advertised routes from this neighbor.

Output Filter allows you to set an [Access List](#), [Prefix List](#) or [Route Map](#) as a filter for outgoing advertised routes.

Custom Options can be used for custom configuration parameters for the config.

16.9 ISIS



ISIS stands for Intermediate System to Intermediate System and is a routing protocol designed to move information efficiently within a network.

You can find the ISIS Settings at **Routing** → **ISIS**.

Area Password is the Authentication password for an area.

Area Password Type can be either *clear* or *md5* and is *clear* by default.

Domain Password is the Authentication password for a domain.

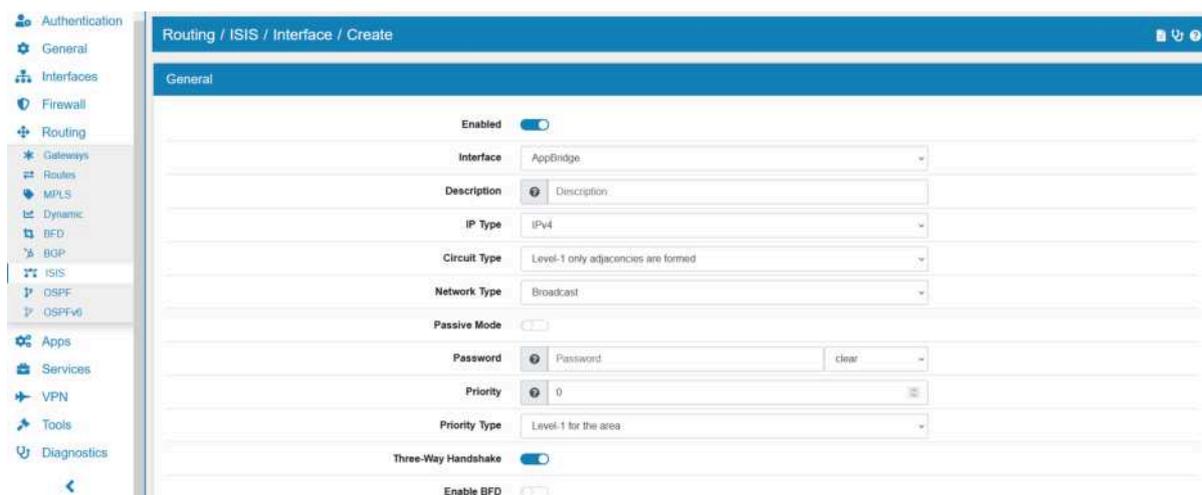
Domain Password Type can be either *clear* or *md5* and is *clear* by default.

Type is one of the three following:

- Level-1 (Act as a station router only)
- Level-1-2 (Act as both a station router and an area router)
- Level-2-Only (Act as an area router only)

Custom Options can be used for custom configuration parameters for the config.

16.9.1 ISIS Interface



An ISIS Interface can be defined under **Routing** → **ISIS** → **ISIS Interface**.

Interface the interface to use.

IP Type is either IPv4 or IPv6.

Circuit Type is one of the three following:

- Level-1 (only adjancencies are formed)
- Level-1-2 (adjancencies are formed)
- Level-2-Only (only adjancencies are formed)

Network Type is either Broadcast or Point-to-Point.

Passive Mode to configure the interface as passive.

Password and if it is cleartext or MD5.

Priority for designated router election.

Priority Type is either Level 1 for the area or Level 2 for the domain.

Three Way Handshake for P2P adjancencies.

Enable BFD for BFD support.

Custom Options can be used for custom configuration parameters for the config.

16.10 OSPF

The screenshot displays the OSPF configuration interface. On the left is a navigation menu with categories: System, General, Interfaces, Routing, Gateways, Routes, Dynamic, BGP, OSPF, OSPFv6, Firewall, Apps, Services, and VPN. The main content area is split into two tabs: 'General' and 'Routes'.

General Tab:

- Enabled:** A toggle switch that is currently turned off.
- Router ID:** A text input field containing 'Router ID'.
- Main Area:** A text input field containing 'Main Area'.
- VRRP Master Only:** A toggle switch that is currently turned off.
- Log Adjacency Settings:** A toggle switch that is currently turned off.

Routes Tab:

- Redistribute Kernel Routes:** A toggle switch that is currently turned on.
- Redistribute Static Routes:** A toggle switch that is currently turned off.
- Redistribute Connected Routes:** A toggle switch that is currently turned on.
- Redistribute Default Route:** A toggle switch that is currently turned off.
- Default Route Route Map:** A dropdown menu currently showing '-----'.
- Networks:** A list of networks with a '+ Add' button. The first entry is 'Network / 24' with a 'Network Area' dropdown and a red 'X' icon.

OSPF version 2 is a routing protocol which is described in RFC 2328. OSPF is for IPv4 only. OSPF is an IGP. Compared with RIP, OSPF can provide scalable network support and faster convergence times. OSPF is widely used in large networks such as ISP backbone and enterprise networks.

You can find the OSPF Settings at **Routing** → **OSPF**.

You can set a **Router ID** that is advertised or let the system configure one automatically.

Main Area the main Area of this OSPF instance.

Redistribute Kernel Routes lets OSPF automatically distribute Kernel Routes.

Redistribute Static Routes lets OSPF automatically distribute Static Routes.

Redistribute Connected Routes lets OSPF automatically distribute Connected Routes.

Please be aware that TBF static routes are classified as kernel routes.

Default Route Route Map lets you filter the default route with a *Route Map*.

Networks let you specify which interface will be advertised if it is in that network. Please be aware that OSPF only advertises networks that the host system has an IP address in. You can not advertise random networks.

Custom Options can be used for custom configuration parameters for the config.

16.10.1 OSPF Interface

Each OSPF Interface that you want to advertise needs to be defined under **Routing** → **OSPF** → **OSPF Interface**.

Interface sets the interface and can only be used once.

Network Type will be detected automatically but you can override it here.

Interface Area must be set to the correct area of the interface.

Metric for this interface if you want to override it.

Passive disabled OSPF packets on this interface. The routes of this interface will be advertised on other interfaces but this interface will not detect any other OSPF members.

MTU Ignore can be used to ignore the MTU mismatch.

Priority for the DR selection.

Enable BFD can be enabled or disabled.

Enable MD5 sets OSPF authentication key to a cryptographic password.

MD5 Password is the password for this Interface. Must be 16 characters or less. The corresponding key ID will be 1.

Custom Options can be used for custom configuration parameters for the config.

16.10.2 OSPF Area

An OSPF Area can be defined under **Routing** → **OSPF** → **OSPF Area**. The default area from the main OSPF page will be available in the normal mode without adding it here.

Main Area is the main Area of this OSPF Area. It is usually 0.0.0.0.

Area Type can be *Normal (default)*, *Stub Area (stub)*, *Totally Stub (stub no-summary)*, *Not so Stub Area (nssa)* or *Not so Totally Stub Area (nssa no-summary)*.

Description for custom description.

16.11 OSPFv6

OSPF version 3 (OSPFv6) is a routing protocol which is described in RFC 2740. OSPFv6 is for IPv6 only. It is not implemented completely and might lack some features.

You can find the OSPFv6 Settings at **Routing** → **OSPFv6**.

You can set a **Router ID** that is advertised or let the system configure one automatically.

Main Area the main Area of this OSPF instance.

Redistribute Kernel Routes lets OSPFv6 automatically distribute Kernel Routes.

Redistribute Static Routes lets OSPFv6 automatically distribute Static Routes.

Redistribute Connected Routes lets OSPFv6 automatically distribute Connected Routes.

Please be aware that TBF static routes are classified as kernel routes.

Networks let you specify which interface will be advertised if it is in that network. Please be aware that OSPFv6 only advertises networks, that the host system has an IP address in. You can not advertise random networks.

Custom Options can be used for custom configuration parameters for the config.

16.11.1 OSPFv6 Interface

The screenshot shows the configuration page for an OSPFv6 Interface. The left sidebar contains a navigation menu with categories like System, Firewall, Routing, and Apps. The main content area is split into two tabs: 'General' and 'Advanced'.

General Tab:

- Enabled:** A toggle switch that is currently turned on.
- Interface:** A dropdown menu showing 'AppBridge'.
- Network Type:** A dropdown menu showing 'Automatic'.
- Interface Area:** A text input field containing 'Interface Area'.
- Description:** A text input field containing 'Description'.

Advanced Tab:

- Metric:** A text input field containing 'Metric'.
- Passive:** A toggle switch that is currently turned on.
- MTU Ignore:** A toggle switch that is currently turned on.
- Priority:** A text input field containing 'Priority'.
- Enable BFD:** A toggle switch that is currently turned on.
- Custom Options:** A large text area for entering custom configuration parameters.

Each OSPFv6 Interface that you want to advertise needs to be defined under **Routing** → **OSPFv6** → **OSPFv6 Interface**.

Interface sets the interface and can only be used once.

Network Type will be detected automatically but you can override it here.

Interface Area must be set to the correct area of the interface.

Metric for this interface if you want to override it.

MTU Ignore can be used to ignore the MTU mismatch.

Priority for the DR selection.

Enable BFD can be enabled or disabled.

Custom Options can be used for custom configuration parameters for the config.

16.12 Access List

The screenshot shows the configuration interface for creating an Access List. The left sidebar contains a navigation menu with categories like System, General, Interfaces, Routing, Gateways, Routes, Dynamic, BGP, OSPF, OSPFv6, Firewall, Apps, and Services. The main content area is titled 'Routing / Dynamic / Access List / Create'. It features a 'General' section with 'Name' and 'Description' input fields. Below that is a 'Networks' section with a 'Sequence' field, a 'Permit' dropdown menu, a 'Network' input field, and a mask field set to '32'. A green '+ Add' button is located at the bottom right of the 'Networks' section.

Access Lists are a simple filtering mechanism based on IP Address Range.

They can be found at **Routing** → **Dynamic** → **Access List**.

Each Access List must have a unique name and a list of IP Addresses/Ranges.

They are ordered by the **Sequence** number.

16.13 Prefix List

The screenshot shows the configuration interface for creating a Prefix List. The left sidebar is identical to the previous screenshot. The main content area is titled 'Routing / Dynamic / Prefix List / Create'. It features a 'General' section with 'Name' and 'Description' input fields. Below that is a 'Prefixes' section with a 'Sequence' field, a 'Permit' dropdown menu, a 'Network' input field, a mask field set to '32', and two additional fields: 'Minimum N' and 'Maximum N'. A green '+ Add' button is located at the bottom right of the 'Prefixes' section.

Prefix Lists are an advanced filtering mechanism based on IP Address Range.

They can be found at **Routing** → **Dynamic** → **Prefix List**.

Each Prefix List must have a unique name and a list of IP Addresses/Ranges.

They are ordered by the **Sequence** number.

Action can either be set to Permit or Deny. A mix of both is possible in a Prefix List.

Minimum Mask is for a range of IP Ranges to be filtered. The prefix list will be applied if the prefix length is less than or equal to the *le* prefix length. This number must be bigger than the Network Mask.

Maximum Mask is for a range of IP Ranges to be filtered. The prefix list will be applied if the prefix length is greater than or equal to the *ge* prefix length. This number must be smaller than the Network Mask.

A Prefix List without the **Minimum Mask** or **Maximum Mask** is the same as an *Access List*.

16.14 Route Map

The image displays three sequential screenshots of the FRR web interface for configuring a Route Map. Each screenshot shows a left-hand navigation menu and a main configuration area.

General

Name	?	Name
Description	?	Description
Action		Permit
Sequence Number	?	Sequence Number
Call Route Map	?	-----
Exit Action	?	Exit

Match Settings

Access List	?	-----
Prefix List	?	-----
Local Preference	?	Local Preference
Metric	?	Metric
Next Hop IP	?	Next Hop IP
AS Path	?	AS Path
Community List	?	-----

Set Settings

Weight	?	Weight
Local Preference	?	Local Preference
Metric	?	Metric
Next Hop IP	?	Next Hop IP
Next Hop IPv6	?	Next Hop IPv6
AS Path	?	AS Path
Community	?	Community
Community Additive		<input type="checkbox"/>

Route Map are a advanced filtering mechanism based on different options.

They can be found at **Routing** → **Dynamic** → **Route Map**.

Route Maps can be chained or call a *Access List* and *Prefix List*.

They can also change the incoming or outgoing route settings e.g. **Weight** or **Metric**.

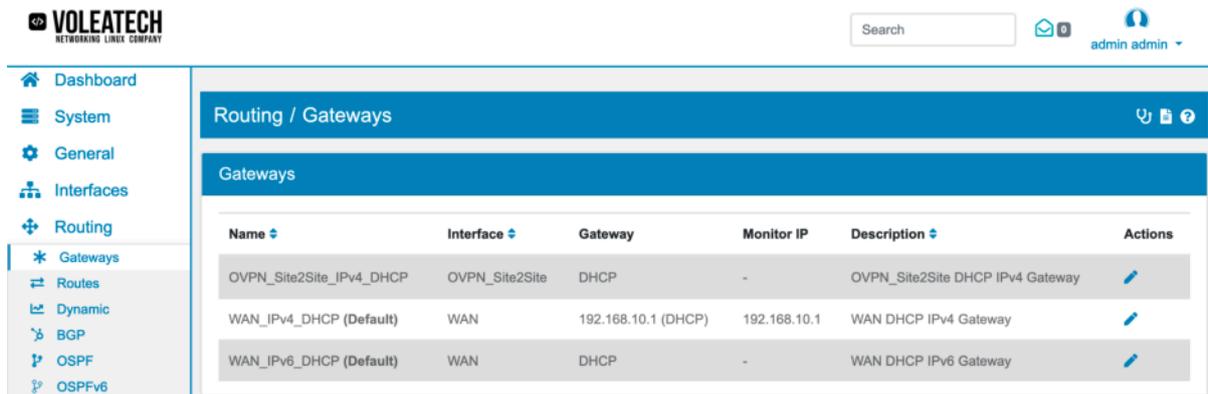
Please have a look at the FRR documentation for advanced descriptions [FRR Routemap](#).

16.15 Use Cases

16.15.1 Multi-Gateway Setup

If you have a setup where you have multiple internet connections from e.g. different ISPs, you can set up multiple Gateways for an Interface that switch automatically if one goes down.

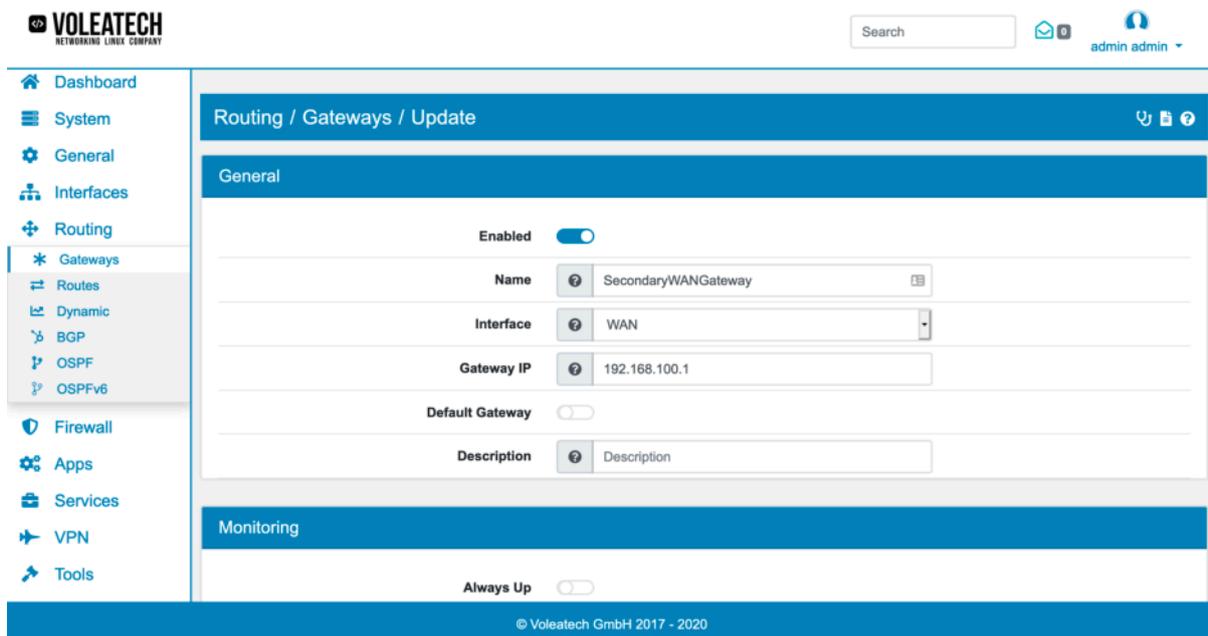
To do so go to **Routing -> Gateways**. Here you can see an overview of all the Gateways that are already configured.



The screenshot shows the Voleatech web interface. The left sidebar contains navigation options: Dashboard, System, General, Interfaces, Routing, Gateways (selected), Routes, Dynamic, BGP, OSPF, and OSPFv6. The main content area is titled 'Routing / Gateways' and shows a table of configured gateways.

Name	Interface	Gateway	Monitor IP	Description	Actions
OVPN_Site2Site_IPv4_DHCP	OVPN_Site2Site	DHCP	-	OVPN_Site2Site DHCP IPv4 Gateway	Edit
WAN_IPv4_DHCP (Default)	WAN	192.168.10.1 (DHCP)	192.168.10.1	WAN DHCP IPv4 Gateway	Edit
WAN_IPv6_DHCP (Default)	WAN	DHCP	-	WAN DHCP IPv6 Gateway	Edit

If you do not have your Gateways setup already, click **Add** to configure a new one. Enter your **Gateway IP** and enable **Default Gateway** if you want this one to be your primary Gateway.



The screenshot shows the Voleatech web interface for configuring a gateway. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Routing / Gateways / Update' and shows the 'General' configuration section.

General

- Enabled:
- Name: SecondaryWANGateway
- Interface: WAN
- Gateway IP: 192.168.100.1
- Default Gateway:
- Description: Description

Monitoring

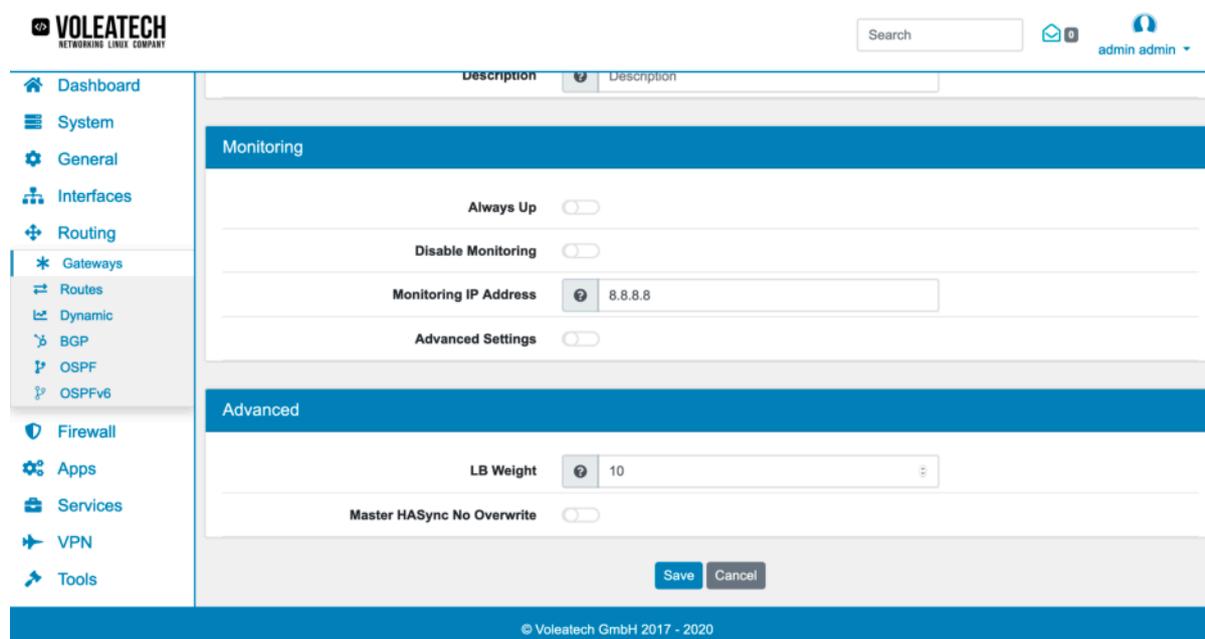
- Always Up:

© Voleatech GmbH 2017 - 2020

In the Monitoring section disable **Always Up** otherwise your TBF assumes that this Gateway is always operational and doesn't switch if the Gateway goes down. The **Monitoring IP address** should be a website (like Google) that is basically guaranteed to be up all the time. This way the system is able to determine whether the route is actually usable beyond your Gateway. You should use different IPs for each Gateway though.

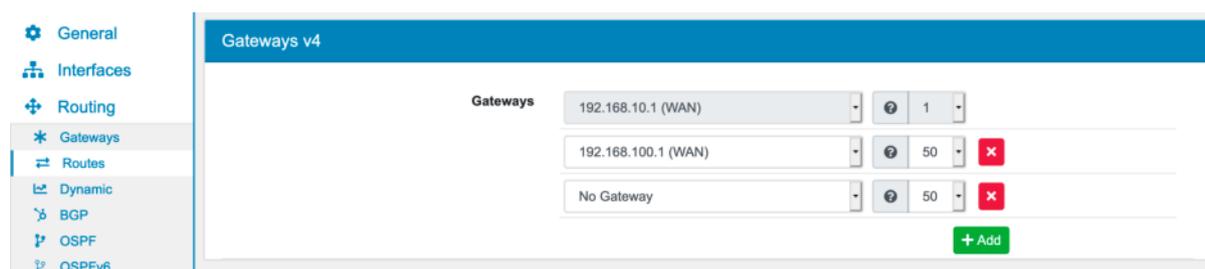
The ranking of the Gateway is determined by its weight factor **LB Weight**. Lower numbers are higher in importance.

Should you run a High Availability setup and you wish to have different Gateways between the Master and Slave devices you can also enable **Master HASync No Overwrite**.



Click **Save**. Next go to your already existing default Gateway and disable **Always Up** and enter a **Monitoring IP** outside of your network.

Go to **Routing** -> **Routes** -> **Routing Tables** and click **Edit** on your Main table. Add your newly created gateway in the Gateway section and assign a priority (lower numbers represent higher priorities).



16.15.2 Policy Routing

Routing tables can be used to create complex yet easy to maintain configurations in your TBF. You can for example route traffic through your main ISP (while the connection is up) but route your VoIP phone service through your secondary ISP.

To configure a setup like this you need to create a gateway for each of your WAN connections. See [Multi-Gateway Setup](#) for further details.

Go to **Routing** → **Routes** → **Routing Tables** and click **Add** to create a new Routing table. Under Gateways add your secondary gateway but not your primary gateway if your VoIP traffic is only allowed to be routed through your secondary ISP's connection. Click **Save**.

Go to **Firewall** → **Rules** → **WAN** and click **Add**. Configure a new Firewall Rule (*Firewall Rules (Forward and Input)*). Your new rule should contain a specific condition that acts as a switch between the different routing tables. If your phones have their own subnet for example select their subnet in the Source section. Your new rule should also be added to the *Top*.

In the **Advanced Settings** Panel you can select your new Routing table under **Routing Table**. Also consider activating the **Routing Table Reverse Main** option. Unlike your Main table your new table does not contain automatically created routes based on your interface configuration. So traffic might not have a route to flow in the reverse direction except you manually create a route in your new table or you force your TBF to use the Main table for the reverse direction (**Routing Table Reverse Main** option).

SERVICES

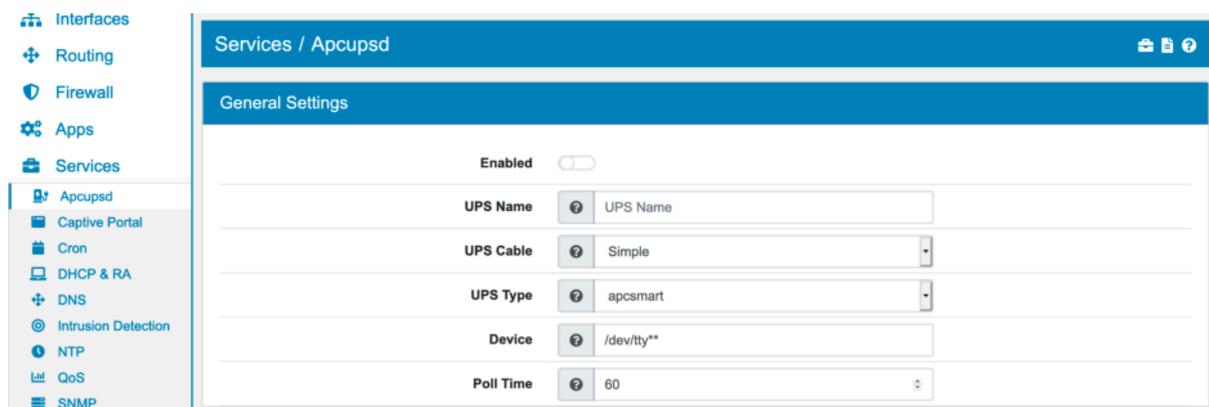
17.1 Apcupsd

You can find the Apcupsd Settings at **Services** → **Apcupsd**.

Apcupsd, short for American Power Conversion (APC) uninterruptible power supply (UPS) daemon, is a utility that allows the computer to interact with APC UPS.

Before you can use the Apcupsd it has to be installed. You can install it at **System** → **Addons**.

17.1.1 Settings



On the page the Apcupsd can be enabled or disabled.

UPS Name is used to give your UPS a name in log files and such. This is particularly useful if you have multiple UPSes.

UPS Cable defines the type of cable connecting the UPS to your computer. It can be *Simple*, *Smart*, *Ether*, *USB* or *Custom*.

UPS Cable Custom is selectable if *UPS Cable* is *Custom*. A specific cable model number may be used: 940-0119A, 940-0127A, 940-0128A, ...

UPS Type must define a UPSTYPE, which corresponds to the type of UPS you have. It can be *apcsmart*, *usb*, *net*, *snmp*, *netsnmp*, *dumb*, *pcnet* or *modbus*.

Device is different depending on the *UPS Type*.

- **apcsmart**: Newer serial character device, appropriate for SmartUPS models using a serial cable (not USB). Format: `/dev/tty**`
- **usb**: Most new UPSes are USB. A blank DEVICE setting enables autodetection, which is the best choice for most installations.

- **net**: Network link to a master apcupsd through apcupsd's Network Information Server. This is used if the UPS powering your computer is connected to a different computer for monitoring. Format: hostname:port
- **snmp**: SNMP network link to an SNMP-enabled UPS device. Hostname is the ip address or hostname of the UPS on the network. Vendor can be can be "APC" or "APC_NOTRAP". "APC_NOTRAP" will disable SNMP trap catching; you usually want "APC". Port is usually 161. Community is usually "private". Format: hostname:port:vendor:community
- **netsnmp**: Same as SNMP above but requires use of the net-snmp library. Unless you have a specific need for this old driver, you should use 'snmp' instead. Format: host-name:port:vendor:community
- **dumb**: Old serial character device for use with simple-signaling UPSes. Format: /dev/tty**
- **pcnet**: PowerChute Network Shutdown protocol which can be used as an alternative to SNMP with the AP9617 family of smart slot cards. ipaddr is the IP address of the UPS management card. username and passphrase are the credentials for which the card has been configured. port is the port number on which to listen for messages from the UPS, normally 3052. If this parameter is empty or missing, the default of 3052 will be used. Format: ipaddr:username:passphrase:port
- **modbus**: Serial device for use with newest SmartUPS models supporting the MODBUS protocol. Leave the DEVICE setting blank for MODBUS over USB or set to the serial number of the UPS to ensure that apcupsd binds to that particular unit (helpful if you have more than one USB UPS). Format: /dev/tty**

Poll Time is the interval (in seconds) at which apcupsd polls the UPS for status. Default is 60.

Power Failures Settings:

Setting	Value
OnBattery Delay	6
Battery Level	5
Minutes	3
Timeout	0
Annoy	300
Annoy Delay	60
Kill Delay	0

OnBattery Delay is the time in seconds from when a power failure is detected until we react to it with an onbattery event. Default is 6.

Battery Level is a time value. If during a power failure, the remaining battery percentage (as reported by the UPS) is below or equal to this value, apcupsd will initiate a system shutdown. Default is 5.

Minutes is a time value. If during a power failure, the remaining runtime in minutes (as calculated internally by the UPS) is below or equal to this value, apcupsd, will initiate a system shutdown. Default is 3.

Timeout is a time value. If during a power failure, the UPS has run on batteries for this value many seconds or longer, apcupsd will initiate a system shutdown. A value of 0 disables this timer. Default is 0.

Annoy is the time in seconds between annoying users to signoff prior to system shutdown. 0 disables. Default is 300.

Annoy Delay is the initial delay after power failure before warning users to get off the system. Default is 60.

Kill Delay If this value is non-zero, apcupsd will continue running after a shutdown has been requested, and after the specified time in seconds attempt to kill the power. This is for use on systems where

apcupsd cannot regain control after a shutdown. 0 disables (default).

UPS Sharing Settings:

The screenshot shows the 'UPS Sharing Settings' configuration page. On the left is a sidebar with navigation options: DNS, Intrusion Detection, NTP, QoS, SNMP, Startup Script, UPnP & NAT-PMP, and Webfilter. The main content area has a blue header 'UPS Sharing Settings'. Below the header are two dropdown menus: 'UPS Class' is set to 'Standalone' and 'UPS Mode' is set to 'Disable'. At the bottom right of the main area are 'Save' and 'Cancel' buttons.

UPS Class is normally standalone unless you share an UPS using an APC ShareUPS card. It can be **Standalone**, **Share Master** or **Share Slave**.

UPS Mode is normally disable unless you share an UPS using an APC ShareUPS card.

17.2 802.1X Authenticator

You can find the 802.1X Authenticator Settings at **Services** → **802.1X Auth.**.

802.1X Authenticator, authenticates devices on the layer 2 before they can access the network. The authentication can be done with a user/password or a certificate. This adds an extra Layer of security to your network as you can block out unknown devices.

Before you can use the 802.1X Authenticator it has to be installed. You can install it at **System** → **Addons**.

Upon activation on a network interface the **802.1X Authenticator** will block all forwarding traffic on the interface until a device is authenticated. The authenticated devices can be seen on the Diagnostics page [802.1X Authenticator](#).

Warning: DHCP Server can not be enabled on any interface when using 802.1X Authenticator. The 802.1X Authenticator is blocking the DHCP Server port and is not starting with an active DHCP Server. This is necessary for the 802.1X Authenticator to detect new devices on the network. Make sure to have another DHCP Server in the network

17.2.1 Settings

On the page the 802.1X Authenticator can be enabled or disabled. You can create an 802.1X Authenticator for each physical interface that you like.

The screenshot shows the 'Services / 802.1X Auth. / Create' configuration page. The left sidebar shows navigation options: Interfaces, Routing, Firewall, Apps, Services, 802.1X Auth., Captive Portal, Cron, DHCP & RA, DNS, and Intrusion Detection. The main content area has a blue header 'Services / 802.1X Auth. / Create'. Below the header is a section titled '802.1X Authenticator'. It contains an 'Enabled' toggle switch which is turned on. Below that are three input fields: 'Description' (empty), 'Interface' (set to 'WAN'), and 'Server Type' (set to 'EAP').

Server Type for authentication. Device authentication can either be sent to a radius server or the 802.1X Authenticator can act as an EAP Authentication Server.

Radius Authentication

An authentication radius server and an accounting radius server can be configured. All requests from devices will be relayed to the server and the result determines if a device is authenticated.

You need to add the radius server, the identifier of the 802.1X Authenticator and a shared secret.

EAP Authentication Server

The 802.1X Authenticator can act as an EAP Authentication Server.

Server Identity sets the identity used in the EAP Authentication.

Server Certificate is optional and must be set if you use certificate authentication

Check CRL for a certificate revocation list.

A device can be configured in the EAP Client list:

Username of the device

Password of the device

Authentication Algorithm the following algorithms are supported: MD5, PSK, MSCHAPV2, TLS, TTLS

Key Value Pairs can be set and sent to the device upon successful authentication. They are in the same format as a radius key/value pair.

17.3 Avahi

You can find the Avahi Settings at **Services** → **Avahi**.

Avahi is used to propagate Apple Services to different networks as the broadcast can not cross L2 otherwise.

Before you can use the Avahi it has to be installed. You can install it at **System** → **Addons**.

17.3.1 Settings

On the page the Avahi can be enabled or disabled.

Interfaces can be specified.

IP Type can be IPv4, IPv6 or both.

Reflection enables the Repetition of mDNS packets across subnets. Allows clients in one subnet to browse for services and clients located in different subnets.

Override Hostname is used for publishing mDNS records. The default is the system hostname.

Override Domain is used for publishing mDNS records. The default is "local".

17.4 Captive Portal

You can find the Captive Portal Settings at **Services** → **Captive Portal**.

Interfaces	MAC Allow (Source)	IP Allow (Source)	Host Allow (Destination)	Description	Actions
INT2	-	-	-	Guest Network	  

Captive Portal is used to authenticate users before they can access the Internet.

You can export the settings in the top right corner as an Excel spreadsheet.

17.4.1 Captive Portal Instance

Each instance of a captive portal can be bound to one or more interfaces. At the moment there is no user authentication implemented, only a checkbox will be checked to login the user.

The screenshot shows the configuration interface for a Captive Portal Instance. The settings are as follows:

- Enabled:**
- Interfaces:** WAN
- Idle Timeout:** 1 Days
- Description:** Guest Network
- Redirect URL:** https://captiveportal.voleatech.de
- Timeout:** 0
- HTTPS:**
- Mode:** Normal
- Use Voucher Authentication:**
- Main File:** Currently: captiveportal/799237ee-8198-4a1a-8aea-6c6ba0f96be6/index.html Clear
- Change:** No file selected.
- Download:**

Users are identified via their devices MAC Address, please make sure to only have a Layer 2 network connected to the Captive Portal interface.

Enabled to enable or disable the Instance

Interfaces can be specified.

Idle Timeout will logout the user if he did not send any new traffic within this time.

Redirect URL will redirect the user to this URL after successful authentication

Timeout the time (in minutes) a user stays logged in. Default is 0, which means no timeout

HTTPS to allow for the Captive Portal to run on HTTPS. A certificate must be selected as well. Be aware that the clients connecting must trust this certificate.

Mode can be *Normal* or *Redirect*.

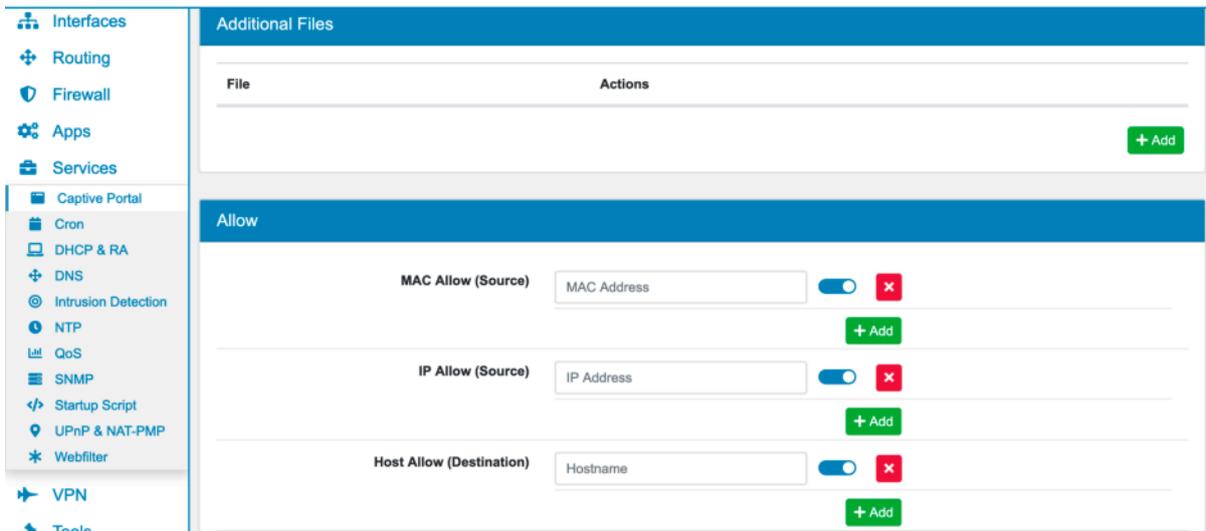
Redirect Address can be setup when *Redirect* mode is chosen. The request will be redirected to a different TBF firewall for processing. This will put the captive portal in forwarding mode and authentication is performed by this server. e.g. <http://vtair.server:port/>.

Use Authentication Server enables the usage of an authentication server for the captive portal.

Authentication Server select one or multiple authentication servers that are defined in [Authentication Server](#). Make sure the login template has a user and password field. The index_auth.html template provides a good example.

Use Voucher Authentication enables the usage of authentication with vouchers.

Main File is the index.html and will be presented to the user when they connect. Only an html file is allowed to upload.



Additional Files can be uploaded like css, js, images or error and success pages.

Mac Allow excludes MACs from the portal authentication.

IP Allow excludes IPs from the portal authentication.

Host Allow excludes Hosts destinations from the portal authentication. This can be used to allow home-pages without authentication.

Note: Captive Portal settings are checked and run before DNAT. The allows and excludes have to be the address before any DNAT change of them.

17.4.2 Captive Portal Files

The main file is the index.html file. It can contain any style and js you like, just make sure it is either inlined or uploaded to additional files.

It is required to have an accept element like this `<input type="submit" name="accept" class="login login-submit" value="Login" id="login">` for the captive portal to check authentication. You can additionally add a redirect input element, if the user should be redirected after the login: `<input name="redirurl" type="hidden" value="https://www.voleatech.de">` It will override the *Redirect URL* option from the GUI.

You can additionally add a error.html for error messages on authentication failures and a success.html when you want a special page after successful authentication. The success page only works when there is no redirect.

In any case the index.html is served if no other page can be found.

You can also download a set of example files on each Captive Portal Instance.

17.4.3 Redirect Device IDs

You can add one or multiple **Device IDs** to a Captive Portal. Other TBF Captive Portal Redirects will be accepted when they come from this deviceid for authentication.



17.4.4 Voucher

You can create vouchers for a Captive Portal. Each voucher has a **Number of Tickets**, which is 100 by default and a **Usage Type** which is *Single Use* or *Multiple Use*. When you have **Use Voucher Authentication** enabled, users can authenticate with the TBF by using a ticket of a voucher. To use the **Voucher Authentication** add an input field to your html page `<input type="password" name="auth_voucher" placeholder="Voucher Code" id="auth_voucher">` the name `auth_voucher` will be checked on submission.

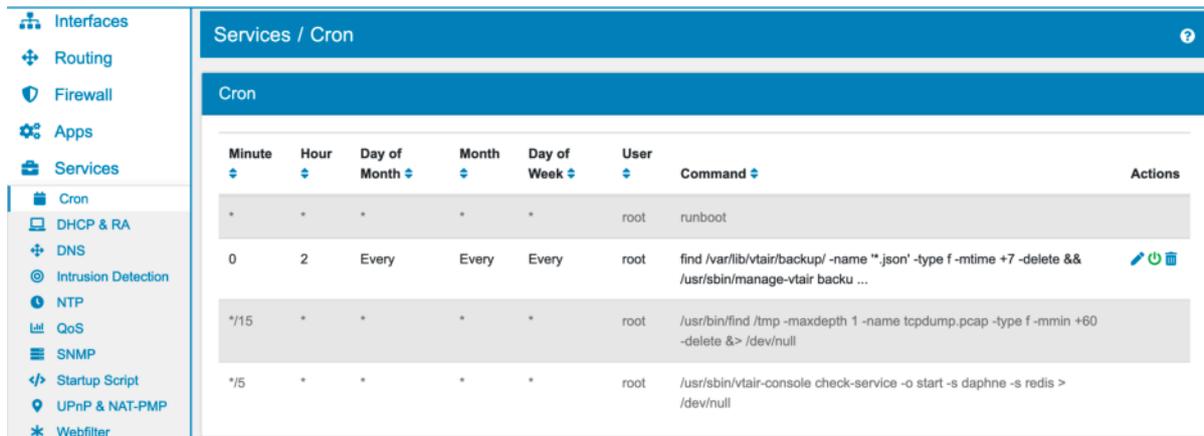
17.4.5 Redirect Mode

If you wish to forward **Captive Portal** requests to a different TBF, you can enable the **Redirect Mode**. It will forward all HTTP requests to the TBF in the **Redirect Address**. It allows you to have a distributed satellite **Captive Portal** where only one TBF instance serves the portal and authenticates users.

The authenticated users are still displayed in the TBF that forwarded the request and also need to be removed on that TBF, if you wish to disconnect users. All authentication features are supported in that setup.

17.5 Cron

You can find the Cron Settings at **Services** → **Cron**.



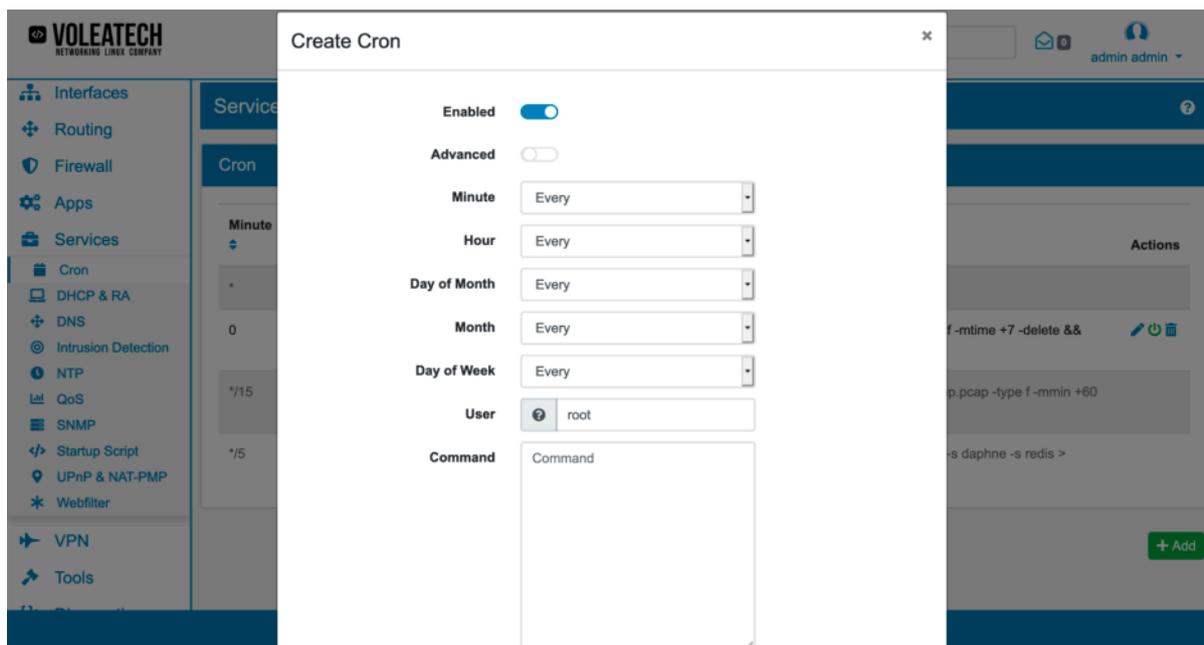
Minute	Hour	Day of Month	Month	Day of Week	User	Command	Actions
*	*	*	*	*	root	runboot	
0	2	Every	Every	Every	root	find /var/lib/vtair/backup/ -name '*.json' -type f -mtime +7 -delete && /usr/sbin/manage-vtair backu ...	 
*/15	*	*	*	*	root	/usr/bin/find /tmp -maxdepth 1 -name tcpdump.pcap -type f -mmin +60 -delete &> /dev/null	
*/5	*	*	*	*	root	/usr/sbin/vtair-console check-service -o start -s daphne -s redis > /dev/null	

Here you can create and manage cron jobs which are commands that run periodically at specific times or intervals. If you open the site the first time, there are already preconfigured cron jobs.

17.5.1 Preconfigured Crons

The **runboot** command is necessary for the system to run the Startup Scripts at boot properly. The **check_service** command checks whether the **Daphne** HTTP WebSocket protocol server and the **Redis** in-memory database are running properly. Those two cron jobs can't be deleted, because they are vital for the system. The last command creates a TBF backup every day at 2 o'clock and copies it into the folder **/var/lib/vtair/backup/**. Each backup has a date in its name and is deleted after 7 days.

17.5.2 Create New



VOLEATECH
NETWORKING LINUX COMPANY

admin admin

Service

Cron

Minute

0

*/15

*/5

Enabled

Advanced

Minute Every

Hour Every

Day of Month Every

Month Every

Day of Week Every

User root

Command

+ Add

If you create a new cron job, you can specify which **user** runs which **command** at which time interval. You can choose between minute, hour, day of the month, month and day of the week. If you enable the **advanced** mode, you can configure special cases with the right syntax.

17.6 DHCP & RA

You can find the DHCP & RA Settings at **Services** → **DHCP & RA**.

The screenshot displays the configuration interface for DHCP & RA, organized into four main sections:

- General:** Contains a sidebar menu on the left with options like Routing, Firewall, Apps, Services, Cron, DHCP & RA, DNS, Intrusion Detection, NTP, and QoS. The main panel shows the 'Services / DHCP & RA / Update' header and tabs for LAN, AppBridge, Sync, Global Options, High Availability, and Relay Server. The 'General' section includes an 'Enabled' toggle (checked), an 'Options' button, and a 'Relay' toggle (unchecked).
- IPv4:** Shows 'Enabled' (checked), 'Subnet' (192.168.1.0), 'Subnet Mask' (255.255.255.0 /24), and 'Available Range' (192.168.1.1 - 192.168.1.254). It features a 'DHCP Pools' table with columns for 'From', 'To', and 'Description', and an 'Options' button.
- IPv6:** Displays a message 'No static IPv6 address for this interface defined'. It includes 'DHCP Pools' and 'Prefix Delegation' sections, each with input fields for 'From', 'To', and 'Prefix', and 'Add' buttons.
- IPv6 Router Advertisement:** Shows a message 'No static IPv6 address for this interface defined' and a 'Subnet Prefix' section with an 'Add' button. Below this is a 'Host Reservation' table with columns for 'Mac Address / DUID', 'IPv4 Address / IPv6 Address', 'Hostname', 'Description', 'Options', and 'Actions', along with 'Add' and 'Add Multiple' buttons.

The **Dynamic Host Configuration Protocol** is used to dynamically assign an IP address and other network configuration parameters to other devices on the network so they can participate in the network communication.

You can export the settings in the top right corner as an Excel spreadsheet.

Each interface has an own tab where DHCP can be enabled individually. IP protocol v4 and v6 need to be enabled and configured separately. An interface needs a static IP address to be configurable. Multiple **DHCP Pools** can be set up, but each one needs to be in the **Available Range** and they cannot intersect each other. The **options** are hierarchically and overwritten by the lower ones. This means that the DHCP Pool options overwrite IP protocol options, the IP protocol options overwrite the interface options and the interface options overwrite the general options.

17.6.1 Network Booting

The functionality of **Network Booting** can be found in the general options of each interface. When enabled, you can configure a **TFTP Server**, **Next Server** and a file name path for **Default BIOS**, **iPXE**, **UEFI 32 bit** and **UEFI 64 bit**.

17.6.2 MAC and DUID Deny

The functionality of **MAC Deny** can be found in the v4 options and the **DUID Deny** can be found in the v6 options of each interface. The MAC and DUID can both be a complete address or a partial address. Clients with their address configured here will be ignored by the DHCP server and will not get a lease.

17.6.3 Extra Options

Additionally to the DHCP options there are a lot of **Extra Options** which can be found in the v4 and v6 options of each interface. There are 254 different options to choose from but duplicates are not allowed. For the predefined options the data type is fixed, whereas for the rest it can be selected individually. All options are forcible set and send with each DHCP packet.

17.6.4 Relay Server

The screenshot displays the Mikrotik WinBox interface for configuring DHCP & RA settings. The left sidebar shows a navigation menu with options like Routing, Firewall, Apps, Services, Cron, DHCP & RA, DNS, Intrusion Detection, NTP, QoS, SNMP, Startup Script, UPnP & NAT-PMP, Webfilter, VPN, and Tools. The main content area is titled 'Services / DHCP & RA / Relay Server' and includes tabs for LAN, AppBridge, Sync, Global Options, High Availability, and Relay Server. The 'Relay Server' tab is active, showing two sections: 'Relay Server v4' and 'Relay Server v6'. Each section contains a table with columns for 'Addresses', 'Description', and 'Actions'. A green '+ Add' button is located at the bottom right of each table.

If a DHCP server already exists in the network you can put it here, so devices will get its information from this DHCP server instead. The DHCP requests will be forwarded to this server. You need to activate the Relay Server on each Interface Tab in the DHCP Settings. You can then choose a **Relay Server v4**.

17.6.5 IPv6 Router Advertisement

With **Router Advertisement** the router advertises its presence in the network for an IPv6 network. A static IPv6 address needs to be set up on the interface to use this functionality. There are four **Modes**: *Router Only*, *SLAAC*, *DHCP* and *Both*. Multiple **Subnet Prefixes** can be added by an IPv6 address. It's also possible to configure several options which are similar to the DHCP ones.

Router Only

Is advertising the presence of TBF as a router for the network interface. The static Interface IPv6 is used for this.

SLAAC

A router is advertised and a prefix as well so the client can configure his IPv6 address automatically.

DHCP

A router is advertised and also the option that the client should contact a DHCP Server for an IPv6 address.

Both

A router is advertised and also SLAAC as well as DHCP.

17.6.6 IPv6 Prefix Delegation

IPv6 **Prefix Delegation** is used to assign a network address prefix and automate configuration and provisioning of public routable addresses for a network. A static IPv6 address needs to be set up on the interface to use this functionality. Multiple **Prefix Delegations** can be added by an IPv6 address as **Prefix**, a **Prefix Length** and a **Prefix Delegation Length**. The Prefix Delegation Length must be greater or equal to the Prefix Length. The Prefix **can't** intersect with an already used IPv6 Pool.

17.6.7 Host Reservation

The screenshot displays the Voleatech Network Linux Company management interface. The left sidebar contains a navigation menu with categories like Routing, Firewall, Apps, Services, Cron, DHCP & RA, DNS, Intrusion Detection, NTP, QoS, SNMP, Startup Script, UPnP & NAT-PMP, Webfilter, VPN, Tools, and Diagnostics. The main content area is divided into two panels.

The top panel, titled "Global DHCP Options", contains the following configuration fields:

- Gateway: Gateway
- Domain Name: Domain Name
- Default Lease Time: Default Lease Time
- Maximum Lease Time: Maximum Lease Time
- DNS Server 1: DNS Server 1
- DNS Server 2: DNS Server 2
- DNS Server 3: DNS Server 3
- DNS Server 4: DNS Server 4
- NTP Server 1: NTP Server 1
- NTP Server 2: NTP Server 2
- TFTP Server: TFTP Server
- Decline Probation Period: 60
- Domain Search List: Domain (with a toggle switch and a red 'x' icon)

The bottom panel, titled "High Availability", shows the following configuration:

- Enabled:
- IP Type: IPv4
- Role: Master
- Syncinterface: WAN
- Max Unacked: 3
- Master Server: 192.168.10.113
- Slave Server: Slave Server
- Backup Server: Backup Server
- Associate Firewall Rule:

Multiple **Host Reservation** can be created with a **MAC Address**, **Hostname** and **IP Address**. For IPv4 you can specify a **Client Identifier** and for IPv6 you can specify a **DUID** (DHCP Unique Identifier).

The **Client Identifier** can be used if there is no **MAC Address** for IPv4. The options are mutually exclusive. The **DUID** is also preferred over the **MAC Address** for IPv6 reservations.

The advanced options are identical to the previous DHCP options.

Each Host Reservation creates a Network Object that can be used in the *Firewall Rules*. If you delete the Host Reservation, you will need to remove it from the *Firewall Rules* first. A list of all active *Firewall Rules* that include the Host Reservation will be shown on the delete action as a warning.

17.7 DNS

You can find the DNS Settings at **Services** → **DNS**.

The **Domain Name System** is mainly used to translate more readable domain names to their numerical IP addresses.

17.7.1 General Settings

The screenshot displays the 'General' settings for the DNS service. The left sidebar shows the navigation menu with 'DNS' selected. The main content area includes the following settings:

- Enabled:** A toggle switch that is currently turned on.
- SSL/TLS Enabled:** A toggle switch that is currently turned on.
- SSL/TLS Certificate:** A dropdown menu showing 'VT AIR Certificate'.
- SSL/TLS Port:** A text input field containing '853'.
- Port:** A text input field containing '53'.
- Interfaces In:** A list box containing 'All', 'LAN', 'WIREGUARD_afsdfdsaf', and 'OVPN_asdfadfs'.
- Interfaces Out:** A list box containing 'All', 'LAN', 'WIREGUARD_afsdfdsaf', and 'OVPN_asdfadfs'.
- Local Zone Type:** A dropdown menu showing 'Transparent'.
- DNSSEC:** A toggle switch that is currently turned on.
- PTR Records:** A toggle switch that is currently turned on.

Below the general settings, there are sections for 'Host Overrides' and 'Domain Overrides', each with a table for configuration and an '+ Add' button. The 'Host Overrides' table has columns for 'Host / Domain', 'IP Address', 'Description', and 'Actions'. The 'Domain Overrides' table has columns for 'Domain', 'IP Address', 'Description', and 'Actions'.

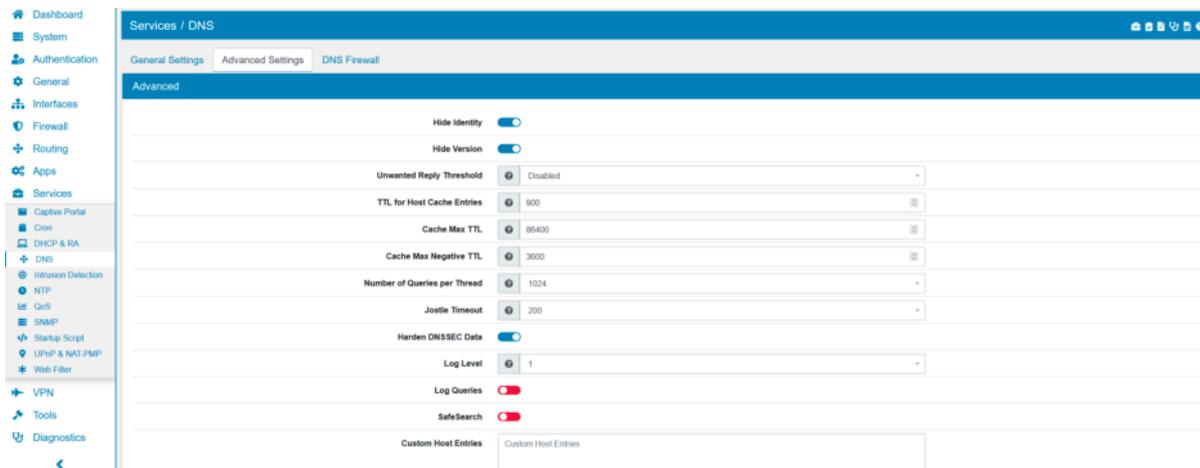
On the page the DNS server can be enabled or disabled. **SSL/TLS** is enabled by default and the TBF Certificate with port 853 is used. You can change **Interfaces In** and **Interfaces Out** and on which **Port** DNS runs on. The **Local Zone Type** can be configured and is on Transparent by default. The option **DNSSEC** controls the Domain Name System Security Extensions and if **PTR Records** is enabled, PTR Records for Host Overrides get added automatically. **DHCP Registration** will register the DHCP leases in the DNS server, while **Static DHCP Registration** will register the DHCP Host Reservations in the DNS server.

By default the DNS Server queries the DNS Root servers and is not forwarding traffic to other servers. If **DNS Forward** is enabled, you can add multiple **DNS Forward Servers** with an IP address for each

and those are used instead of the Root Servers.

You can export the settings in the top right corner as an Excel spreadsheet.

17.7.2 Advanced Settings



Hide Identity if enabled `id.server` and `hostname.bind` queries are refused.

Hide Version if enabled `version.server` and `version.bind` queries are refused.

Unwanted Reply Threshold if set, a total number of unwanted replies is kept track of in every thread. When it reaches the threshold, a defensive action is taken and a warning is printed to the log.

TTL for Host Cache Entries time to live for entries in the host cache. The host cache contains roundtrip timing, lameness and EDNS support information. It is 900 by default.

Cache Max TTL time to live maximum for RRsets and messages in the cache. When the TTL expires, the cache item has expired. It is 86400 by default.

Cache Max Negative TTL time to live maximum for negative responses, these have a SOA in the authority section that is limited in time. It is 3600 by default.

Number of Queries per Thread the number of queries that every thread will service simultaneously. It is 1024 by default.

Jostle Timeout timeout used when the server is very busy. Set to a value that usually results in one roundtrip to the authority servers. It is 200 by default.

Harden DNSSEC Data require DNSSEC data for trust-anchored zones, if such data is absent, the zone becomes bogus.

Log Level the Log verbosity level. It is 1 by default.

SafeSearch enables the SafeSearch functionality. It is disabled by default.

Log Queries logs all queries.

Custom Host Entries for custom host or domain entries. They will be copied to the configuration directly.

Custom Options custom configuration parameters can be defined here.

Please refer to the Unbound documentation at [Unbound](#).

17.7.3 Host Overrides

They allow the configuration of a specific DNS entry for a particular host.

17.7.4 Domain Overrides

They allow the configuration of a specific DNS server for a particular domain. If you define a domain multiple times, all DNS server will be used together.

17.7.5 DNS Firewall

Name	Details	Actions
ads	•	○
adult	•	○
aggressive	•	○
agnostic	•	○
app	•	○
assocations_religions	•	○
astrology	•	○

Since most web traffic is encrypted the most effective way to block access to websites is DNS blocklisting. It will send a *fake* IP back to your client for a domain.

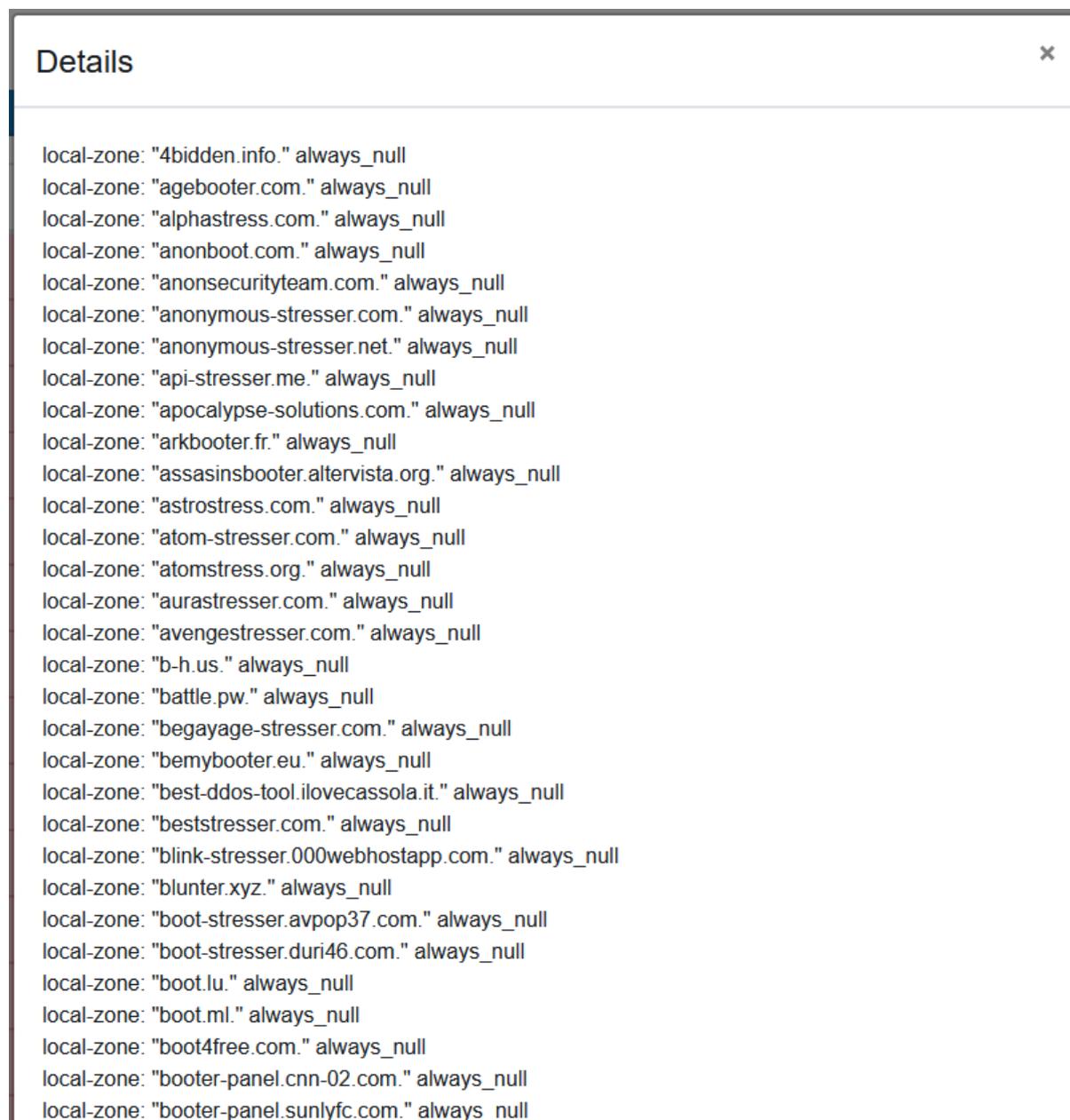
TBF uses list of domains in a few categories for you to choose or you can add your own domains and hostnames.

Update Interval is set to weekly by default and can be changed to daily or monthly.

Categories

Blocklist Categories allow you to block hosts by different categories.

By default, the categories *cryptojacking*, *ddos* and *malware* are enabled. You can enable or disable each category individually.



Each categorie has a button which opens a modal with detailed information. All hosts and IPs of that blocklist are listed here.

Custom Blocklists

Multiple Custom Blocklist entries can be added with a hostname or domains. Each one can be enabled or disabled, independently from the categories.

All subdomains of the entered domain or hostname will be included in the blocklist.

17.7.6 Redirect DNS Requests

You can redirect all DNS requests to your TBF device and block other DNS servers (especially outside of your network). To do so go to **Firewall** → **NAT** → **DNAT** and click **Add**.

Select the **Interface** of your local network e.g. *LAN*, *TCP/UDP* as **Protocol** and the **Address Family** you want your rule to be active on.

Enable **Invert IP Match** and select *LAN_Address* and **Port DNS (53)** as the Destination. This selects all DNS requests that are not targeted at the local DNS server.

Select *Localhost* and *DNS (53)* as the **Redirect IP** and **Port**. This redirects all DNS requests to your TBF device. Enable **Associate Firewall Rule** and set **NAT Reflection** to *Disabled*.

If you block outside DNS requests you can also effectively use the Blocklist feature described above without configuring each device individually in your network.

17.7.7 Wildcard Domain DNS Entries

If you need to create a wildcard DNS entry like `*.subdomain.domain.com` you can do so in the **Custom Host Entries** field. The structure is the following, replace the IP with the host that should be returned for all subdomain queries:

Note: local-zone: "subdomain.domain.com." redirect local-data: "subdomain.domain.com. A 192.168.1.10"

17.7.8 DNS Troubleshooting

Note: If you use a forward server that returns private IPs, they will be rejected since the DNS server will see them as a DNS rebind attack. In order to deactivate the check for domains, declare them as private in the *Custom Host Entries* field with **private-domain: "mydomain.ending"**.

Note: If you use an internet load balancer, more than one WAN at the same time, you need to provide an upstream DNS server and change the mode to forwarding. Otherwise the DNS request might not be answered correctly and you will see hangs in the DNS requests.

17.8 HAProxy

You can find the HAProxy Settings at **Services** → **HAProxy**.

The **HAProxy** is a high availability load balancer and proxy server for TCP and HTTP.

Before you can use the HAProxy it has to be installed. You can install it at **System** → **Addons**.

17.8.1 General Settings

The screenshot displays the HAProxy configuration page in a web interface. The page is titled "Services / HAProxy" and has a navigation menu with tabs for "Settings", "Backend", "Frontend", "Error Page", and "Diagnostics". The "General Settings" section is active and shows the following configuration:

- Enabled:** A toggle switch is turned on.
- Maximum Connections:** A dropdown menu is set to 1009.
- Hard Stop After:** A dropdown menu is set to 15 Minutes.
- SSL Ciphers:** A text area containing the list of supported ciphers: ECDHE-RSA-CHACHA20-POLY1305 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-CCM DHE-RSA-AES256-CCM8 DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES128-CCM DHE-RSA-AES128-CCM8 DHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256.
- SSL Options:** A list of checkboxes for "no-sslv3", "no-tlsv10", "no-tlsv11", and "no-tls-tickets", all of which are currently unchecked.
- Let's Encrypt ACL:** A toggle switch is turned on.
- Custom Options:** A text input field labeled "Custom Options" is empty.

On the page the HAProxy can be enabled or disabled.

The **Maximum Connections** can be configured and is 1000 by default.

Hard Stop After defines the maximum time allowed to perform a clean soft-stop. This may be used to ensure that the instance will quit even if connections remain opened during a soft-stop.

SSL Ciphers is a list of ssl ciphers separated by colons.

SSL Options can be a selection of *no-sslv3*, *no-tlsv10*, *no-tlsv11*, *no-tls-tickets*, *no-tlsv12* and *no-tlsv13*.

Let's Encrypt ACL will redirect all letsencrypt requests to the TBF firewall for renewal of certificates. Use this option if TBF itself is renewing the certificates in the web mode.

Custom Options can be used for custom configuration parameters for the config.

HAProxy will automatically be started with one thread per CPU core to load balance connections.

You can export the settings in the top right corner as an Excel spreadsheet.

17.8.2 Backend

A backend is a server behind the firewall that HAProxy should send data to. Data are received on the *Frontend*, are processed and forwarded to a backend.

The screenshot displays the HAProxy configuration interface. The left sidebar shows the navigation menu with 'HAProxy' selected. The main content area is divided into two sections: 'Backend' and 'Advanced Settings'.

Backend Configuration:

- Enabled:** A toggle switch is turned on.
- Name:** A text input field labeled 'Name'.
- Description:** A text input field labeled 'Description'.
- Load Balancing:** A dropdown menu currently set to 'None'.

Server List:

Server	Name	Mode	IP Address	SSL Encrypt	SSL Checks	Enabled
	<input type="text" value="Name"/>	<input type="text" value="active"/>	<input type="text" value="IP Address"/>	<input type="text" value="80"/>	<input type="checkbox"/>	<input type="checkbox"/>

A green '+ Add' button is located at the bottom right of the Server List table.

Advanced Settings:

- Connection Timeout:** 30000
- Server Timeout:** 30000
- Maximum Backend Connections:** Maximum Backend Connections
- Retries:** 3
- Send Proxy:** No
- Source Address:** Any
- Custom Options:** Custom Options

The screenshot displays the HAProxy configuration interface. On the left is a sidebar menu with categories: Firewall, Apps, Services, Cron, DHCP & RA, DNS, HAProxy, Intrusion Detection, NTP, QoS, SNMP, Startup Script, UPnP & NAT-PMP, Webfilter, VPN, and Tools. The main content area is divided into two sections: 'Health checking' and 'Stick Table'. The 'Health checking' section contains several fields: 'Health check method' (HTTP), 'Check frequency' (1000), 'Log checks' (disabled), 'Health check method' (OPTIONS), 'Uri used by http check requests' (/), and 'Http check version' (Http check version). The 'Stick Table' section has an 'Enabled' toggle switch.

Each **Backend** has a **Name**, **Description** and can be enabled or disabled. You can add multiple **Servers**, each with a name, mode, IP address, port and ssl encrypt and ssl checks to each backend in case you want to load balance them.

SSL Encrypt enables SSL deciphering on connections instantiated from this listener.

SSL Checks forces encryption of all health checks over SSL, regardless of whether the server uses SSL or not for the normal traffic.

Load Balancing can be *Round Robin*, *Static Round Robin*, *Least Connections* or *Source*.

Connection Timeout is the maximum time (in milliseconds) to wait for a connection attempt to a server to succeed. The default value is 30000.

Server Timeout is the maximum inactivity time (in milliseconds) on the server side. The default value is 30000.

Maximum Backend Connections is the maximum amount of connections that all backends should process. If no value is specified the value is computed by the global Maximum Connection value.

Retries are the number of times a connection attempt should be retried on a server when a connection either is refused or times out. The default value is 3.

Send Proxy if the proxy protocol should be used to connect to the backend and if so which version.

Source Address in order to change the source of the connection from HAProxy to the firewall. This might be useful in HA Setups to use the virtual ip as sender.

WAF Error Page File is a Custom Error Page if WAF is activated and access is blocked for this backend. Has to be a HTML file.

Custom Options can be used for custom configuration parameters for the config.

Health check method can be *None*, *Basic*, *HTTP*, *SMTP* or *LDAP*.

Check frequency is the check frequency in milliseconds. The default value is 1000.

When **Log checks** is enabled, any change of the health check status or to the server's health will be logged.

Health check method can be *OPTIONS*, *HEAD*, *GET*, *POST*, *PUT*, *DELETE* or *TRACE*.

Uri used by http check requests defaults to / if left blank.

Http check version defaults to "HTTP/1.0" if left blank.

Stick Table can be enabled.

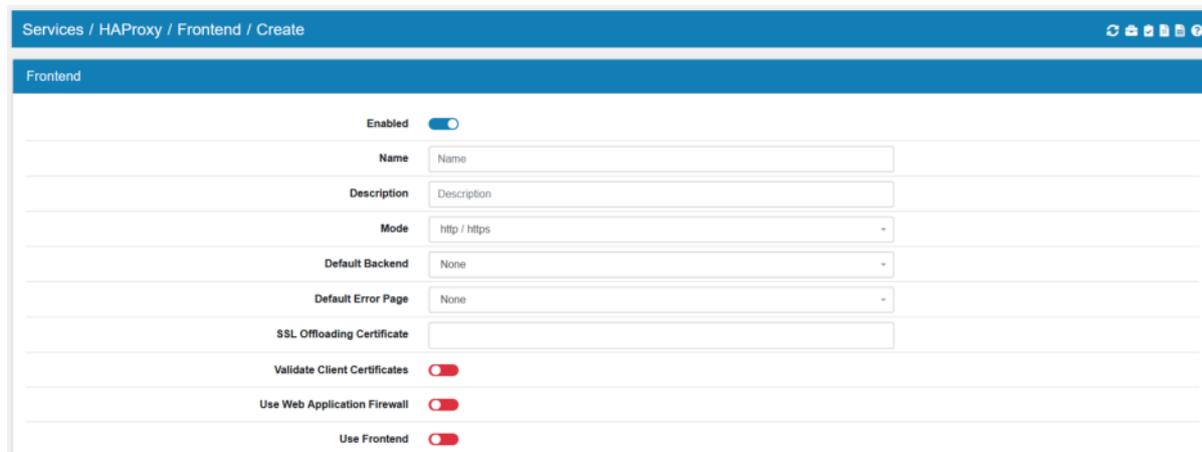
Type is the stick table type.

Size is the stick table size in MB. The default value is 1 MB.

Expire is the stick table expire time in seconds. The default value is 10 seconds.

17.8.3 Frontend

Frontend is the service where HAProxy is listening for connections to process. A frontend is listening on an IP Address and port pair.



Each **Frontend** has a **Name**, **Description** and can be enabled or disabled.

A **Frontend** can either be standalone or connected to another frontend. In the case of a connected frontend, only the acl and actions will be available and all other settings are merged from the connected frontend.

A frontend can have multiple addresses with an IP address and port. You can also add multiple ACLs with a description, expression, backend and value. The value can be negated and checked for case-sensitivity.

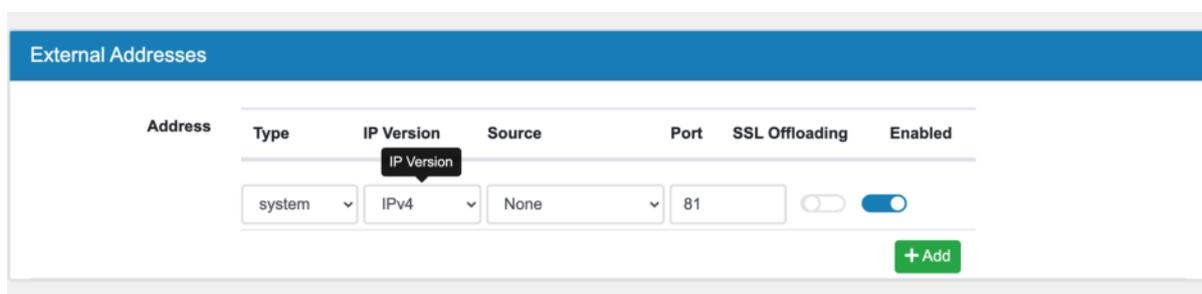
Mode can be *http / https*, *ssl / https (TCP mode)* or *tcp*.

Default Backend is the default connection to a backend when no specific one is chosen in a following option.

Default Error Page is the default error page. It has to be created in the system beforehand.

SSL Offloading Certificate allows you to SSL Offload connections. HAProxy can have more than one certificate and they are chosen based on CName and the request that is coming in. To enable SSL Offloading the IP address and port have to be explicitly set to enabled even when certificates are selected here. Only HTTP connections can be offloaded and not TCP or TLS connections.

Validate Client Certificates can be enabled. If enabled, you also need to choose a **Certificate Authority**. This is only possible on *http / https* and *tcp* mode with SSL Offloading enabled for external addresses. **Client Certificate Verification** will also be configurable and can be either *Required* or *Optional*.



Each *Frontend* can listen on one or more IP addresses and ports. You need to set the type (IPv4 or IPv6) and which address to use. *System* addresses are Network Objects from the Firewall. You can enable *SSL Offloading* for each Pair.

In order to use the **Web Application Firewall** on encrypted connections you can enable the *SSL Offloading* to transparently encrypt traffic to the user but still give access to the WAF.

Use Web Application Firewall enables the web application firewall for this frontend. The traffic will be inspected by the WAF and if a threat is detected it will be blocked with a 404 error.

Use Frontend lets you select and use another **HAProxy Frontend**. In order to make managing different Frontends easier, you can connect one Frontend to another Frontend. All settings except ACLs and Actions are shared between the Frontends. The Frontends are merged together in the configuration to display one unified Frontend. Different use cases make it more user friendly to separate the Frontends in the GUI like multiple complex Backends or separating by Customer.

Advanced

Advanced allows to set some settings for the entire frontend.

Maximum Connections limit the sockets to this number of concurrent connections.

Client Timeout is the maximum inactivity time (in milliseconds) on the client side. The default value is 30000.

Forwardfor Option enables the insertion of the X-Forwarded-For header to requests sent to servers.

HTTP/s Redirect can be enabled.

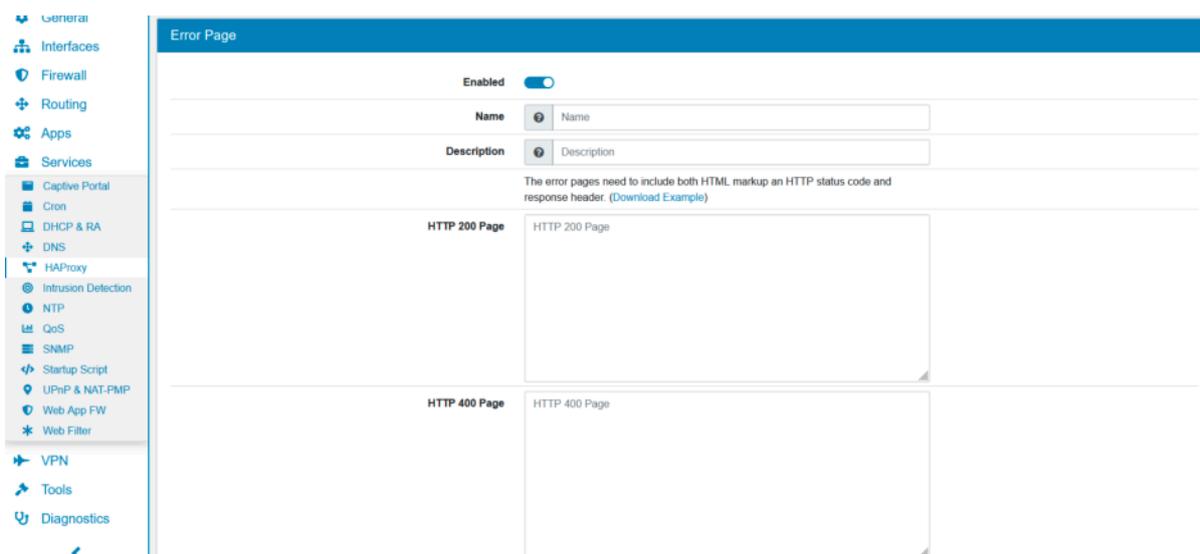
Httpclose Option enables passive HTTP connection closing.

Backend Separation If we have an ACL with host matches, use a copy of the backend for each action and run the backend health check with this host name. This allows only this host to be not available in case of problems especially when a backend is hosting multiple homepages under different hostnames.

Custom Options can be used for custom configuration parameters for the config.

17.8.4 Error Pages

Error Pages with custom error pages can be configured and linked to actions and acls. The following HTTP codes are supported: 200, 400, 401, 403, 404, 405, 407, 408, 410, 425, 429, 500, 502, 503 and 504. An example file can be downloaded from the GUI. The error pages need to include both HTML markup an HTTP status code and response header.



17.8.5 Access Control Lists

Access Control Lists are rules to match against which can be used in Frontends and Backends. In the Frontend they depend on the mode and include host names and source ips. Each ACL needs a unique name for the frontend so it can be used in the actions assignment.

Access Control Lists							
Expression	CS	Negation	Value	Name	Description	Enabled	
Source IP matches IP or Network Object		<input checked="" type="checkbox"/>	192.168.10.112	ac1	Description	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Host matches	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	haproxy.1wt.de	ac2	Description	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Host starts with	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	exchange	ac3	Description	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
None	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Value	Name	Description	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[+ Add](#)

17.8.6 Actions

Actions can be linked to one or many **ACLs**. Multiple ACLs can be AND/OR together to get a flexible assignment. Frontend and Backend Actions have different specific actions to choose from.

A **Error Page** can be assigned to a Frontend Action or set as Default Error Page in a Frontend. They have to be created in the system beforehand.

A **Error Page Backend Down** can be assigned to a Frontend Action. It will be used, if the selected backend is down.

Order	Action	Operator	ACLs	Description	Enabled
1	http-request allow	AND	acl1 x ACLs	Description	<input checked="" type="checkbox"/>
2	http-request deny	AND	acl2 x ACLs	Description	<input checked="" type="checkbox"/>
3	Use Backend	AND	acl1 x acl2 x acl3 x ACLs	Description	<input checked="" type="checkbox"/>
	main-backend				
-	None	AND	ACLs	Description	<input checked="" type="checkbox"/>

[+ Add](#)

17.8.7 General

Please be aware that port 443 and port 80 are occupied by Nginx. If you want to use them for HAProxy, please use DNAT on the interfaces to a different Port that the Frontend of HAProxy is using.

You can simply redirect the port 443 and 80 from WAN to HAProxy. HAProxy needs to run on a different port, for example 444 and 81.

An example for the DNAT rule can be found in the following image.

Enabled	<input checked="" type="checkbox"/>
Interface	WAN_Telekom
NAT Type	Inbound (DNAT)
Address Family	IPv4+IPv6
Protocol	TCP
Description	HAProxy
▼	
▲	
Invert IP Match	<input type="checkbox"/>
Original Destination IPs	WAN_Telekom_Address / 128
+ Add	
Destination Ports	HTTPS (443)
+ Add	
▼	
Redirect IP	WAN_Telekom_Address / 128
Redirect Port(s)	Port 444

17.9 IGMPProxy

You can find the IGMPProxy Settings at **Services** → **IGMPProxy**.

The **IGMPProxy** is used to propagate multicasts across L2s.

Before you can use the IGMPProxy it has to be installed. You can install it at **System** → **Addons**.

17.9.1 Upstream

On the page the IGMPProxy can be enabled or disabled.

Interface sets the interface. This interface can not be used as Downstream interface.

Threshold for the TTL of the multicast to avoid looping. Default value is 1.

You can add multiple **Networks**, each with an IP Address and Netmask.

17.9.2 Downstream

You can add multiple **Downstreams**, each with an Interface and Threshold.

After saving a *Downstream Interface* you can optionally set Networks to specify who is allowed to communicate via the IGMP proxy.

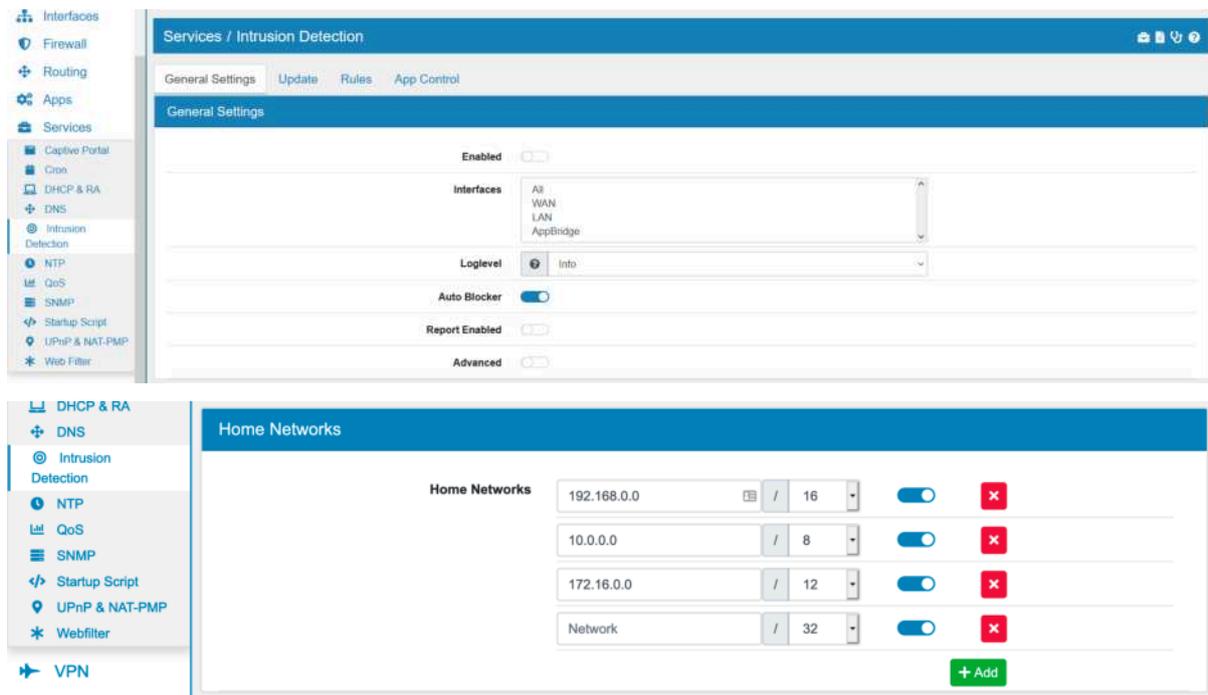
It's not possible to use the Upstream interface as Downstream interface.

17.10 Intrusion Detection

You can find the Intrusion Detection Settings at **Services** → **Intrusion Detection**.

The Intrusion Detection is using **Suricata**, an open source-based intrusion detection system (IDS) and intrusion prevention system (IPS).

17.10.1 General Settings



On this page Suricata can be enabled or disabled.

The **Mode** can be *IDS* (Intrusion Detection System), *IPS* (Intrusion Prevention System) or *IDS & IPS*.

One or more **Interfaces** can be selected where traffic should be analyzed by Suricata.

Disable for Internal Traffic will disable Intrusion Detection for private network IPs. This will make it faster for internal traffic while securing internet facing traffic.

Loglevel for Suricata can be setup and is *Info* by default.

Auto Blocker will block IP Adresses that were matched by a security event rule.

Note: Only IPs that are not in the *Home Networks* and from one of the following categories will be blocked for 60 seconds: - Attempted Denial of Service - Denial of Service - A Network Trojan was detected - Detection of a Denial of Service Attack - Web Application Attack - Exploit Kit Activity Detected - Successful Credential Theft Detected - Crypto Currency Mining Activity Detected - Malware Command and Control Activity Detected

Report Enabled can be enabled or disabled. If it is enabled you can define a **Report Email** that should receive reports. Make sure to configure an Email server in the settings. The report will contain information about alerts and blocked events in the given period.

The option **Advanced** allows the usage of **Pass Last** and **Custom Options**.

Pass Last will change the order of rule execution. Usually Pass rules are evaluated before drop rules.

IPS Check Firewall will also monitor all traffic coming and going from the TBF itself. Be aware that this might block traffic to the GUI or services on the Firewall. The default is off, it is better to use good Firewall Rules to protect the TBF itself.

IPS on Bridge will also monitor all traffic passing through all configured Bridges on the Layer 2 level. This will only affect traffic, that is not filtered by the firewall in a VLAN or another type of interface that is on top of the Bridge.

Multiple **Home Networks** can be added with their ip address and port. By default the networks 192.168.0.0/16, 10.0.0.0/8 and 172.16.0.0/12 are created. **Home Networks** are often used in the default

rules to identify internal and external traffic and to apply different rules. You can export the settings in the top right corner as an Excel spreadsheet.

17.10.2 Performance Settings

Intrusion Detection performance heavily depends on memory settings.

Setting	Value
Max Pending Packets	1024
Default Packet Size	1514
Encryption Bypass	<input checked="" type="checkbox"/>
Defragmented Packet Memory (MB)	168
Flow Packet Memory (MB)	2464
Flow Hash Size	65536
Flow Prealloc	10000
TCP Stream Memory (MB)	1648
TCP Stream Prealloc	10656
TCP Stream Reassembly Memory (MB)	3280
TCP Stream Reassembly Segment Prealloc	10656
TCP Stream Bypass	<input checked="" type="checkbox"/>

[Reset Performance Settings](#)

Max Pending Packets This can range from one packet to tens of thousands/hundreds of thousands of packets. It is a trade of higher performance and the use of more memory (RAM), or lower performance and less use of memory. A high number of packets being processed results in a higher performance and the use of more memory. A low number of packets, results in lower performance and less use of memory.

Default Packet Size With the default-packet-size option, you can set the size of the packets on your network. It is possible that bigger packets have to be processed sometimes. The engine can still process these bigger packets, but processing it will lower the performance.

Encryption Bypass Encrypted traffic has very little information for IPS. With this option it will be off-loaded after initial inspection which leads to a huge speedup and frees resources to process more packets.

Defragmented Packet Memory (MB) Maximum memory to use to reassembly defragment packets.

Flow Packet Memory (MB) Maximum amount of bytes the flow-engine will use. More memory will result in faster processing.

Flow Hash Size Higher Hash size gives better performance but needs more memory.

Flow Prealloc To mitigate the engine from being overloaded, this option instructs Suricata to keep a number of flows ready in memory.

TCP Stream Memory (MB) Maximum amount of bytes the tcp stream engine will use. More memory will result in faster processing.

TCP Stream Prealloc Sessions prealloc per stream thread

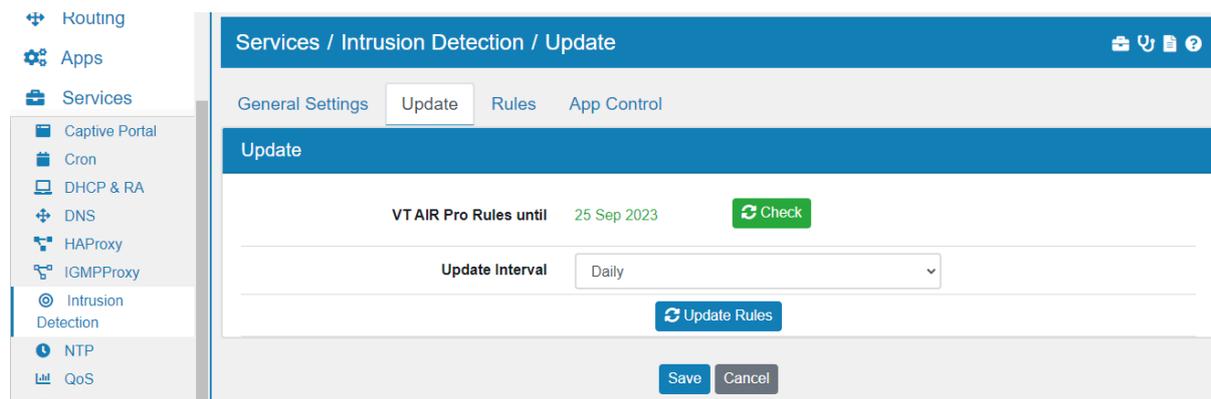
TCP Stream Reassembly Memory (MB) Maximum amount of bytes the tcp stream reassembly engine will use. More memory will result in faster processing.

TCP Stream Reassembly Segment Prealloc Reassembly Segment prealloc per stream thread

TCP Stream Bypass The bypass option activates 'bypass' for a flow/session when either side of the session reaches its depth. Bypass can lead to missing important traffic. It is still enabled by default as it leads to speedups.

Reset Performance Settings will calculate a general value based on available memory resources for each option. You can tweak the values if your setup requires different settings.

17.10.3 Update



Here you can configure see the rules that are used. If you purchased * TBF Pro Rules** your device will pull the licence from the TBF Portal* and you can see the licence and expiration date here. If not the **ETOpen Emerging Threats rules** will automatically be activated instead.

The TBF Pro Rules* already include the *ETOpen Rules*.

Update Interval is a cronjob which will update the rules according to the selected time interval.

Be aware that the more rules you select the slower Suricata gets. It might be advisable to only use rules and categories that you need.

17.10.4 Rules



Here you can see all installed and used rule files which usually correspond to a single category. You can click on the detail icon of each rule to see the specific definition of it. Each rule file can be *disabled*, set to *alert* or *drop* on the actions column on the right side. Below the list there are also three buttons to change all rules at once: *Drop All*, *Alert All* and *Disable All*.

Multiple **SIDs** can be added to disable specific rules by their Signature ID.

At the bottom you can add **Custom Rules**.

17.10.5 Example Suricata Configuration

In your TBF's software you get to choose between two rule packages that you can enable. Each set of rules is divided into different categories. Based on these categories you can specify in greater detail what kind of traffic you want to be blocked. Not all of these might be desirable under all circumstances.

By default Suricata creates its own set of rules. These can be found [here](#).

When enabling the Emerging Threats Open Rules they will be shown to you as emerging-XXX under **Services** → **Suricata** → **Rules**. A detailed description of the different categories can be found in the [official documentation](#).

Rule Name	File Path	Status
emerging-imap	/var/lib/suricata/rules/emerging-imap.rules	⏻
emerging-inappropriate	/var/lib/suricata/rules/emerging-inappropriate.rules	⏻
emerging-info	/var/lib/suricata/rules/emerging-info.rules	⏻
emerging-malware	/var/lib/suricata/rules/emerging-malware.rules	⏻
emerging-misc	/var/lib/suricata/rules/emerging-misc.rules	⏻
emerging-mobile_malware	/var/lib/suricata/rules/emerging-mobile_malware.rules	⏻
emerging-netbios	/var/lib/suricata/rules/emerging-netbios.rules	⏻
emerging-p2p	/var/lib/suricata/rules/emerging-p2p.rules	⏻
emerging-policy	/var/lib/suricata/rules/emerging-policy.rules	⏻
emerging-pop3	/var/lib/suricata/rules/emerging-pop3.rules	⏻
emerging-rpc	/var/lib/suricata/rules/emerging-rpc.rules	⏻
emerging-scada	/var/lib/suricata/rules/emerging-scada.rules	⏻
emerging-scan	/var/lib/suricata/rules/emerging-scan.rules	⏻

© Voleatech GmbH 2017 - 2020

We recommend to set the **Interfaces** to any and create a firewall rule to only filter relevant traffic. As a recommendation you should create a *Global Firewall Rules (Forward and Input)* with *Input Interface Any*, *Output Interface Any*, the *Action Match*, *Source Private Networks*, *Destination Private Networks* and under *Advanced Settings* set the option **Bypass IDS/App Control**. The rule should be the first user created rule under the Global Rules.

17.11 Netflow

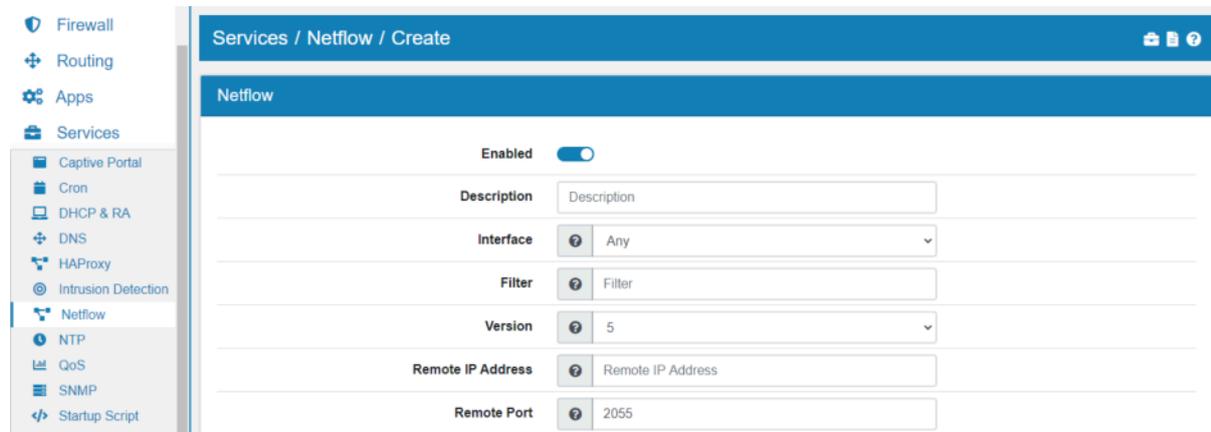
You can find the Netflow Settings at **Services** → **Netflow**.

Netflow is used for collecting network traffic data and emitting it as NetFlow flow towards a specified collector.

Before you can use the Netflow it has to be installed. You can install it at **System** → **Addons**.

17.11.1 Settings

You can create multiple netflow instances, each will send the data to a collector.



On the page the Netflow can be created, updated, enabled or disabled.

Interface to listen to traffic to.

Filter is a TCPDump style filter expression selects which packets will be captured. If no expression is given, all packets on the interface will be captured.

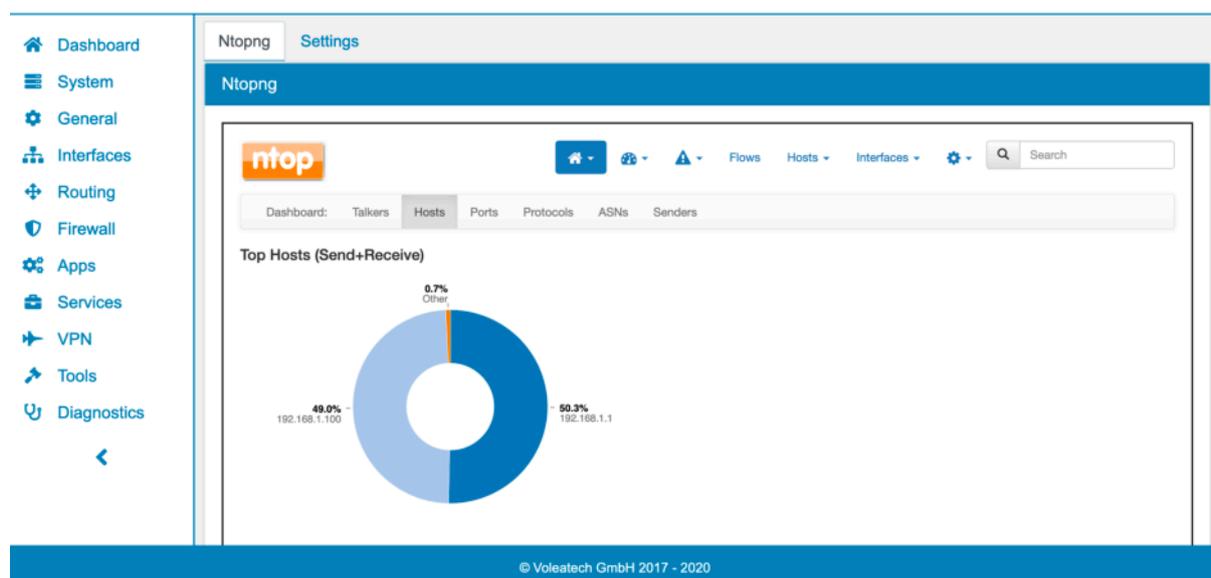
Version is the Netflow Version and 5 by default.

Remote IP Address defines the Remote Netflow collector IP Address.

Remote Port is the Remote Netflow collector Port and 2055 by default.

17.12 Ntopng

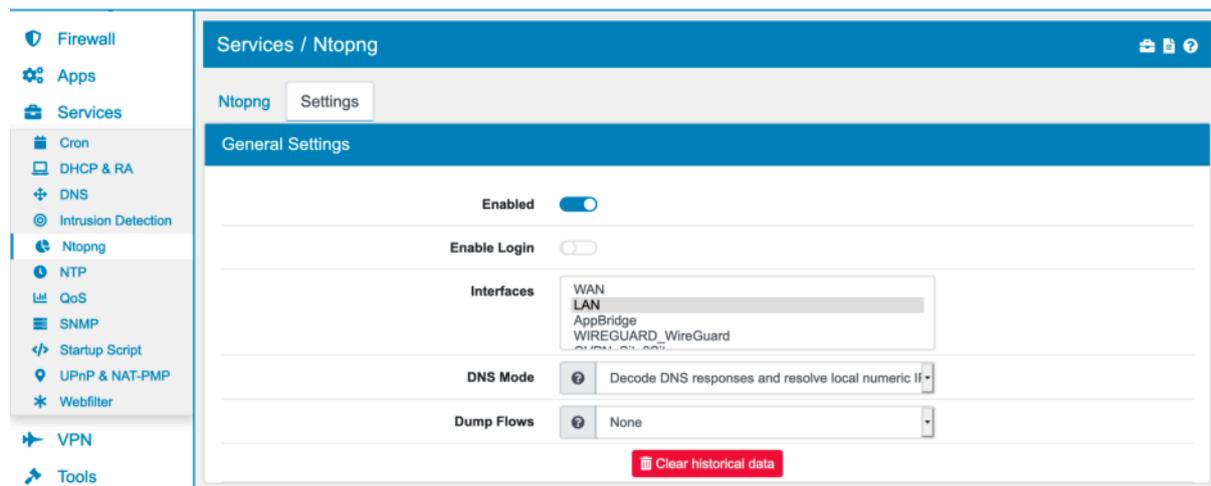
You can find the Ntopng Settings at **Services** → **Ntopng**.



Ntopng is a network traffic probe that monitors network usage.

Before you can use the Ntopng it has to be installed. You can install it at **System** → **Addons**.

17.12.1 Settings



On the page the Ntopng can be enabled or disabled.

Enable Login enables *Username* and *Password*.

Username is *admin* and cannot be changed.

Password for the ntopng GUI.

Interfaces can be specified and determine where the network traffic is collected. Data are only collected in Ntopng for enabled interfaces.

DNS Mode is the DNS address resolution mode and can be one of the following:

- Decode DNS responses and resolve local numeric IPs only
- Decode DNS responses and resolve all numeric IPs
- Decode DNS responses and don't resolve numeric IPs
- Don't decode DNS responses and don't resolve numeric IPs

Clear historical data will remove all recorded data so far.

Dump Flows save flows to a backend system. The available options are MySQL, ElasticSearch, Logstash

17.13 NTP

You can find the NTP Settings at **Services** → **NTP**.

The screenshot shows the NTP configuration page. The left sidebar lists various services, with 'NTP' selected. The main configuration area is titled 'General' and includes the following settings:

- Interfaces:** A dropdown menu set to 'All', with options for WAN, LAN, and Sync.
- Time Servers:** A list of three servers:
 - 0.pool.ntp.org: Prefer (off), No Select (off), and a red 'X' icon.
 - 1.pool.ntp.org: Prefer (off), No Select (off), and a red 'X' icon.
 - Server Address: Prefer (off), No Select (off), and a red 'X' icon.
 A green '+ Add' button is located below this list.
- Orphan Mode:** A dropdown menu set to '12'.
- Logging Peer Messages:** A toggle switch that is currently off.
- Logging System Messages:** A toggle switch that is currently off.

The **Network Time Protocol** lets you synchronize the system time over the network.

You can **enable** or disable it completely and define whether it uses all **interfaces** or a subset. The **orphan mode** is 12 by default and allows a group of ntpd processes to autonomously select a leader in the event so that all real time sources become unreachable. With **Logging Peer Messages** you can enable additional peer log information and with **Logging System Messages** additional system log information.

A variable number of time servers can be added, each with a **server address**. If you select **prefer**, this time server will be chosen before other servers when all other settings are equal. The option **no select** marks the server as unused, except for display purposes.

17.13.1 Default Access Restrictions

The screenshot shows the 'Default Access Restrictions' configuration page. The left sidebar lists various services, with 'NTP' selected. The main configuration area is titled 'Default Access Restrictions' and includes the following settings:

- Kiss of Death:** A toggle switch that is currently off.
- Modifications:** A toggle switch that is currently on.
- Queries:** A toggle switch that is currently off.
- Service:** A toggle switch that is currently off.
- Peer Association:** A toggle switch that is currently on.
- Trap Service:** A toggle switch that is currently on.

Below this is the 'Custom Access Restrictions' section, which includes:

- Networks:** A field for 'IP Address' followed by a slash and a dropdown menu set to '32'.
- Restrictions:** A row of toggle switches for 'KOD', 'Nomodify', 'Noquery', 'Noserve', 'Nopeer', and 'Notrap', all currently off. A red 'X' icon is to the right.
- A green '+ Add' button is located at the bottom right of this section.

© Voleatech GmbH 2017 - 2020

In the **ACLs** tab, you can configure more options:

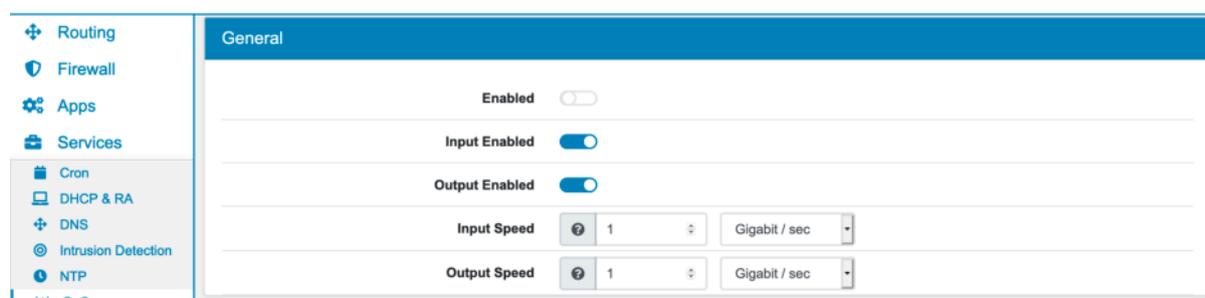
Option	Description	Command
Kiss of Death	Enable KOD packets	kod limited
Modifications	Deny run-time Configuration by ntpq and ntpdc	nomodify
Queries	Disable ntpq and ntpdc queries	noquery
Service	Disable all except ntpq and ntpdc queries	noserve
Peer Association	Deny packets that attempt a peer association	nopeer
Trap Service	Deny mode 6 control message trap service	notrap

17.13.2 Custom Access Restrictions

Here you can add specific restrictions per **network** with all the options listed above.

17.14 QoS

You can find the QoS Settings at **Services** → **QoS**.



QoS can be configured and enabled on a per base interface basis. This means VLANs must be shaped on the underlying base interface, otherwise bandwidth can be used twice, for each VLAN in top of the base interface. Therefore please create different classes on the base interface to manage VLANs. It can be enabled also for Input and Output separately.

QoS usually can only be achieved on traffic leaving the interface. In Order for us to shape traffic that enters the interface, a dummy interface with the name INTNAME-ifb is created. ALL traffic that goes into the interface will go through this DUMMY interface and therefore can also be shaped.

For Bridge members you can only configure the Output Speed.

Note: Output and Input meaning depend on the interface. On WAN Output is traffic leaving the interface to the ISP and therefore upload. Input is download because it is incoming traffic from the ISP. For LAN Input is traffic originating with clients and therefore upload. Output is traffic leaving to the clients and download.

Since traffic is shapped as it either arrives on an interface (INPUT) or leaces an interface (OUTPUT), different setups can be formed. To shape WAN traffic it is enough to enable QoS on WAN only with INPUT (download) and output (upload).

17.14.1 QoS Classes

QoS is organized in classes. Each class can have a **name** and can be **enabled** individually. **All Interfaces** have the same classes, if you create a class in one interface it will also be present on all other interfaces. Classes are limited to **30**. Each class can be configured individually on each interface though regarding to priority and speed.

Classes all have a **priority**. Classes with a higher priority are preferred when there is available bandwidth. The priority is very aggressive though and it is usually advisable to use the same **priority** for all classes and work with the **minimum** and **maximum** values so classes with a high priority are not starved of bandwidth.

Spare/shared Bandwidth is bandwidth that is currently not used. Each class can have a minimum (guaranteed) bandwidth. If it does not use it, it will be shared with other classes as spare bandwidth. Also bandwidth not assigned to any class is spare bandwidth. It will be used by all classes that need them in order by their priority. The minimum bandwidth will be assigned to any class that needs it instantly though and will be removed from shared bandwidth when needed.

Higher priorities are preferred over lower priorities.

Input Min. sets the guaranteed minimum bandwidth for the input. Spare bandwidth is shared with the other classes though.

Input Max. sets the maximum bandwidth for the input. Even when more spare bandwidth is available it will not be used.

Output Min. sets the guaranteed minimum bandwidth for the output. Spare bandwidth is shared with the other classes though.

Output Max. sets the maximum bandwidth for the output. Even when more spare bandwidth is available it will not be used.

17.14.2 QoS Assignment

QoS is assigned in Firewall Rules either global or local *Firewall Rules (Forward and Input)* under the advanced settings. You can choose a class for input and output. Those will be used on any enabled QoS interface. Make sure the according interfaces have QoS enabled.

17.14.3 Limiter

If you need to only set Limiters, they are tied to the firewall rules and can be found at *Firewall Rules (Forward and Input)* under the advanced setting of each firewall rule. All matching traffic is bound to the limiter setting.

Be aware that firewall rules limiters are only “one way”. If you want to limit upload and download, you need to have two firewall rules. The Download must always be shaped on WAN and Upload on LAN, where the traffic enters the firewall first. *Global Firewall Rules (Forward and Input)* with the parameter matching might be better suited for a flexible limiter setup. With match, the rule will only do the shaping. A separate allow rule is still required.

17.15 SNMP

You can find the SNMP Settings at **Services** → **SNMP**.

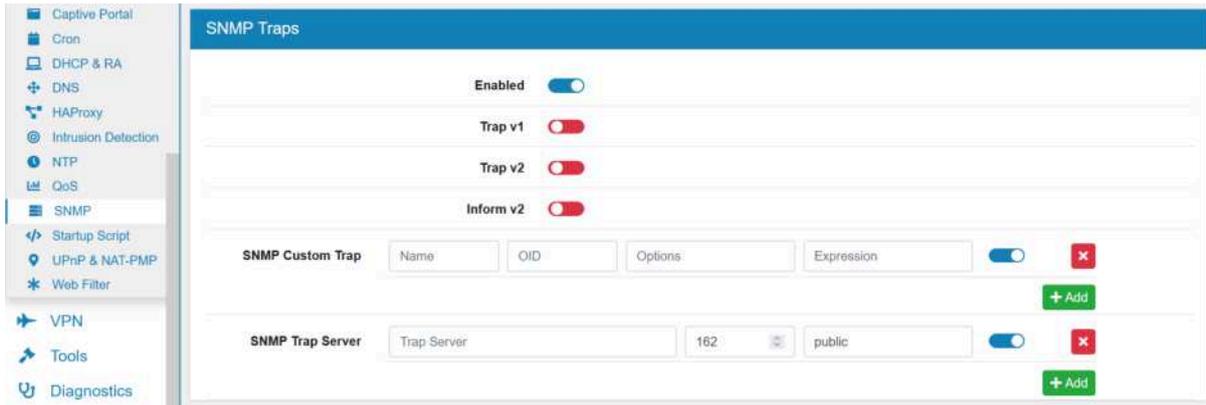
The screenshot displays the Mikrotik WinBox configuration for SNMP. On the left is a sidebar menu with categories like Routing, Firewall, Apps, Services, Cron, DHCP & RA, DNS, Intrusion Detection, NTP, QoS, SNMP, Startup Script, UPnP & NAT-PMP, Webfilter, and VPN. The main area is divided into sections: 'General' (with fields for Enabled, Interfaces, Port, System Location, System Contact, Enable SNMP v2, and Read Community String), 'SNMPv3' (with a form for adding a user including Username, SHA, Hash Password, AES, and Encryption Password), and 'SNMP Traps' (with an Enabled toggle).

The **Simple Network Management Protocol** lets you collect and organize information about the TBF from other devices.

At general you can **enable** or **disable** the whole service and define on which **interface** it's running. The **port** is 161 by default. **System location** and **system contact** have placeholder words and can also be changed. The **read community string** is *public* by default and can be left blank to disable read access.

The **write community string** is disabled by default. You can only write to TBF OIDs not to general system OIDs.

For **SNMPv3** multiple users can be created with the parameters username, access rights, password, hash and encryption algorithm.



At the bottom of the page SNMP traps can be enabled. Select whether the trap should be for V1 and or V2 and an information request shall be sent.

You can create multiple custom traps with a name, OID, options and expression. Also multiple trap servers with an IP address and port can be specified, together with a community string.

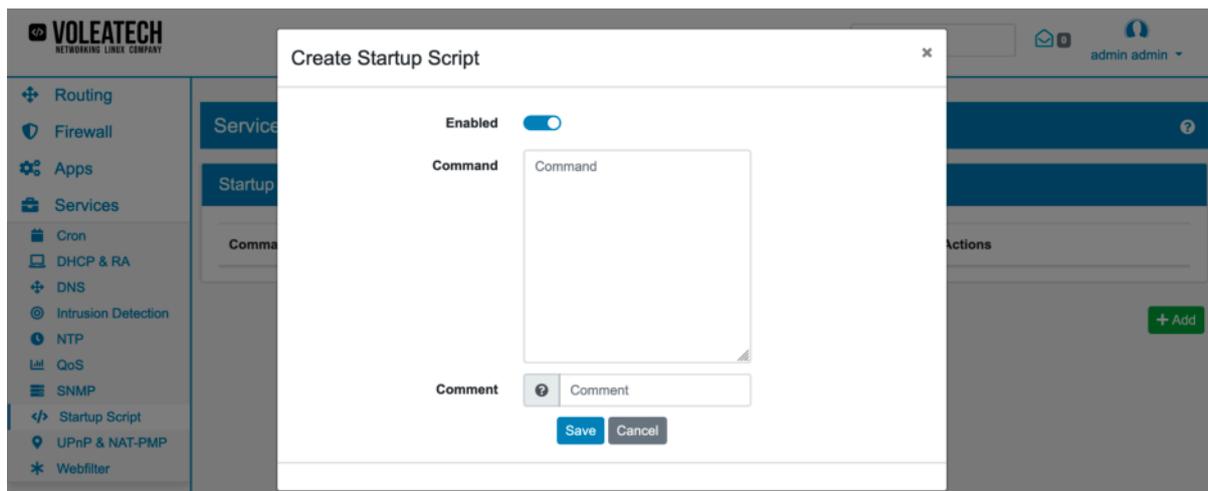
17.15.1 SNMP MIB

The TBF offers custom system information via MIB (Management Information Base) for the following OIDs:

- 1.3.6.1.4.1.53277.1.1.1.1 - SHDSL
- 1.3.6.1.4.1.53277.1.2.1.1 - VDSL
- 1.3.6.1.4.1.53277.2.1.1.1 - Software
- 1.3.6.1.4.1.53277.3.1.1 - Interfaces
- 1.3.6.1.4.1.53277.4.1.1.1 - Temperature
- 1.3.6.1.4.1.53277.5.1.1.1 - System
- 1.3.6.1.4.1.53277.6.1.1.1 - IPSec
- 1.3.6.1.4.1.53277.7.1.1.1 - Open VPN Server
- 1.3.6.1.4.1.53277.8.1.1.1 - Open VPN Client
- 1.3.6.1.4.1.53277.9.1.1.1 - WireGuard
- 1.3.6.1.4.1.53277.10.1.1.1 - Cellular

17.16 Startup Scripts

You can find the Startup Script Settings at **Services** → **Startup Script**.



Here you can see all commands which get executed when the system boots up.

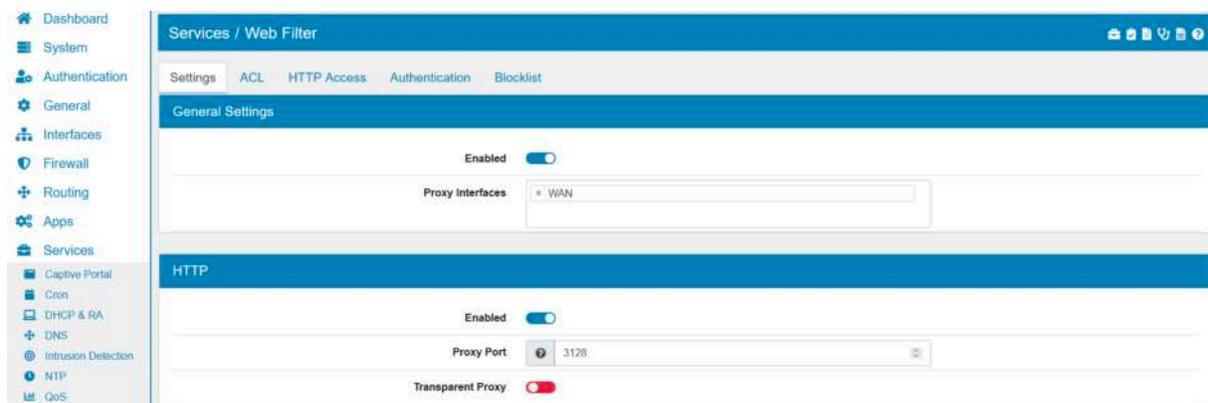
You can create your own startup entries with your own **command**. If the command needs a file, for example if it executes a script, the file has to be put into place manually.

17.17 Web Filter

You can find the Web Filter Settings at **Services** → **Web Filter**.

The Web Filter is using **SquidProxy**, a caching proxy for the Web supporting HTTP, HTTPS and more.

17.17.1 Settings



General Settings

Enabled can be changed to enable or disable Web Filter. It's disabled by default.

Proxy Interfaces are the interfaces and addresses the proxy is running on.

You can export the settings in the top right corner as an Excel spreadsheet.

HTTP

Enabled can be changed to enable or disable HTTP. It's enabled by default.

Proxy Port is the port the HTTP proxy server will listen on. Default is 3128.

Transparent Proxy can be enabled to make the proxy act as a transparent proxy. It's disabled by default. The Transparent HTTP Proxy always runs on 127.0.0.1 port 3129. Please DNAT the traffic to the address.

HTTPS

Enabled can be changed to enable or disable HTTPS. It's disabled by default.

Proxy Port is the port the HTTPS proxy server will listen on. Default is 3129.

Transparent Proxy can be enabled to to make the proxy act as a transparent proxy. It's disabled by default. The Transparent HTTPS Proxy always runs on fd00:7371:7569:6470:726f:7879::1 port 3129. Please DNAT the traffic to the address. Since traffic is encrypted and the Transparent Proxy of TBF does not do a Man in the Middle Attack the desired information are obtained from looking at the connection start and extracted IPs and the SNI field. This leaves the client without warnings about the connection while obtaining enough information to evaluate HTTP Access rules.

HTTPS Proxy Mode can be configured when *Transparent Proxy* is enabled. It can be either *SNI Scan* or *Man-in-the-Middle*. *SNI* will look at the SNI field during the TLS handshake. *Man-in-the-Middle* will break the connection and presents the client it's own *Certificate*. The client must trust the *Certificate* or a browser warning is generated.

Verify DNS Verify HTTPS Header Domain against the DNS entry. Disabling this allows security risks like spoofing. On the other hand google or amazon sites usually do not work when transparent SSL is enabled because they use so many DNS entries.

Certificate can be configured which certificate will be used.

The screenshot displays the configuration page for the Webfilter service in the Beldin Firewall (TBF) management interface. On the left is a navigation menu with options like Routing, Firewall, Apps, Services, Cron, DHCP & RA, DNS, Intrusion Detection, NTP, QoS, SNMP, Startup Script, UPnP & NAT-PMP, Webfilter (selected), VPN, and Tools. The main content area is divided into two sections: 'HTTPS' and 'Cache Settings'. The 'HTTPS' section includes:

- Enabled:** A toggle switch that is currently turned on.
- Proxy Port:** A text input field containing the value '3129'.
- Transparent Proxy:** A toggle switch that is currently turned off.
- Verify DNS:** A toggle switch that is currently turned on.
- Certificate:** A dropdown menu showing 'VT AIR Certificate'.

 The 'Cache Settings' section includes:

- Memory Cache Size:** A text input field containing the value '256'.
- Hard Disk Cache Size:** A text input field containing the value '100'.

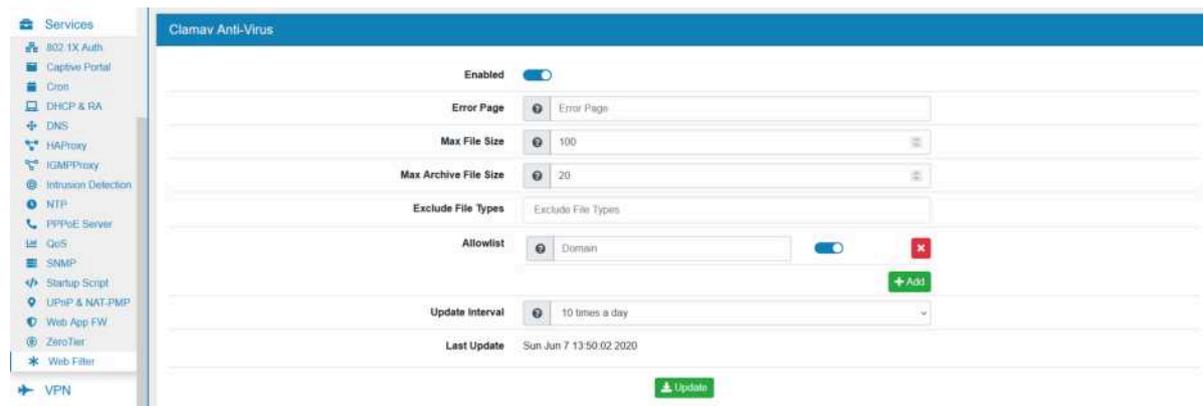
Cache Settings

Hard Disk Cache Size is the amount of disk space to use in megabytes. The default is 100 MB.

Memory Cache Size specifies the ideal amount of memory to be used in megabytes. Default is 256 MB.

Clamav Anti-Virus

ClamAV can scan the webtraffic of the proxy for viruses. This only works when the traffic can actually be seen unencrypted and is ineffective in the transparent HTTPS case.



Enabled enable or disable the virus scan.

Error Page is the complete url of an error page where the user is redirected to if a virus is found.

Max File Size is maximum file size to scan in MB.

Max Archive File Size is maximum archive file size to scan (e.g. ZIP) in MB.

Exclude File Types can be used to exclude specific file types from the virus scan.

You can add multiple *Domains* to configure an **Allowlist**. Traffic from those Domains will not be scanned by the virus engine.

Update Interval specifies how often the virus definition should be updated during a 24 hour period.

WPAD Autoconfigure

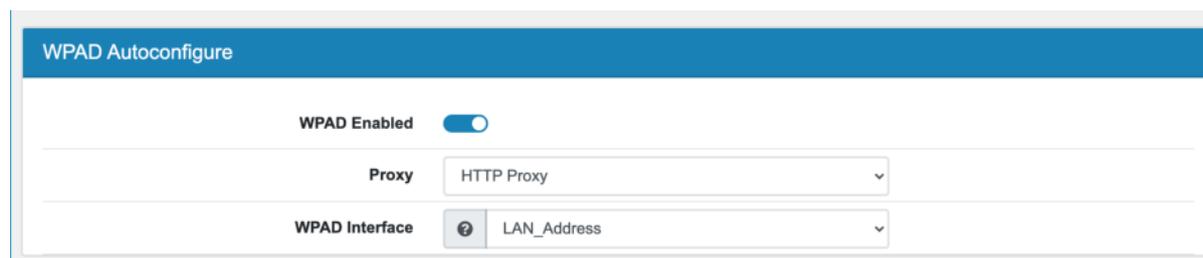
WPAD allows your clients to enable the Auto Proxy setting and find the TBF Webfilter.

Proxy lets you choose the HTTP or HTTPS proxy port.

WAPD Interface is the interface address used to propagate to the clients. Only one ipaddress can be used here so make sure that the connection is allowed in the Firewall.

A DNS record with wpad is created to find the settings.

The wpad file is served by the webserver over port 80.



Advanced

Upstream Proxy URL is the entire Upstream Proxy URL e.g. `http://user:password@proxy.server:port/`.

Visible Hostname will be displayed in proxy server error messages. Default is localhost.

Administrator's Email will be displayed in error messages to the users. Default is `admin@localhost`.

DNS Server 1 and **DNS Server 2** can be configured here.

Number of CPUs is by default the number of available CPUs minus one. The Webfilter will run on all configured CPUs allowing for a higher processing capacity.

Pre ACL Custom Options can be used for custom configuration parameters for the config. They will be placed before the ACL data.

Post ACL Custom Options can be used for custom configuration parameters for the config. They will be placed after the ACL data.

The screenshot shows the 'Advanced' configuration page for the Web Filter. The left sidebar contains a navigation menu with items like Interfaces, Firewall, Routing, Apps, Services, Captive Portal, Cron, DHCP & RA, DNS, HAProxy, Intrusion Detection, NTP, QoS, SNMP, Startup Script, UPnP & NAT.PMP, Web Filter, VPN, Tools, and Diagnostics. The main content area is titled 'Advanced' and contains the following configuration fields:

- Upstream Proxy URL:** A text input field with a help icon.
- Visible Hostname:** A text input field with a help icon, containing 'localhost'.
- Administrator's Email:** A text input field with a help icon, containing 'admin@localhost'.
- DNS Server 1:** A text input field containing 'DNS Server 1'.
- DNS Server 2:** A text input field containing 'DNS Server 2'.
- Number of CPUs:** A numeric input field containing '11'.
- Pre ACL Custom Options:** A large text area for custom configuration parameters.
- Post ACL Custom Options:** A large text area for custom configuration parameters.

17.17.2 ACL

The screenshot shows the 'Services / Web Filter / ACL' configuration page. The left sidebar contains a navigation menu with items like Dashboard, System, Authentication, General, Interfaces, Firewall, Routing, Apps, Services, Captive Portal, Cron, DHCP & RA, DNS, Intrusion Detection, NTP, QoS, SNMP, Startup Script, and UPnP & NAT.PMP. The main content area is titled 'Services / Web Filter / ACL' and contains a sub-menu with 'Settings', 'ACL', 'HTTP Access', 'Authentication', and 'Blocklist'. The 'ACL' sub-menu is selected, and the page shows a table of ACL entries:

ACL Type	Definition	Description	Actions
Port	80 21 443 70 210 1025-65535 280 488 591 631 777	Safe Ports	
Port	443	SSL Ports	
Source	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 fc00::/7 fe80::/10	Localnet	
Custom	localhost	localhost	
Custom	proxy_auth REQUIRED	LDAP Authentication required	
Custom	all	All	

At the bottom right of the table, there is a '+ Add' button. At the bottom center, there is a page number '1' in a box.

Defining an Access List. An ACL has a type Source, Destination Domain, Destination Regex, Port, Protocol or Custom. *Custom* allows you to pick an ACL Type from the Squid manual ([Squid ACL](#)).

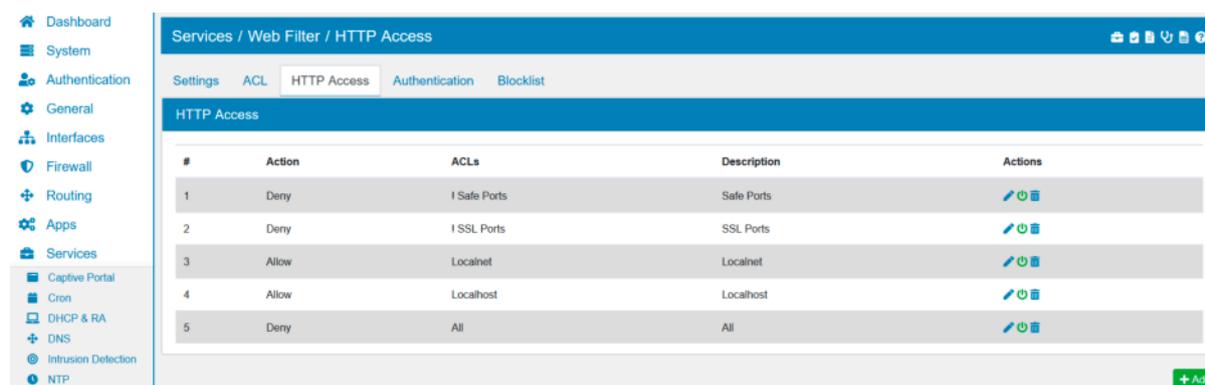
An ACL entry can have one or multiple entries and you have to enter one per line. For example the ACL Source could contain:

- 192.168.100.1
- 192.168.101.0/24

Log Full Traffic enables you to log the full data packet that matches this ACL. For HTTPS traffic it must be bumped first so it can be read unencrypted.

SSL Bump SSL Bump and look into SSL traffic. Splice reads the SNI field and the certificate but does not decrypt the traffic. Bump will create a MITM with the squid certificate and encrypt and decrypt all traffic. The option allows you to only read or encrypt matching traffics. Please run Squid in HTTPS mode and choose a **Certificate** or this option will not have an effect.

17.17.3 HTTP Access



#	Action	ACLs	Description	Actions
1	Deny	I Safe Ports	Safe Ports	
2	Deny	I SSL Ports	SSL Ports	
3	Allow	Localnet	Localnet	
4	Allow	Localhost	Localhost	
5	Deny	All	All	

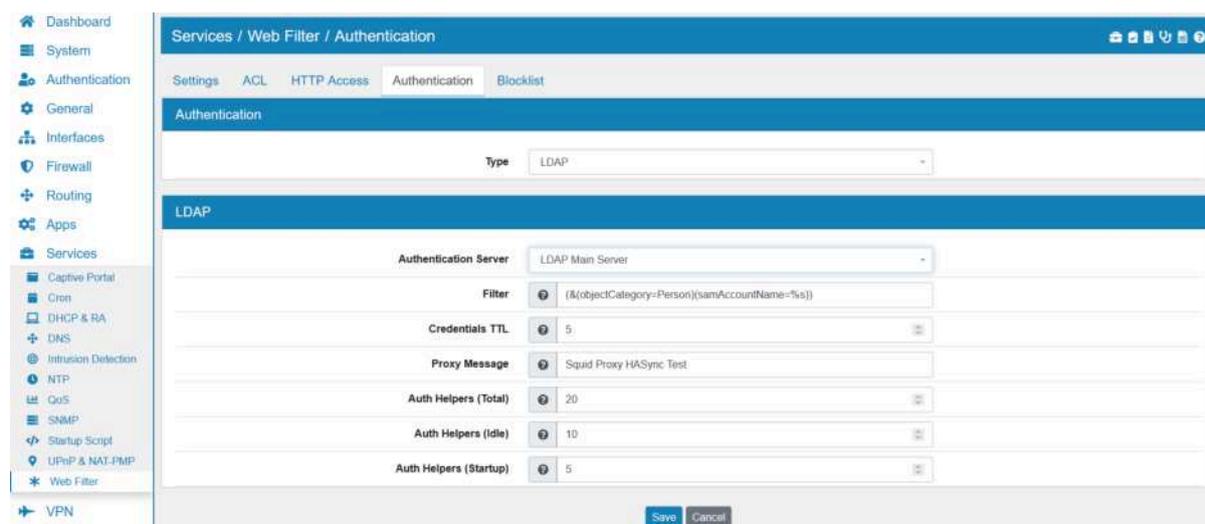
Allowing or Denying access based on defined access lists. HTTP Access lists are defined by combining ACLs with either AND or OR. You can also negate an ACL with NOT.

This allows you to define access or decline access based on ACLs.

For example to deny access to www.google.com you have to create an ACL of type Destination Domain. You can use that ACL in HTTP Access of type Deny.

The order of HTTP Access matters and you can *drag & drop* entries in the list to create the desired order.

17.17.4 Authentication



Type: LDAP

Authentication Server: LDAP Main Server

Filter: (&(objectCategory=Person)(samAccountName=%s))

Credentials TTL: 5

Proxy Message: Squid Proxy HASync Test

Auth Helpers (Total): 20

Auth Helpers (Idle): 10

Auth Helpers (Startup): 5

Save Cancel

Here you can setup an additional authentication method. You can choose between *LDAP* and *Active Directory*.

LDAP

Authentication Server can be selected from the authentication servers you created in the TBF.

Filter is an LDAP search filter to locate the user DN. Required if the users are in a hierarchy below the base DN, or if the login name is not what builds the user specific part of the users DN. It is (&(objectCategory=Person)(samAccountName=%s)) by default.

Credentials TTL is the time in minutes after credentials will be rechecked. Default value is 5.

Proxy Message is the proxy authentication informational message for your proxy users. Default is Squid Proxy.

Auth Helpers (Total) is the total number of authentication helpers to run. It is recommended to set it equal to the approximate number of proxy users in the network. Default value is 20.

Auth Helpers (Idle) is the idle number of authentication helpers to run. It is recommended to make it equal to about half of the total number of users in the network. Default value is 10.

Auth Helpers (Startup) is the number of authentication helpers to run at startup. It is recommended to make it equal to about a quarter of the total number of users in the network. Default value is 5.

In order to enforce the authentication, you need to create a HTTP Access rule that includes the predefined ACL **proxy_auth REQUIRED**.

Active Directory

Domain name short is the first part of the domain name.

Domain name long is the full domain name.

Authentication Processes is the number of authentication processes. It is recommended to make it equal to about a quarter of the total number of users in the network. Default value is 10.

17.17.5 Blocklist

Allows you to use the UT1 blocklist by selecting several categories.

The screenshot shows the configuration page for the Web Filter Blocklist. The 'Enabled' toggle is turned on. The 'Update Interval' is set to 'Weekly'. The 'Error URL' field contains the following text: `http://admin.foo.bar.de/cgi-bin/blocked.cgi?clientaddr=%a&clientname=%n&clientuser=%s&clientgroup=%s&targetgroup=%t&url=%u`. Below the settings is a table of Blocklist Categories:

Name	Domains	URLs	Actions
ads	ⓘ	ⓘ	ⓘ
adult	ⓘ	ⓘ	⊘
aggressive	ⓘ	ⓘ	ⓘ
agresif	ⓘ	ⓘ	ⓘ

Enabled enable or disable the blocklists.

Update Interval specifies how often the blocklist definition should be updated.

Error URL can be defined and is `http://admin.foo.bar.de/cgi-bin/blocked.cgi?clientaddr=%a&clientname=%n&clientuser=` by default. An error URL **NEEDS** to be defined or no blocking will happen.

Blocklist Categories can be enabled or disabled. By default *adult*, *cryptojacking*, *ddos* and *malware* are enabled. The *Domains* and *URLs* of each category can be displayed by clicking on the information button.

Multiple **Whitelists** can be added with their ip address and netmask.

17.17.6 Example Proxy Configuration

Web Filter can be configured as a Proxy in your network. This means that traffic from inside your network can be analyzed before leaving towards the internet and web content entering your network can be cached. This is useful for blocking access to specific services that are unwanted but not necessarily malicious (which is a task for Intrusion Detection *Intrusion Detection*) and to save on bandwidth when browsing the internet with multiple clients in your local network.

A typical configuration is shown here. Go to **Services** → **Web Filter** and enable the package. Typically you'd want your local network (e.g. *LAN*) selected as the **Interface**.

Transparent Proxy

Top configure your Web Filter as a transparent proxy that caches web traffic for your local network, enable **HTTP** and **HTTPS** as well as the **Transparent Proxy** option on both.

Be aware that the **HTTPS** transparent proxy can not look inside encrypted traffic. Only the certificate and hostname are visible to make decisions.

Proxy with anti-virus

Then Enable **ClamAV Anti-Virus** and choose an update interval. The anti virus can only inspect unencrypted traffic. For **HTTPS** transparent proxy no virus scan can be performed.

Blocklists

Enable **Blocklist** and choose an update interval to pull in the predefined blocklists.

To configure your blocklist settings go to **Services** → **Web Filter** → **ACL**. Here you can find an overview of all the blocklisting categories that are available. Go to **Services** → **Web Filter** → **HTTP Access** to create the filtering rules.

Click **Add** or **Edit** to create or edit the blocklist rule. Set **Action** to *Deny*, **Logical Operator** to *OR* and add all the blocklist categories that you want to block under **ACL**.

The screenshot shows the Voleatech web interface for configuring a Squid Proxy ACL rule. The left sidebar contains a navigation menu with options like Routing, Firewall, Apps, Services, Cron, DHCP & RA, DNS, NTP, QoS, SNMP, Squid Proxy (selected), Suricata (IDS/IPS), Startup Script, UPnP & NAT-PMP, VPN, Tools, and Diagnostics. The main content area is titled "Services / Squid Proxy / Create" and includes a search bar and a user profile "admin admin". The configuration form has the following fields:

- Name:** (empty text field)
- Enabled:** A toggle switch that is currently turned on.
- Action:** A dropdown menu set to "Deny".
- Logical Operator:** A dropdown menu set to "OR".
- Description:** A text input field with the placeholder "Description".
- ACL:** A list of three items, each with a toggle switch and a red 'X' icon:
 - Toggle: off, Path: /etc/squid/blacklist/anonvpn
 - Toggle: off, Path: /etc/squid/blacklist/chat
 - Toggle: off, Path: /etc/squid/blacklist/hacking
- + Add:** A green button to add more ACL entries.
- Save / Cancel:** Buttons at the bottom of the form.

© Voleatech GmbH 2017 - 2020

17.18 UPnP & NAT-PMP

You can find the UPnP & NAT-PMP Settings at **Services** → **UPnP & NAT-PMP**.

The screenshot shows the Voleatech web interface for configuring UPnP & NAT-PMP settings. The left sidebar is the same as in the previous screenshot, with "UPnP & NAT-PMP" selected. The main content area is titled "General" and includes the following configuration options:

- Enabled:** A toggle switch that is currently turned on.
- UPnP Port Mapping:** A toggle switch that is currently turned on.
- NAT-PMP Port Mapping:** A toggle switch that is currently turned on.
- External Interface:** A dropdown menu set to "WAN".
- Interfaces:** A list of available interfaces: Localhost, WAN, LAN (selected), AppBridge, and UPnP & NAT-PMP.
- Override External Address:** A text input field with a question mark icon and the placeholder "Override External Address".
- Packet Log:** A toggle switch that is currently turned off.
- System Uptime:** A toggle switch that is currently turned off.
- Default Deny:** A toggle switch that is currently turned off.
- Custom Presentation URL:** A text input field with a question mark icon and the placeholder "Custom Presentation URL".

© Voleatech GmbH 2017 - 2020

The **Universal Plug and Play** allows network devices to see each other on the network and establish a network connection. While the **NAT Port Mapping Protocol** allows automatic configuration of address translation and port forwarding.

Both will create Firewall and NAT table entries automatically.

On the setup page it's possible to **enable** the service which is disabled by default. You can enable the **UPnP Port Mapping** or the **NAT-PMP Port Mapping** as well as both. The **External Interface** as well as a set of **Interfaces** can be set up. With **Override External Address** an alternate external address to accept inbound connections, e.g. IP Alias or CARP Virtual IP address, can be setup. **Default Deny** denies access by default. **Packet Log** enables the logging of packets. **System Uptime** reports the system uptime instead of the daemon uptime. You can configure a **Custom Presentation URL** but by default the TBF URL will be used. For the optional **Custom Model Number** the TBF firmware version will be used by default. Finally multiple **ACL Entries** can be configured. Each entry is either allow or deny, has an **External and Internal Port**, an **IP Address** and an optional **Netmask**. Otherwise devices will create NAT and Firewall entries without a way of controlling them.

17.19 Web Application Firewall

You can find the Web Application Firewall Settings at **Services** → **Web Application FW**.

The **Web Application Firewall** (WAF) is a specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service.

Before you can use the Web Application Firewall it has to be installed. You can install it at **System** → **Addons**.

You can export the settings in the top right corner as an Excel spreadsheet.

The **Web Application Firewall** is integrated into HAProxy and requires you to configure HAProxy accordingly. The Web Application Firewall needs to be able to read the entire web traffic without encryption. HAProxy might need to be configured for SSL Offloading for that purpose.

17.19.1 OWASP Core Ruleset

The TBF **Web Application Firewall** uses the OWASP ModSecurity Core Rule Set.

The OWASP Core Ruleset is designed to work as a single entity to calculate a threat score and execute an action based on that score. When a rule in the ruleset matches a request, the threat score increases according to the rule score. If the final threat score is greater than the configured score threshold, WAF executes the action configured in the last rule of the ruleset.

17.19.2 Settings

Here the Web Application Firewall can be enabled or disabled.

The **Security Rule Engine** can be *On*, *Off* or *DetectionOnly*.

The **Paranoia Level** is defined as a number between 1 and 4. With a higher paranoia level additional rules are enabled and the level of security increases. However, higher paranoia levels also increase the possibility of blocking some legitimate traffic due to false alarms. Default is 1.

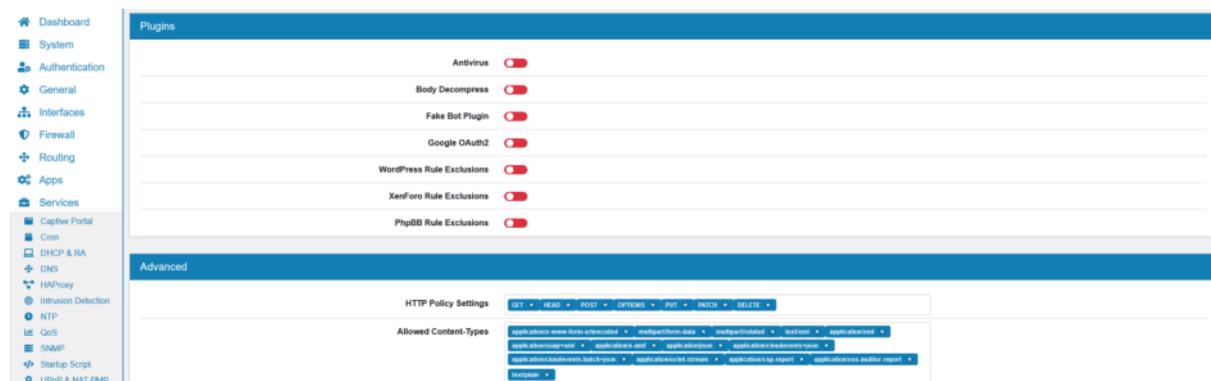
Rules Update Interval is a cronjob which will update the rules according to the selected time interval.

17.19.3 Allowlist

Multiple **Allow IPs** can be added with their ip address and port. The IPs will not be checked by the WAF.

Multiple **Allow URIs** can be added with their URI. The URIs will not be checked by the WAF.

17.19.4 Plugins



Here you can enable the following WAF plugins:

- Antivirus
- Body Decompress
- Fake Bot Plugin
- Google OAuth2
- WordPress Rule Exclusions
- XenForo Rule Exclusions
- PhpBB Rule Exclusions

If you use any of the applications it is advisable to enable the plugin. The plugins will enable special rules and exceptions for the Application for extra protection or to avoid false positives.

17.19.5 Advanced

HTTP Policy Settings and default is GET, HEAD, POST, OPTIONS, PUT, PATCH and DELETE.

Allowed Content-Types are the Content-Types that a client is allowed to send in a request. Default is application/x-www-form-urlencoded, multipart/form-data, multipart/related, text/xml, application/xml, application/soap+xml, application/x-amf, application/json, application/cloudevents+json, application/cloudevents-batch+json, application/octet-stream, application/csp-report, application/xss-auditor-report and text/plain.

Allowed HTTP versions and default is HTTP/1.0, HTTP/1.1, HTTP/2 and HTTP/2.0.

Forbidden file extensions and default is asa, asax, ascx, axd, backup, bak, bat, cdx, cer, cfg, cmd, com, config, conf, cs, csproj, csr, dat, db, dbf, dll, dos, htr, htw, ida, idc, idq, inc, ini, key, licx, lnk, log, mdb, old, pass, pdb, pol, printer, pwd, rdb, resources, resx, sql, swp, sys, vb, vbs, vbproj, vsdisco, webinfo, xsd and xsx.

Forbidden request headers and default is proxy, lock-token, content-range, if and user-agent.

File extensions considered static files and default is jpg, jpeg, png, gif, js, css, ico, svg and webp.

Allowed Charsets are the Content-Types charsets that a client is allowed to send in a request. Default is utf-8, iso-8859-1, iso-8859-15 and windows-1252.

At the bottom you can add **Custom Rules**.

17.19.6 Rules

Name	Details	Actions
REQUEST-901-INITIALIZATION		
REQUEST-905-COMMON-EXCEPTIONS		
REQUEST-910-IP-REPUTATION		
REQUEST-911-METHOD-ENFORCEMENT		
REQUEST-912-DOS-PROTECTION		
REQUEST-913-SCANNER-DETECTION		
REQUEST-920-PROTOCOL-ENFORCEMENT		

Here you can see all installed and used rule files. Each rule file can be disabled and enabled on the actions column on the right side. You can also click on the detail icon of each rule to see the specific definition of it.

Multiple **Remove Rules** can be added to disable specific rules by their Rule ID.

17.20 ZeroTier

You can find the ZeroTier Settings at **Services** → **ZeroTier**.

ZeroTier creates secure networks between on-premise, cloud, desktop, and mobile devices. The connection of **ZeroTier** is a spoke connection.

Please sign up for [ZeroTier](#) first to use configure the service.

Before you can use the ZeroTier it has to be installed. You can install it at **System** → **Addons**.

Here you can see all ZeroTiers which have been created.

A ZeroTier can be enabled or disabled.

Name so you can identify it.

The **Network ID** is a 16 character long value. You must get the network ID from your zero tier configuration.

Allow Managed lets a Zero Tier One Manage the IP Address assignment. In a Bridge setup, disables this option and set IP Address on the Bridge interface manually.

17.20.1 Multipath

Allows you to use more than one interface at a time in Fallback or Bonding mode.

The **Bonding Policy Port** can be either *None*, *Active Backup*, *Broadcast*, *Balance RR*, *Balance XOR* or *Balance Aware*.

Multiple **ZeroTier Links** can be added with an *Interface*.

Each Link has the following settings:

The **Speed** is how fast this link is (in arbitrary units). It's a value between 1 and 1000000.

Allocation is a relative value representing a desired allocation. It's a value between 1 and 255.

The **Mode** determines whether this link is used by default or only after failover events. It can be either *undefined*, *primary* or *spare*.

It is enough to set either **Speed** or **Allocation** in order to distribute the traffic between the links.

18.1 IPsec

18.1.1 IPsec General Settings

You can find the IPsec Settings at **VPN** → **IPsec** → **Global Settings**.

The screenshot shows the 'VPN / IPsec / Settings' page with the 'Global Settings' tab selected. The left sidebar contains a navigation menu with items: Dashboard, System, Authentication, General, Interfaces, Firewall, Routing, Apps, Services, VPN, IPsec, OpenVPN, WebVPN, WireGuard, Tools, and Diagnostics. The main content area is divided into two sections: 'General' and 'Logging'. The 'General' section includes: 'Enable Cisco Extensions' (toggle on), 'Exclude LAN Network' (toggle on), 'Replay Window Protection' (dropdown set to 2048), and 'Hardware Offload' (dropdown set to Auto). The 'Logging' section includes: 'IKE SA' (dropdown set to Control), 'IKE SA Child' (dropdown set to Control), 'Configuration Backend' (dropdown set to Control), and 'Advanced Settings' (toggle on).

Enable Cisco Extension might be necessary to have multiple *IPsec Phase 2* entries in IKEv1, if the remote side needs it.

Exclude LAN Network allows to exclude traffic from LAN subnet to LAN IP address from IPsec.

Replay Window Protection is the size of the AH/ESP replay window, in packets. Default is 2048. The replay window affects the performance.

Hardware Offload can be Auto or No. Default is Auto. If you have a Mellanox or Intel card with a compatible IPsec offload auto will detect and offload the connection.

Logging

You can configure various logging settings. The three most important logging settings are

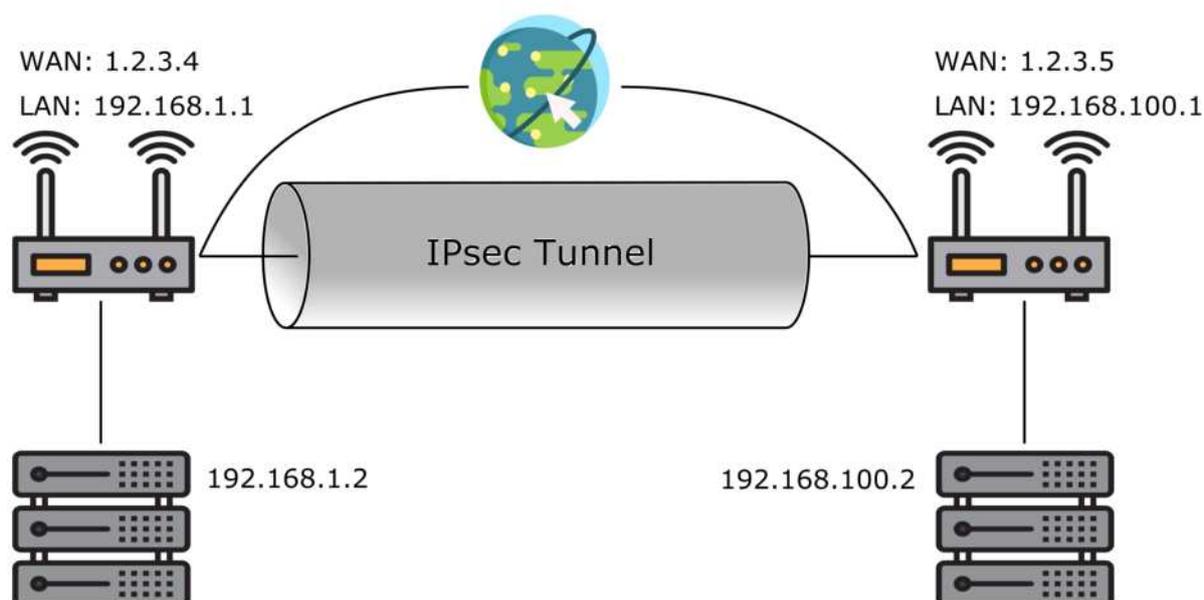
- IKE SA
- IKE SA Child
- Configuration Backend

If you run into any configuration issues with IPsec, it is advisable to change the logging to DEBUG on those Settings. Under **Advanced Settings** you can configure more advanced logging settings.

18.1.2 IPsec Phase 1

IPsec, also known as the Internet Protocol Security or IP Security protocol, defines the architecture for security services for IP network traffic.

It secures traffic between two entities, either by full encryption or by authentication only.



This image was created with icons by [srip](#) and [Freepik](#) from [Flaticon](#).

You can find the IPsec Settings at **VPN** → **IPsec**.

The screenshot shows the VPN / IPsec configuration interface. The sidebar on the left contains navigation options: Dashboard, System, General, Interfaces, Routing, Firewall, Apps, Services, VPN, IPsec, and OpenVPN. The main content area displays the VPN / IPsec configuration page with tabs for Tunnels, Client Settings, and Global Settings. The IPsec Entries table shows one entry: Site2Site, IKEv2, Tunnel, WAN, 1.2.3.4, LAN_Network -> 192.168.1.0/24 (Tunnel 1), Site2Site. There is a + Add button at the bottom right.

Name	Type	Mode	Source	Remote Endpoint	Phase 2	Description	Actions
Site2Site	IKEv2	Tunnel	WAN	1.2.3.4	LAN_Network -> 192.168.1.0/24 (Tunnel 1)	Site2Site	Edit Refresh Delete

Phase 1

The IPsec Phase 1 negotiates the encryption and setting parameter. In TBF you have various options to configure a Phase 1.

Interfaces is the sender Interfaces. It also sets the source IP of the IPsec Tunnel on the TBF end. If the Interface is a VRRP virtual IP of a HA Setup, only the Master holding the IP has the tunnel activated. The Slave will be on standby for the IPsec. You can select multiple Interfaces here. Be aware that the default route of the system is used when the TBF is initializing the connection and therefore only the IP of the interface of the default Route is used. If you choose *Any* the system will select the IP based on the default route and active interfaces. This is useful for Backup connections if you have multiple Gateways and will select the current interfaces faster.

IPsec Interface lets you choose an existing IPsec interface. It only works if the Phase 2 networks don't overlap.

IP Type is either IPv4 or IPv6.

IKE Type can be IKEv1 and IKEv2. It is highly recommended to use IKEv2 as it is saver, more robust and easier to setup.

Connection Type can be

- Tunnel
- Transport

Tunnel creates a tunnel between the two tunnel endpoints. Traffic is automatically encrypted if the source and destination match the *IPsec Phase 2*.

Transport mode causes the IPsec protocol to encrypt only the payload of an IP packet. The protocol then encloses the encrypted payload in a normal IP packet. Traffic sent in Transport mode is less secure than traffic sent in Tunnel mode, because the IP header in each packet is not encrypted. It encrypts all traffic between the two entities and only has a single *IPsec Phase 2* to configure the transport parameter.

Encryption Type is either ESP or AH.

ESP (Encapsulating Security Payloads) provides confidentiality, data-origin authentication, connection-less integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic-flow confidentiality.

AH (Authentication Headers) provides connectionless data integrity and data origin authentication for IP datagrams and provides protection against replay attacks.

Init Type can either be Start/On Demand, Start or Nothing. Start/On Demand will try to connect immediately and will install a policy to initiate a connection when the first package is flowing. The policy makes sure that no packet will travel to the endpoint unencrypted and will also start a reconnect when the tunnel is down. Nothing will put the Phase 1 in responder only mode.

Interface will create a XFRM interface in the system for this IPsec Tunnel. The interface can be used like any other interface. You need to manually create routes *Routes* from the Phase 2 to enter the interface. You can also set an IP Address on the interface settings *Configure Interfaces*. The interface will automatically be set to up or down when the Phase 1 is connected or disconnected. It allows for custom routes and metrics that are removed and added when the interface is up or down. You can also choose an existing XFRM interface, as long as the Phase 2 IP pairs do not overlap. This is useful to manage multiple tunnels in a single Interface.

Remote Endpoints one or more IP Addresses of the remote end. Hostnames are also supported but a working DNS is required for them to be resolvable. There is no DNS caching so if a connection is reestablished the name will be looked up again. This allows for DynDNS hostnames. A remote endpoint of 0.0.0.0 will create an any entry in case your remote IP is dynamic. Identification will be done via Identifier and PSK/Certificate in that case.

Note: As an initiator, the first IP Address is used to initiate the connection to. As a responder, the initiator source address must match at least to one of the specified addresses, subnets or ranges. If

FQDNs are assigned they are resolved every time a configuration lookup is done.

Phase 1 Authentication

Phase 1 Authentication provides you with different options to authenticate the connection.

Authentication Method is either Pre Shared Key, Certificate, EAP TLS (Certificate), EAP MD5 or EAP MSCHAPv2. You can either enter a pre shared key that must match on both ends or a certificate and the corresponding CA. EAP MD5 and EAP MSCHAPv2 are usually used for client authentication with a username and password.

Local Identifier is the identifier of the TBF and it is one of

- My IP Address
- IP Address (Custom IP)
- Other

Remote Identifier is the identifier of the remote side and it is one of

- Any
- Peer IP Address
- IP Address (Custom IP)
- Other

Use Two Authentications allows you to define a secondary authentication which has the same options as above.

Phase 1 Settings

Phase 1 Algorithms can be a mix of any of the algorithms. You can add as many combinations as you like.

Lifetime must also match the remote sides lifetime.

Advanced Options give you some more control over the IPSec connection.

Associate Firewall Rule will generate a firewall rule for you and keeps it up to date with any changes you do.

Rekey will let the TBF start renegotiation if the connection is about to expire. If turned off, only the remote side can start the negotiation.

Responder Only if you don't want TBF to start the connection but waits for the remote side to start it.

Close Action can either be Connect, On Demand or Nothing. Connect will try to connect immediately while on demand only initiates a connection when the first package is flowing. Nothing will only close the connection. The default is nothing.

NAT-T should be set to automatic so IPSec can figure out the correct remote IP.

MOBIKE is for the IKEv2 Mobike protocol. Please have a look at [Strongswan Mobike](#) for a more detailed explanation.

IPComp is the IP Payload Compression.

Split Connection for IKEv2 creates a new connection for each *IPSec Phase 2* entry. Usually they are grouped and sent through a single connection. Depending on the endpoint this is not supported and Split Connection needs to be enabled. This is usually required for Cisco ASA.

Dead Peer Detection lets IPSec check if the remote endpoint is still alive.

DPD Delay defines the time between checks. It is 10 by default.

DPD Timeout defines the time before a connection is restarted if the DPD check failed. It is 30 by default.

DPD Action can either be Restart, On Demand or Nothing. Restart will try to restart immediately while demand only initiates a new connection when the first package is flowing. Nothing will only close the connection without further action.

Traffic Selector can only be selected in transport mode. It can be either Any, GRE or VXLAN. In cases other than Any only the selected Protocol/Traffic will be encrypted between the two endpoints.

Fallback IPsec lets another IPsec act as a fallback for this Phase 1. Each IPsec can only be selected once in a fallback scenario.

Ping Check and the following ping options can only be configured if a *Fallback IPsec* has been chosen. The ping check determines when the fallback IPsec should be used.

Ping IP Address defines the Ping IP Address for the fallback check.

Ping Interval defines the interval between the checks in minutes. It is 5 by default.

Ping Retries defines the number of retries before the connection is terminated and initiated when the ping check failed. It is 3 by default and a value of 0 means disabled.

Ping Fallback defines whether there shall be a fallback to the primary tunnel if ping works again. This option depends on if you ping an outer or inner IP. If you ping an inner IP it will be available on the fallback as well. If you ping the primary IP endpoint this option will check the tunnel endpoint and enabling it is advisable.

Ping Cron lets you select an existing Cron object.

Restart Gateway Change Restart the Tunnel on Main Routing Table Gateway Change. This is useful in Multi WAN setups since ipsec does not always change the gateway automatically.

IPsec Action Best Practice

IPsec has three different parameters to manage the start and reconnect behaviour: **Init Type**, **Close action** and **DPD Action**. If not set correctly a combination of them can lead to duplicate tunnel connections.

Two sets of configurations make the most sense:

1. Start connection immediately and restart on failure: **Init Type**: Connect **DPD Action**: Restart **Close Action**: Nothing

If no DPD is used the **Close Action** should be Restart.

2. Start connection when traffic is flowing (also makes sure that no unencrypted traffic is flowing): **Init Type**: On Demand **DPD Action**: Nothing **Close Action**: Nothing

For *Encryption* AES-256 SHA 256 DH-16 is recommended as a minimum for the **phase 1**. AES-GCM is not recommended for the phase 1 but highly recommended for the **phase 2** encryption, as it provides the fastest speed for IPsec.

IPSec Multi WAN Setup

Creating a Multi WAN Setup with automatic failover to a backup WAN also requires to set **Restart Gateway Change**. The IPSec Tunnel does not always follow the Gateway change to a different WAN. The restart will disconnect and reconnect the tunnel to force it to the new active WAN connection.

IPsec with Failover

If you want to configure your IPsec with failover support you can configure your server and clients as described in [IPSec](#).

If you haven't configured your High Availability setup do so as described in [High Availability](#) and enable the Configuration Sync option. Note the Virtual IP address of the Interface your IPsec server runs on.

On your remote device go to **VPN** → **IPsec** and configure your VPN connection. Enter the Virtual IP you noted earlier as **Remote Endpoint** instead of the real address of the device. This way the IP address of the remote device doesn't change in case the secondary router takes control.

Performance

Note: Each SA is assigned to a single CPU. To get the best performance you might want to enable *Split Connection* if you have multiple phase 2 entries. This will create one SA for each phase 2 and therefore utilize more CPUs. It has to be enabled on both ends of the connection.

IPSec Firewall Rules

Note: You need to create Firewall Rules on the IPSec Tab or if you chose to create an Interface, in the newly create XFRM_XXX Interface, in order to allow network traffic from the other end of the ipsec. Please have a look at [Firewall Rules \(Forward and Input\)](#) for a detailed explanation on how to create Firewall Rules for an interface.

18.1.3 IPSec Phase 2

Phase 2 entries can be created below the current Phase 1 entry.

Local Network is the network or address on the TBF that should be accessible from the remote side.

Remote Network is the network or address that should be accessible from the TBF side on the remote side.

VPN / IPsec / Phase 2 / Update

Tunnels Client Settings Global Settings

General

Enabled

Description

Local Network 192.168.0.0 / 24

Remote Network 192.168.1.0 / 24

Each pair of Local <-> Remote Networks needs a Phase 2 entry. In the background the system will create a mapping between the two in order to send it through the IPsec Tunnel.

Algorithms can be a mix of any of the algorithms. You can add as many combinations as you like.

Lifetime must also match the remote sides lifetime.

Phase 2 Algorithms

Ciphers

Lifetime

Ping Check

Ping Check enables a ping check against an IP on the other side of the tunnel. Make sure that at least one of the IP addresses of the TBF is part of the Phase 2 network definition.

Ping IP Address the remote IP address to ping (must be in the remote network range)

Ping Interval the seconds between checks

Ping Retries before the phase 2 is disconnected and reconnected. If you set this value to 0 no disconnect/reconnect is performed on ping errors.

Ping Check

Ping Check

Ping IP Address

Ping Interval

Ping Retries

Note: If you need to create a custom behaviour on the ping check, a custom script can be added to the location `/usr/local/bin/check_ipsec_custom`. It receives two environment variables, PHASE2 with the phase2 name and RESULT with the ping result. 0 is success and 1 is failure.

18.1.4 IPSec Client Settings

You can find the IPSec Client Settings at **VPN** → **IPSec** → **Client Settings**.

General settings allows you to set an EAP Radius Server from the authentication servers to be used for radius authentication for an IPSec Tunnel.

Secrets allow you to define usernames and password for Client authentication. They are either for Pre Shared Keys or EAP MD5/MSCHAPv2. The identifier has to match the remote identifier.

Be aware that secrets are not tunnel specific but will match on any defined Phase 1.

Pools define IP Address Pools to use with a specific Phase 1. The IPs will be send to the client as a DHCP address.

18.1.5 IPSec Route Based (VTI/XFRM)

In TBF it is possible to configure route-based VPNs. Here IPSec processing does not (only) depend on negotiated policies but may e.g. be controlled by routing packets to a specific IPSec interface.

You can create an Interface out of the IPSec Tunnel, which is often referred to as VTI or the newer term XFRM Interface. The advantage of the Interface is that static routes defined on the interface are automatically deleted, when the interface goes down. The Interfaces up and down status is tied to the phase 1 beeing up or down.

The interface does not change the IPSec traffic, therefore the other end of the tunnel does not need any knowledge of it. The Route Based IPSec can also be configured on one end only.

It allows for failover setups where multiple IPSec Tunnels carry the same routes but with different metrics. You can set the Interface to enabled in the Phase 1 settings. The Phase 2 can have any network or networks defined.

You need to manually create routes *Routes* from the Phase 2 to enter the interface. You can also set an IP Address on the interface settings *Configure Interfaces*.

The interface works as any other interface and can have firewall and NAT rules, as well as services running on it. It allows for DNAT/SNAT before the tunnel.

Another advantage of this approach is that the MTU can be specified for the IPSec innterface allowing to fragment packets before tunneling them.

18.1.6 GRE over IPSec

GRE/GRETAP over IPSec can be configured in TBF. This is useful for encrypted site-to-site connections. In most cases it should not be necessary to have a GRE/GRETAP tunnel within your IPsec tunnel since you can add the remote subnets directly to your Phase 2 configuration.

First create a GRE Interface as described in *Tunnel*. Make sure to activate the option **assign to a new interface**. Afterwards configure the Interface in *Configure Interfaces*. Set the GRE Endpoints and the internal IPs (local and remote tunnel IPs) for example 10.10.10.1 (local) and 10.10.10.2 (remote).

Create a new *IPSec Phase 1* and choose **Connection Type** Transport. The **Interfaces** must be the WAN interface that is used to send the GRE packets to the endpoint. The **Remote Endpoints** is the remote tunnel IP (the external tunnel IP of the remote end e.g. 1.2.3.4). Also enable the option **GRE over IPSec** to encrypt only the GRE traffic. Configure the other parameters according to your IPSec endpoint.

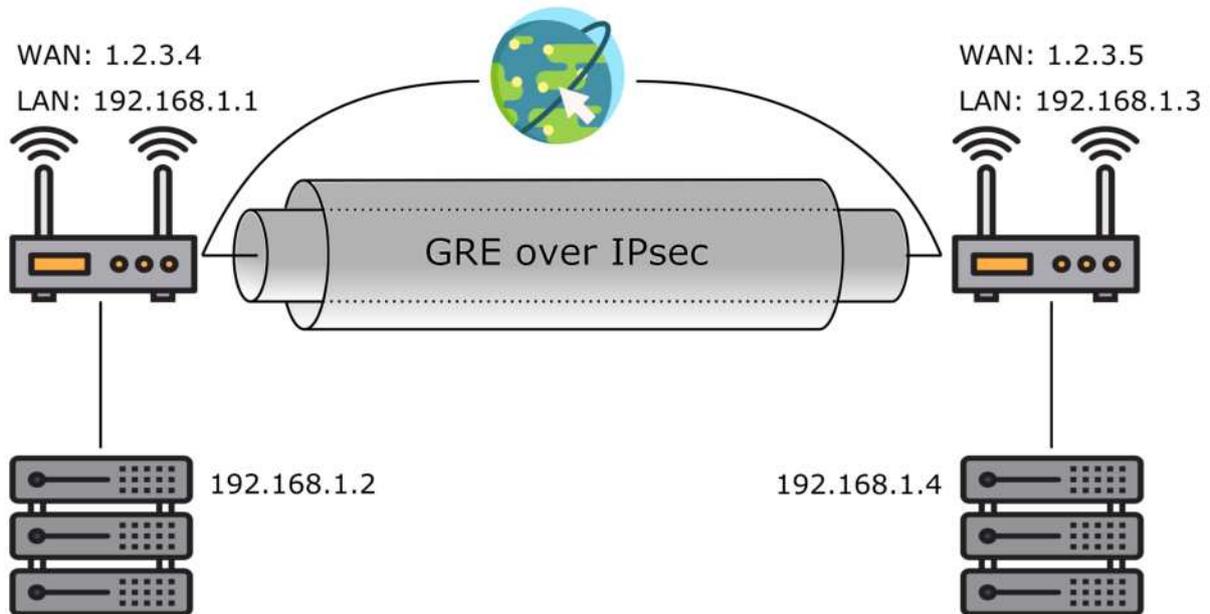
A *IPSec Phase 2* has to created as well with matching encryption parameters.

When the IPSec Tunnel is up it will encrypt all the GRE packets to the remote endpoint.

You might need to add *Routes* to have additional traffic pass the GRE tunnel as well as *Firewall Rules (Forward and Input)* to allow the traffic.

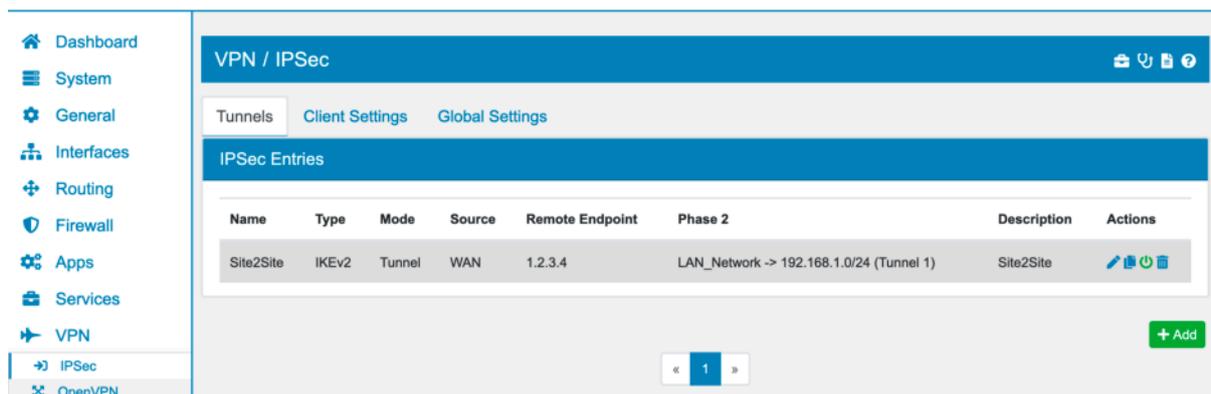
Encrypting Site-to-Site networks

To combine multiple physical locations of your network into e.g. one large company network in a secure way you can use IPsec (and GRE/GRETAP). Follow the steps above and/or refer to *Bridging Scenarios*. This leaves you with a GRE/GRETAP tunnel that is encapsulated and encrypted in an IPsec tunnel. Your networks will then appear as if they were one physical network.



This image was created with icons by [srip](#) and [Freepik](#) from [Flaticon](#).

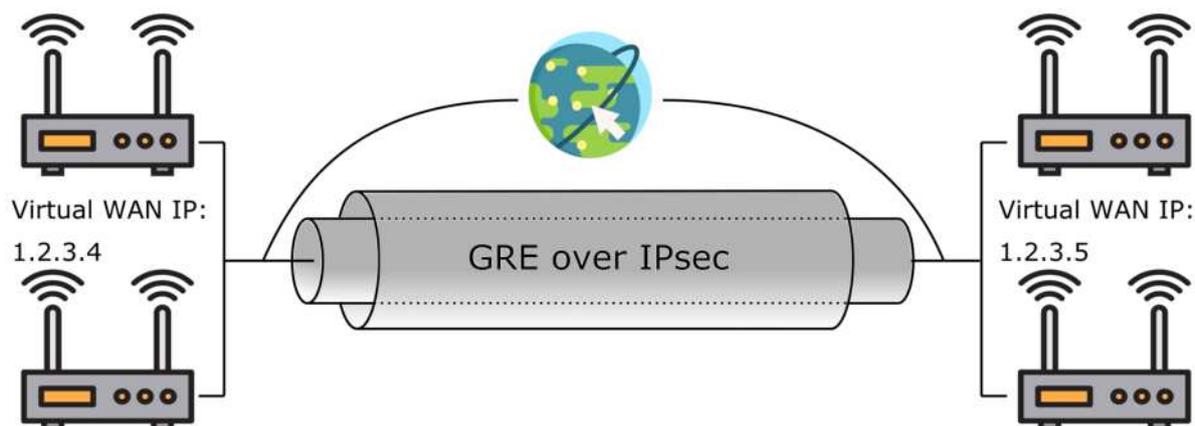
Alternatively to using GRE over IPsec you can also use a standalone IPsec tunnel. Simply add the remote network and the local network that you want to connect as a Phase 2 entry in your IPsec tunnel. In the example below your local LAN network will be tunneled to the remote network with the public IP address 1.2.3.4 and the private IP address range of 192.168.1.0.



Failover Support

In a High Availability setup you can also include your GRE over IPsec tunnel. This keeps the tunnel open even if the secondary router takes control. First, configure your tunnel without failover support and configure your High Availability setup as described in [High Availability](#). Then take note of the virtual IP address that you assigned for the Interface your tunnel is running on.

Add the virtual IP to both your GRE tunnel and your IPsec tunnel as described in [IPsec with Failover](#) and [GRE with Failover](#). Your tunnel will now work seamlessly on all the TBF devices that are included in your High Availability setup.



18.1.7 IPsec Troubleshooting

Re-connecting problems with your IPsec tunnel can oftentimes be resolved by following these steps and retrying after each step:

- Double check your configuration on both ends of your tunnel
- Change the **Init Type** to *On Demand* instead of *Connect*
- Create a cron job under **Services** → **Cron** that pings an IP address on the other side of the tunnel every 5 minutes to keep the connection open. Use the command `ping -c 3 IP_ADDRESS &> /dev/null` to do so.

Note: parsed INFORMATIONAL_V1 request 0 [N(NO_PROP)] received NO_PROPOSAL_CHOSEN error notify

This error message usually means that the Phase 1 Encryption Parameters do not match and the other side rejected them. Please double check both sides.

Note: invalid HASH_V1 payload length, decryption failed?

This is most likely due to an incorrect PSK on one of the peers. Since the PSK is incorporated into the key material used to secure the IKEv1 packets they can't be decrypted properly if the PSKs don't match.

18.2 OpenVPN

18.2.1 OpenVPN General

OpenVPN implements virtual private network (VPN) techniques to create secure point-to-point or site-to-site connections.

Independently of the connection type you always need to run an OpenVPN server and an OpenVPN client. The device they're running on can vary however. For a site-to-site connection you'd typically have the server running on your local TBF device and the client on a remote TBF device (or other router that supports OpenVPN). The VPN tunnel would then forward all the traffic in the remote network to your local network.

Alternatively you can also create point-to-point connections. If you want to use your phone for example on the go and still have access to your local network you can open a VPN tunnel to your local network from any device as long as it supports OpenVPN. This is also helpful if you want your traffic to be routed through your local network for security reasons or to avoid certain restrictions when browsing from specific locations.

The TBF allows the creation of OpenVPN **Servers** and OpenVPN **Router Clients**.

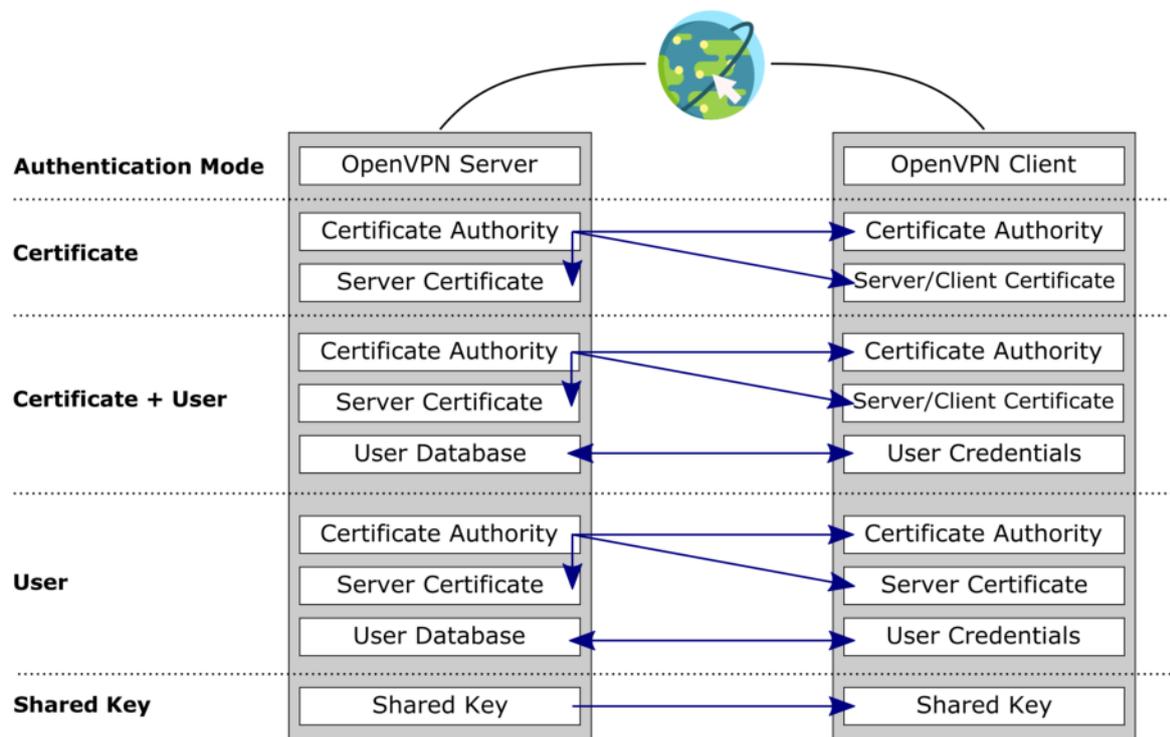
For a secure site-to-site connection, one site needs to have a OpenVPN server configured and the other one a OpenVPN router client. To get a working connection, both sites need to be configured with the same device mode, authentication mode, encryption algorithms, digest algorithms and tunnel network.

18.2.2 OpenVPN Settings

You can find the OpenVPN Settings at **VPN** → **OpenVPN**.

Prefill from File lets you prefill the fields with an OpenVPN config file.

Authentication Mode is either *Certificate*, *User* or *Shared Key*:



This image was created with icons by [Freepik](#) from [Flaticon](#).

- **For the Certificate authentication mode the OpenVPN server needs a server certificate and the OpenVPN client needs a client certificate.** Additionally you can enable the option **Additional User Auth.** to have a two factor authentication (Certificate + User). The same conditions apply to the additional user authentication then a user only authentication below.
- For the **User** authentication mode both sides need the same Certificate Authority and the client needs to add a **Username** and **Password** at the **User Authentication** setting. This user needs to exist as system user on the TBF where the OpenVPN server is running. The user also needs the **User permission** *open vpn - OpenVPN User Login* which can be assigned at **System** → **User**. Alternatively you can add the user to the Group *OpenVPN Access*. This will also give them the same user permission.
- For the **Shared Key** authentication mode both sides need a shared key. When you create the OpenVPN server the TBF can generate a shared key automatically. This shared key needs just to be copied to the OpenVPN client.

Protocol can be either UDP or TCP and whether it's only for IPv4, only for IPv6 or for both. Both IPv4 and IPv6 is multihome only, which means the interface can not be specified and only *All* can be selected.

Device Mode is either tun (Layer 3) or tap (Layer 2).

Interface can be specified or just *All* selected. If the Interface is a VRRP virtual IP of a HA Setup, only the Master holding the IP has the OpenVPN activated. The Slave will be on standby for the OpenVPN.

Local Port can be defined or if left blank, a random port will be used.

Use TLS Key allows the usage of *Transport Layer Security* and can only be used in certificate or user authentication mode. The same **TLS Key** needs to be provided for both sides. The key can be automatically generated when creating an OpenVPN server.

Encryption Algorithm can be one of many algorithms. It's also possible to select none. It has to be the same on both sides.

Enable NCP allows Negotiable Cryptographic Parameters. At **NCP Algorithm(s)** multiple algorithms can be selected. The order of the selected algorithms is respected by OpenVPN. It is only available for OpenVPN 2.4 and upwards.

Auth. Digest Algorithm can be one of a few algorithms. It has to be the same on both sides. If none is selected, TLS can not be used.

IPv4 Tunnel Network and **IPv6 Tunnel Network** define the tunnel network for the connection.

Remote Network(s) allows the usage of multiple remote networks.

Compression is the compression for the tunnel packets using the LZO algorithm and can be one of the the following:

- Omit Preference (Use OpenVPN Default)
- LZ4 Compression [`compress lz4`]
- LZ4 Compression v2 [`compress lz4-v2`]
- LZO Compression [`compress lzo`, equivalent to `comp-lzo yes` for compatibility]
- Enable Compression (stub) [`compress`]
- Omit Preference, + Disable Adaptive LZO Compression [Legacy style, `comp-noadapt`]
- Adaptive LZO Compression [Legacy style, `comp-lzo adaptive`]
- LZO Compression [Legacy style, `comp-lzo yes`]
- No LZO Compression [Legacy style, `comp-lzo no`]

Type-of-Service Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Topology specifies the method used to configure a virtual adapter IP address.

Custom Options is for custom configuration parameters for the config.

Gateways lets you choose which Gateways should be created in the System. Gateways can be used to create additional Routes or Routing Tables.

Send/Receive Buffer is the Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds.

Log Level is the log verbosity level. 0 is silent, except for fatal errors. 4 is reasonable for general usage. 5 and 6 can help to debug connection problems. 9 is extremely verbose.

Keepalive Interval is the keepalive interval in seconds and its default is 10.

Keepalive Timeout is the keepalive timeout in seconds and its default is 60.

Renegotiation specifies after how many seconds the data channel key gets renegotiated. The default is 3600. A value of 0 disables it.

You can export the settings in the top right corner as an Excel spreadsheet.

Server Only Settings

Authentication Server if you have user authentication enabled. It allows you to use a predefined authentication server from *Authentication Server* for authentication. The users do not need to be created in TBF and the control is only based on the response of the authentication server.

Radius Attributes if your authentication server is a radius server you can use the radius attributes to set client override settings. The following attributes are supported

- Framed-IP-Address
- Framed-Route

Use CRL enables the usage of the CRL of the selected Peer Certificate Authority.

Two Factor Authentication can be enabled if you use User Authentication. Only the TOTP authentication will be used, no One Time Password. Make sure that all relevant Users have the Two Factor Authentication enabled as they will not be able to login otherwise. It is NOT necessary to enable Two Factor Authentication for the webgui for this to work.

Certificate Depth defines the depth to which certificate-based client logins are accepted.

DH Parameter Length is the Diffie-Hellman parameter set used for key exchange.

ECDH Curve is the Elliptic Curve to use for key exchange.

Redirect Gateway can be enabled to force all client generated traffic through the tunnel.

Concurrent connections specifies the maximum number of clients allowed to concurrently connect to this server.

Push Compression can be enabled to push the selected Compression setting to connecting clients.

Inter-client communication can be enabled to allow communication between clients connected to this server. A Firewall Rule is still needed for this to work.

Duplicate Connection can be enabled to allow multiple concurrent connections from clients using the same Common Name.

Associate Firewall Rule can be enabled so an OpenVPN associated Firewallrule will be created and updated.

Dynamic IP can be enabled to allow connected clients to retain their connections if their IP address changes.

DNS Settings can be enabled to configure several advanced DNS options as well as four **DNS Servers**.

DNS Default Domain provides a default domain name to clients.

Block Outside DNS make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.

Register DNS kicks Windows into recognizing pushed DNS servers.

NTP Settings can be enabled to configure two **NTP Servers**.

Client Only Settings

Server host or address and **Server Port** are the IP address or hostname of the OpenVPN server and the port it's running at.

Limit outgoing bandwidth is the maximum outgoing bandwidth for this tunnel. Can be left empty for no limit. The input value has to be something between 100 bytes/sec and 100 Mbytes/sec.

Do not pull routes can be enabled to bar the server from adding routes to the client's routing table.

Do not add/remove routes can be enabled to not add or remove routes automatically.

Proxy host or address is the address for an HTTP Proxy this client can use to connect to a remote server.

Proxy Port is the port of the proxy and its default is 1080.

Proxy Authentication can be enabled to use a **Username** and/or **Password**.

Example Configurations

Site-to-Site connections

To obtain a stable OpenVPN connection between two or more physically separated sites you need to run an OpenVPN server and the associated clients. This chapter shows you how to configure a basic OpenVPN site-to-site connection on your TBF device.

In case you haven't created a Certificate Authority yet go to **General** → **Certificates** → **CAs** and click **Add**.

Fill in all the information (**Common Name** specifies your companies URL) and select a **Key Size** and an **Algorithm**. Double check with your client devices that they support the selected key lengths and algorithms since some large values are not supported on all devices. For a connection between two TBF devices this is not a problem.

Click **Save** to create your Certificate Authority.

© Voleatech GmbH 2017 - 2020

Next, go to **General** → **Certificates** → **Certificates** and click **Add**. Create a Server Certificate for your OpenVPN server by selecting your new Certificate Authority and Server as the **Type**.

© Voleatech GmbH 2017 - 2020

Go to **VPN** → **OpenVPN** and click **Add**.

Select a **Name** and an **Authentication Mode** (see description above). This example uses the Certificate + User Authentication Mode. For some authentication modes you're given the choice to make your connection a peer-to-peer connection that only allows one client. In a site-to-site connection with only one remote location this should be enabled.

Under **Protocol** you can select the protocol that is being used. Typically UDP is used for OpenVPN as it's faster and more reliable. If you need an IPv6 connection you can select it here. In most cases IPv4 is sufficient.

Under **Device Mode** you're given the choice between tun and tap. Tun is more widely used, compatible with mobile client such as iOS and Android and more stable than tap mode.

The **Interface** of your server would typically be WAN or Multihome in a site-to-site setup that communicates over the internet. The **Port** can be left on it's default value except if that port is already in use on

your network.

The screenshot shows the 'VPN / OpenVPN / Create Server' configuration page. The left sidebar contains a navigation menu with options: Dashboard, System, Authentication, General, Interfaces, Firewall, Routing, Apps, Services, VPN, IPSec, OpenVPN, WebVPN, WireGuard, Tools, and Diagnostics. The main content area is titled 'General' and includes the following settings:

- Prefill from File:
- Enabled:
- Name:
- Description:
- Authentication Mode: Certificate
- Protocol: UDP (IPv4 only)
- Device Mode: tun (Layer 3)
- Interface: All
- Local Port: 1194

Under Certificate select your Certificate Authority and the newly created OpenVPN Server Certificate. Leave **Certificate Depth** at one for a basic setup like this. If you want your server to be aware of revoked certificates in the future then enable the **Use CRL** option. This helps with keeping your VPN connection safe even if a certificate gets stolen and needs to be replaced in the future you can revoke them in the *Certificate Manager*.

Since this setup uses the Certificate + User Authentication Mode enable **User Authentication**.

The screenshot shows the 'Certificate' and 'User Authentication' configuration pages in the Voleatech interface. The top navigation bar includes the Voleatech logo, a search bar, and a user profile 'admin admin'. The left sidebar is the same as in the previous screenshot. The main content area is divided into three sections:

- Certificate**:
 - Certificate Authority: OpenVPN CA
 - Use CRL:
 - Server Certificate: OpenVPN Server Cert (Server)
 - Certificate Depth: One (Client + Server)
- User Authentication**:
 - Additional User Auth.:
- TLS**:
 - Use TLS Key:
 - Auto. TLS Key generation:

© Voleatech GmbH 2017 - 2020

For the cryptography settings pay special attention to your client device's capabilities again. Some may not support all key lengths or cryptographic algorithms. If you enable NCP you can specify that your OpenVPN server can negotiate alternate algorithms with the client in case the primary algorithm is not supported.

The screenshot shows the 'Cryptography' configuration page in the Voleatech interface. The settings are as follows:

- DH Parameter Length: 4096 bit
- ECDH Curve: Default
- Encryption Algorithm: AES-256-CBC (256 bit key, 128 bit block)
- Enable NCP:
- NCP Algorithm(s): AES-256-GCM (256 bit key, 128 bit block)
- Auth. Digest Algorithm: SHA512 (512-bit)

The address and address range you define under **Tunnel Network** are the addresses assigned to the VPN clients. Choose an address range that is unused by the rest of your local network. If you have only a single client connected to your VPN choose single IP address (range 30). The maximum number of concurrent connections is therefore set to one.

If you wish to force all traffic through your VPN tunnel enable the **Redirect Gateway** option. This forces all traffic through the tunnel no matter its destination. If you leave this disabled only relevant traffic that has a destination on the other side of the tunnel will be forwarded through your VPN.

Under **Remote Network** you can specify the local networks that can be accessed via the VPN connection. When creating a multi-site network that is supposed to work as if it was one common local network you'd enter your local network addresses here.

If you enable compression for your tunnel you will save on bandwidth at the cost of an increased amount of needed processing power. For high speed connections this can lead to additional latency though. Refer to the description above for details on compression modes. Via the **Push Compression** option you can force your clients to use the compression you specify here instead of their own configuration.

Inter-Client communication stays off in this example since the number of clients is limited to one and therefore there is no other client to communicate with.

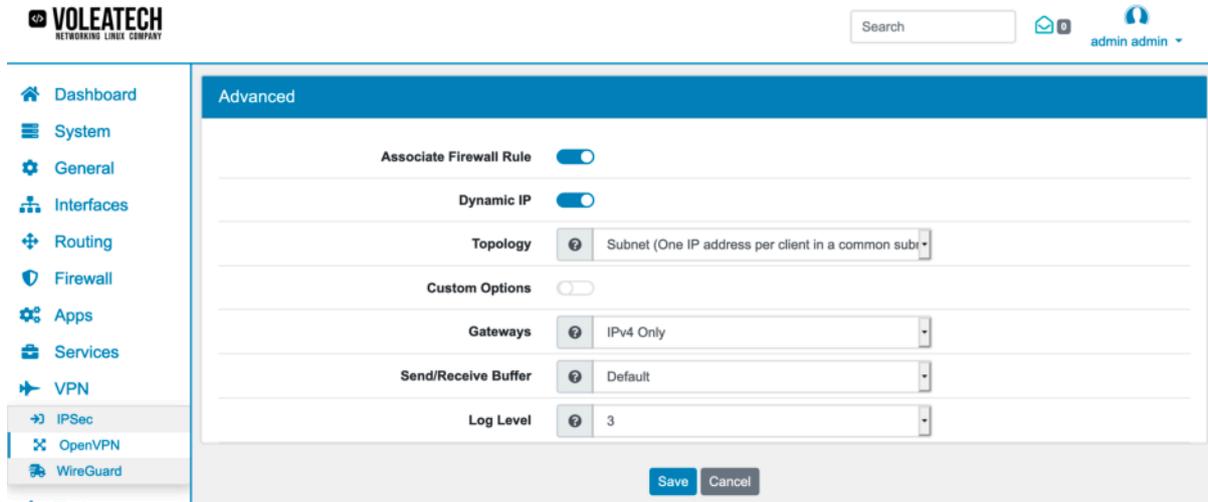
The screenshot shows the 'Tunnel' configuration page in the Voleatech interface. The settings are as follows:

- IPv4 Tunnel Network: 192.168.100.0 / 30
- IPv6 Tunnel Network: IPv6 Tunnel Network / 64
- Redirect Gateway:
- Remote Network(s): 192.168.1.0 / 24
- Concurrent connections: 1
- Compression: Omit Preference (Use OpenVPN Default)
- Push Compression:
- Type-of-Service:
- Inter-client communication:

Should your clients operate on a dynamic IP address you can enable the **Dynamic IP** option to retain the connection even when the IP address of a client changes. Otherwise the client would need to re-login every time the IP address changes.

Under **Topology** you can choose if your server creates a new subnet with only one IP address per client or a common subnet for all clients. Since this configuration has only one client this setting is basically

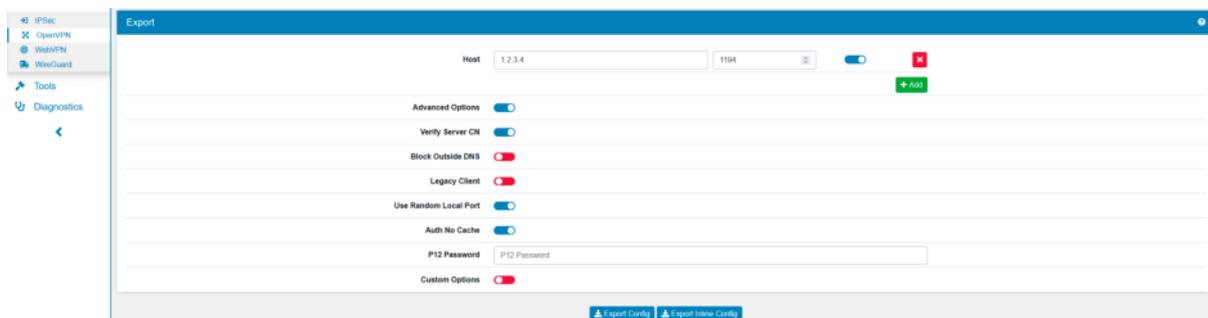
irrelevant. Under **Gateways** you can choose whether you want to create Gateways for both IPv4 and IPv6 or just one of them. In this IPv4 only configuration set this to IPv4.



Click **Save** to create your OpenVPN Server.

On the client device(s) you can either go to **VPN** → **OpenVPN** → **Router Clients** and click **Add** to manually enter your server's settings.

To export your settings go back to your server device and go to **VPN** → **OpenVPN** → **Servers** click the **Edit** button of the server you wish to connect your client to and scroll all the way to the bottom. Under **Export** you'll find a field **Hostname/IP address** where you enter the address of your OpenVPN server and the port you chose for it. Click **Export** and save the file. Unzip the file you just downloaded.



When you click on **Advanced Options** the following options will show:

Verify Server CN optionally verifies the server certificate Common Name (CN) when the client connects.

Block Outside DNS blocks access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.

Legacy Client does not include OpenVPN 2.5 settings in the client configuration.

Use Random Local Port uses a random local source port (lport) for traffic from the client. Without this set, two clients may not run concurrently.

Auth No Cache lets username and password inputs immediately forgotten after they are used.

P12 Password is the password for the P12 file.

Custom Options are custom configuration parameters for the config.

OpenVPN Firewall Rules

Note: You need to create Firewall Rules on the newly create OpenVPN_XXX Interface, in order to allow network traffic from the clients. Please have a look at [Firewall Rules \(Forward and Input\)](#) for a detailed explanation on how to create Firewall Rules for an interface.

18.2.3 OpenVPN Export

Once an OpenVPN server is created and saved it's possible to export OpenVPN client configs. Besides the default export, it's also possible to export the config in an inline format. This functionality can be found at the bottom of the page when when an OpenVPN server is edited. Several configurations are available:

Host allows the setup of multiple hosts with their hostname or IP address and port.

Advanced Options shows more specific configurations.

Verify Server CN will optionally verify the server certificate Common Name (CN) when the client connects.

Block Outside DNS will block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.

Legacy Client will not include OpenVPN 2.5 settings in the client configuration.

Use Random Local Port enables the usage of a random local source port (lport) for traffic from the client. Without this set, two clients may not run concurrently.

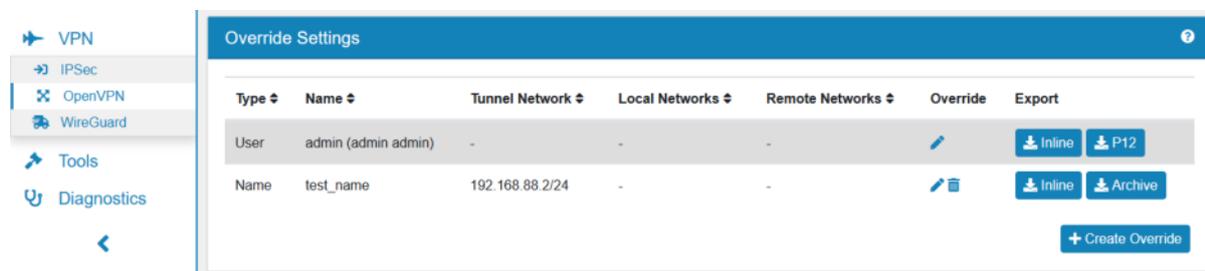
P12 Password a password to encrypt the config in the P12 format.

Custom Options is for custom configuration parameters for the config.

If the authentication mode is **Certificate** it's possible to export the client config for each certificate. This functionality can be found below the default export. Those exports are available either in the **Inline** or **P12** format. For each certificate an [OpenVPN Override](#) can be configured.

18.2.4 OpenVPN Override

The **OpenVPN Override** is available for the authentication mode *Certificate* and *User*. This functionality can be found at the bottom of the screen once a OpenVPN server has been created and saved. A separate override for each certificate and user can be configured, as well as a custom one.



The following options can be used:

Enabled determines whether this override shall be used or not.

IPv4 Tunnel Network and **IPv6 Tunnel Network** define the tunnel network for the connection.

Block Connection blocks this client connection based on its certificate common name.

Redirect Gateway can be enabled to force all client generated traffic through the tunnel.

Local Network(s) allows the usage of multiple local networks.

Remote Network(s) allows the usage of multiple remote networks.

Custom Options is for custom configuration parameters for the config.

Multiple Clients with separate Networks

If you want to use an OpenVPN setup for multiple clients where each uses its own separate network, you can use the override to accomplish this. All networks for all clients have to be configured in the OpenVPN server settings at *Remote Network(s)*. Then each client needs to use the override to set their specific network at *Remote Network(s)*.

18.3 WireGuard

WireGuard implements virtual private network (VPN) techniques to create secure point-to-point or site-to-site connections.

WireGuard uses state-of-the-art cryptography, like the Noise protocol framework, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF, and secure trusted constructions. It makes conservative and reasonable choices and has been reviewed by cryptographers.

It also aims at having a better performance and a lower power consumption than IPsec and OpenVPN have while being easier to set up.

18.3.1 Settings

Port each WireGuard connection needs a unique port.

Private Key is the private key of the TBF. Never give it to another party.

Public Key is the public key of the TBF and must be given to the remote peer.

Tunnel IP is the local IP Address of the WireGuard connection and the netmask must be set to the entire network. The Tunnel IP can be IPv4 and/or IPv6.

DNS Server can be an IP Address of a DNS Server.

MTU is the Maximum Transmission Unit and 1420 by default. If you have a PPPoE connection you need to set it to 1412.

Associate Firewall Rule can be enabled so an OpenVPN associated Firewallrule will be created and updated.

Routing Table can be changed and uses the *Main* routing table by default. The peer remote networks will be added to this routing table.

Master Only Only start WireGuard if the TBF is the network master in a HA setup.

Additional Tunnel IPs are additional IP addresses on the local server or peers.

You can export the settings in the top right corner as an Excel spreadsheet.

18.3.2 Export Settings

The export settings will set basic options for peer exports.

Enter the hostname where the WireGuard server is accessible over the internet to your Peers. It can be a hostname or IP Address.

The **Local Network(s)** are all networks that should be accessible from the peer. Usually you enter the networks behind the WireGuards server the Peer should access.

Note: If you want to enable Peer to Peer communication, also Enter the **IPv4 Tunnel Network** to the **Local Network(s)** All Local Network(s) are added to the Additional IPs configuration setting.

18.3.3 Peer

A Peer is a remote device and it can be a site or a client. There is no difference, every remote endpoint is a peer.

Keep Alive can be sent every few seconds to make sure that the connection is up.

Private Key is the private key of the Peer and not required for the connection. You have the option to generate a Key Pair here if your Peer can not do so. In that case it will be shown here.

Public Key is the public key of the Peer and required for the connection.

Preshared Key is optional and can be added as a secondary authentication.

Tunnel IP is the remote IP Address of the WireGuard connection. The Tunnel IP can be IPv4 and/or IPv6 and must be in the Settings Tunnel IP Range.

Endpoint Address can be an IP or Hostname of the Peer.

Endpoint Port is the remote port of the Peer.

Remote Networks are networks that are reachable behind that peer.

Additional Tunnel IPs are additional IP addresses on the local server or peers.

18.3.4 Export

If you created a peer you can export the peer config. You can find the export at the quick edit at the bottom of the corresponding wireguard edit page.

18.3.5 QR Code

Once a peer is created a QR code is available. It contains the peer config. You can find it at the quick edit at the bottom of the corresponding wireguard edit page.

18.3.6 Import Config

Instead of creating a new WireGuard you can import settings from an existing WireGuard config. You can find the **Import Config** button at the bottom right corner of the WireGuard management page. The TBF will create the data structure and try to import almost all settings from the config.

18.3.7 Example WireGuard Configuration

Go to **VPN** → **WireGuard** and click **Add**. The address and address range you define under **Tunnel Network** are the addresses assigned to the VPN clients. Choose an address range that is unused by the rest of your local network. If you have only a single client connected to your VPN choose single IP address (range 30).

When creating peers (clients) pay special attention that in WireGuard it is only possible to have as many peers as you have manually configured since every peer is assigned a unique static Tunnel IP address. You also cannot log in with the same peer multiple times concurrently.

Click **Add** to create a new peer. Enter an **Tunnel IP address** that is not used by any other peer and within the range that you specified in your server's configuration. You can also specify additional Tunnel IP addresses under **Additional Tunnel IPs**.

Auto PSK Generation automatically creates a secure Pre-Shared Key that your peer can use for connecting. The PSK is optional and gives a second layer of authentication besides the key.

If you choose **Endpoint Type Static** you can specify your server's public IP address and the port that you entered in your WireGuard configuration. Under **Remote Networks** you can specify which local networks are available behind the peer. The remote networks will then be reachable from the server. If you do not want to access any network behind the peer, leave the **Remote Networks** empty.

The **Local Network(s)** in the peer can be used to have specific Networks that should be reachable only for this Peer. They are in addition to the global **Local Network(s)**.

Click **Save** to save the peer and after creating all the peers click **Save** again to save the whole configuration.

Export the peer configuration via the **Export** panel above the **Save** button.

You can also click **Add Multiple** to easily create multiple peers at once. You only need to provide the peer name, the IP Address will be filled automatically if you do not enter one.

WireGuard Peers	Name	IPv4	IPv6
	WG1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	WG2	<input type="checkbox"/>	<input type="checkbox"/>

Note: You need to create Firewall Rules on the new Wireguard_XXX Interface in order to allow network traffic from the peers. Please have a look at [Firewall Rules \(Forward and Input\)](#) for a detailed explanation on how to create Firewall Rules for an interface.

18.4 WebVPN

WebVPN uses *Apache Guacamole* and is a clientless web remote desktop gateway.

You can find the WebVPN Settings at **VPN** → **WebVPN**.

Before you can use the WebVPN it has to be installed. You can install it at **System** → **Addons**.

18.4.1 WebVPN Settings

Enabled is false by default.

Hostname is TBF by default.

Web HTTPS Port is 443 by default.

Certificate can be configured which certificate will be used for the WebVPN Page.

2FA Enable Two Factor Authentication if the user has a TOTP Token enabled in TBF. If a user has not TOTP Token the 2FA won't be enforced for them.

Logo is a file that can be uploaded and has to be in the PNG format. Users will see it on the WebVPN Page.

You can export the settings in the top right corner as an Excel spreadsheet.

You also need to make sure to add a Firewall Rule to allow access to the TBF on that Port. The Web-server is listening to the hostname for connections. The WebVPN is using HTTPS and a WebGUI to connect to all Servers.

18.4.2 WebVPN Server Settings

To connect to a Server via the WebVPN you need to create it and assign to users.

Type can be RDP, SSH, Telnet or VNC. It is RDP by default.

Name can be configured and has to be unique.

Description is a description of the server.

Hostname has to be an IP Address or hostname of a server in your network that should be accessible through the WebVPN.

Port defaults to 3389 for RDP, 5900 for VNC, 22 for SSH and 23 for Telnet.

Username is optional. It will be asked on connection time if not set.

Password is the password for the username and is also optional. It will be asked on connection time if not set.

Domain is the domain to use when attempting authentication (RDP only).

Security can be Any, NLA, Extended NLA, TLS, VM Connect or RDP. It is Any by default.

Keyboard Layout is the default keyboard layout and is English (US) by default (RDP only).

Keepalive Interval allows you to configure the the interval in seconds at which the client connection sends keepalive packets to the server. The default is 0, which disables sending the packets. The minimum value is 2.

The screenshot shows the 'WebVPN Server' configuration page. At the top, there is a breadcrumb 'VPN / WebVPN / Update' and a help icon. The page title is 'WebVPN Server'. The configuration is as follows:

- Enabled:** A toggle switch is turned on.
- Type:** A dropdown menu is set to 'SSH'.
- Name:** A text input field contains 'Test'.
- Description:** A text input field contains 'Test'.
- Hostname:** A text input field contains '192.168.10.1'.
- Port:** A text input field contains '22'.
- Username:** A text input field contains 'root'.
- Password:** A text input field contains 'Password'.
- Keepalive Interval:** A text input field contains '0'.

At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

18.4.3 WebVPN User Settings

A WebVPN User connects a TBF user to a WebVPN server. Each user can have multiple servers. This is required for authentication.

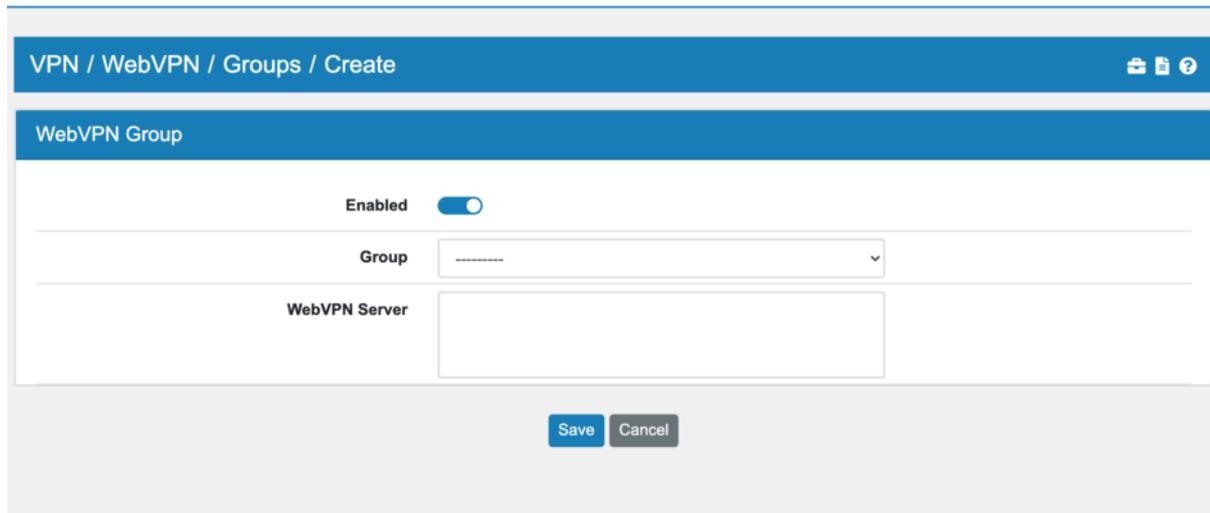
The screenshot shows the 'WebVPN User' configuration page. At the top, there is a breadcrumb 'VPN / WebVPN / Update' and a help icon. The page title is 'WebVPN User'. The configuration is as follows:

- Enabled:** A toggle switch is turned on.
- User:** A dropdown menu is set to 'admin'.
- WebVPN Server:** A list box contains 'Test' and 'Test2'.

At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

18.4.4 WebVPN Group Settings

A WebVPN Group connects a TBF user to a WebVPN server. Each group can have multiple servers. In case a user is already connected to a server via the WebVPN user settings, the config will be merged together.



The screenshot shows a web interface for creating a WebVPN Group. The breadcrumb trail at the top reads "VPN / WebVPN / Groups / Create". The page title is "WebVPN Group". The configuration includes:

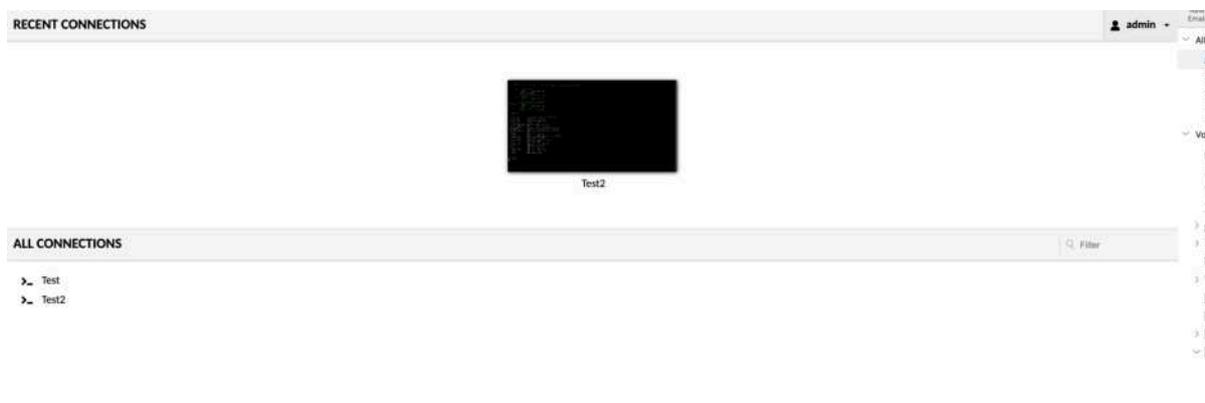
- An "Enabled" toggle switch, which is currently turned on.
- A "Group" dropdown menu with a placeholder "-----".
- A "WebVPN Server" text input field.
- "Save" and "Cancel" buttons at the bottom.

18.4.5 WebVPN Usage

When you connect to the WebVPN you first need to login with the Users credential that was set in WebVPN. A User is either from TBF or an LDAP Authentication Server.



After the login you can see all available Servers for this User.



If you select one of the servers, your browser will connect to it and you can login and interact with the server through the browser.

```
← → ↻ ⚠ Not Secure | 192.168.10.103:444/guacamole/#/client/VGVzdDIAWwB2dGFpci1hdXRo
📱 Apps 🌟 Bookmarks 🍏 Apple 🇩🇪 Heute 📺 Spiegel 🌐 Tom's Hardware

VT AIR
Model: RCC-VE - Serial: 1112161106 - Device ID: 1f4b049c1a07be3a6e834600cebffbcc

WAN: enp0s20f0(WAN)
speed = 1000MB, up = yes
192.168.10.112/24
fe80::208:a2ff:fe0a:8855/64
LAN: enp0s20f1(LAN)
speed = 1000MB, up = yes
192.168.1.1/24
fe80::208:a2ff:fe0a:8856/64
AppBridge: brapp (APPBRIDGE)
speed = 0MB, up = yes
172.30.0.1/24
fe80::42:ceff:feal:7b61/64

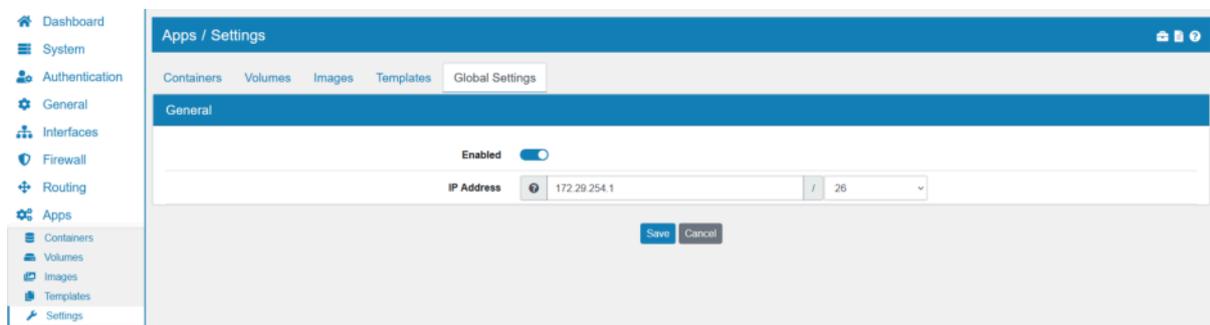
Commands

allowallwan Allow all Firewall Rule for WAN
assignlan Assign LAN Interface
assignwan Assign WAN Interface
check-service Check service
default-gateway Assign Default Gateway
factory-defaults Reset to factory defaults
interfaceip Assign IPs or DHCP to an Interface
interfaces-all Show all interfaces in the system
licence Add Licence
reboot Reboot the system
reset-admin Reset the admin password to default
restart-webgui Restart the webgui
route-check Force a Route Service Check
shell Open up a shell
showservices Show all active services
shutdown Shutdown the system
ssh Enable or Disable SSH
unlock-user Unlock a blocked user
update Update from vtair terminal
vtair-cli Open up the cli

(vtair)# █
```

19.1 Settings

You can find the App Settings at **System** → **Apps** → **Settings**.



You can change the default docker bridge settings here, please use a network that you don't need and that does not conflict with your setup. It is not relevant for the apps but needs to be created in the system for apps to work.

Backup will create a nightly backup of all docker container and volumes. It keeps the last 3 backups at /opt/docker_backups. Please be aware of the space requirements and if the hard drive has enough space for this. You can also run manual backups with the docker-backup.sh command in the shell.

19.1.1 Apps Overview

We are utilizing Docker as an App Container Framework. Apps have different building blocks. The most important are:

- Images
- Volumes
- Container

Images are blueprints for Containers. Each container uses a copy of the Image to run. An image can be an operating system like Debian or a programm like Java.

Volumes are folders or files that are mounted inside a container. Otherwise any data will be deleted when the Container is deleted.

Containers are the running environment for the apps. Each Container loads an Image and mounts the selected Volumes in a selected location. You can also specify hardware limitations, mount devices and enable networking. It runs in a sandboxed environment and can not access the host's data.

19.1.2 Networking

Due to the way Docker configures the network, there are 2 bridges in the system:

- docker0
- brapp

The **docker0** is the default docker bridge and **NOT** used by TBF. It needs to exist in the system though.

The **brapp** is the network bridge all containers are connected to.

19.2 Images

You can find the App Images at **System** → **Apps** → **Images**.

You can either upload an image that you have or search for an image in the Docker Registry. The Docker Registry has a lot of prepared images you can use.

Please visit the Docker Hub website to browse available Images [Dockerhub](#).

If the TBF has a working internet connection you can enter a search word and it will show you any docker image that matches the word. You can select it and it will be downloaded for use in a Container.

19.3 Volumes

You can find the App Volumes at **System** → **Apps** → **Volumes**.

A Volume is a directory on the TBF hard drive.

All Volumes are created at `/var/lib/docker/volumes/NAME/_data` on the hard drive.

19.4 Containers

You can find the App Containers at **System** → **Apps** → **Containers**.

A Container is the actual App. On the overview page you can see all Containers in the system and if they are running or not. If a container is running it will display an info icon in the first column. When hovering over this icon with the mouse, it will display all used ports by the container. For more container details, you can hover over and click the information icon in the second column.

You can get the logoutput of the container or connect to the containers screen if it is running. You can also start, stop, restart, delete or edit a container.

Be aware that most container settings can not be changed after creating it. You must delete and recreate the container.

19.4.1 Container Options

Name so you can identify the container.

Image that the container should be based on.

Start if you want it to start right away after creation.

CPUs you can limit the container to a certain number of CPUs if you like.

RAM Limit to limit the amount of memory.

Restart Policy if the app should start automatically.

Auto Remove if the app should be deleted when it finishes running.

Hostname if you want to set a custom hostname inside the container.

Interactive is necessary for containers that need user input and output. For example if you start debian as a container you want to enable this option.

Command if the container can execute commands at startup. For debian it would be good to start `/bin/bash` here.

Temporary FS if you want to mount a RAM Filesystem inside the container.

Networking can be enabled or disabled.

IP and MAC you can set a custom MAC address here as well as IP Addresses. If not set one will be allocated for you. IP Addresses can only be in the Bridge App range.

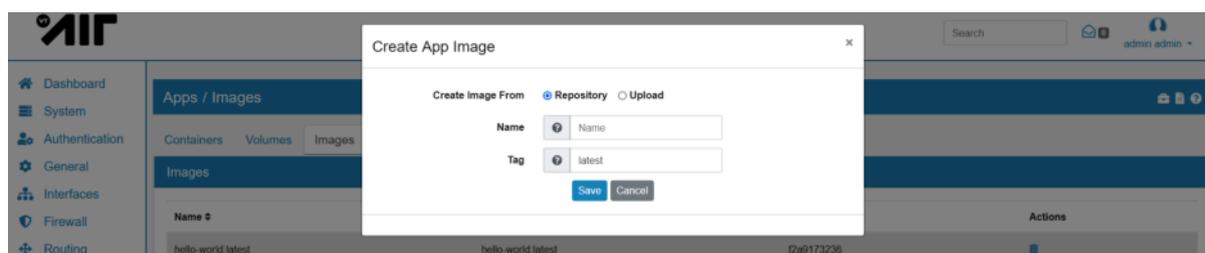
Environment Variables can be created here. Each environment variable consists of a key and value pair.

Volumes that you created can be mounted inside the container here. Enter the path inside the App/Container where it should be mounted to and if it is read/write.

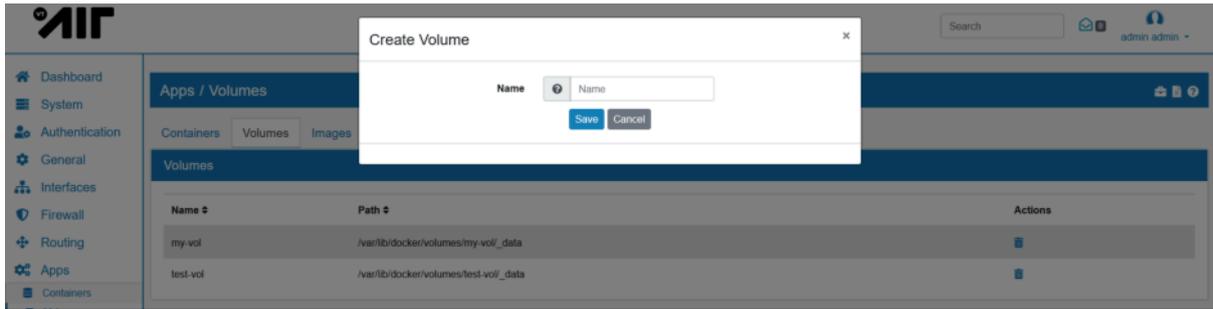
Devices if you want to add a device like a USB connector to the container.

19.5 Running a new Application

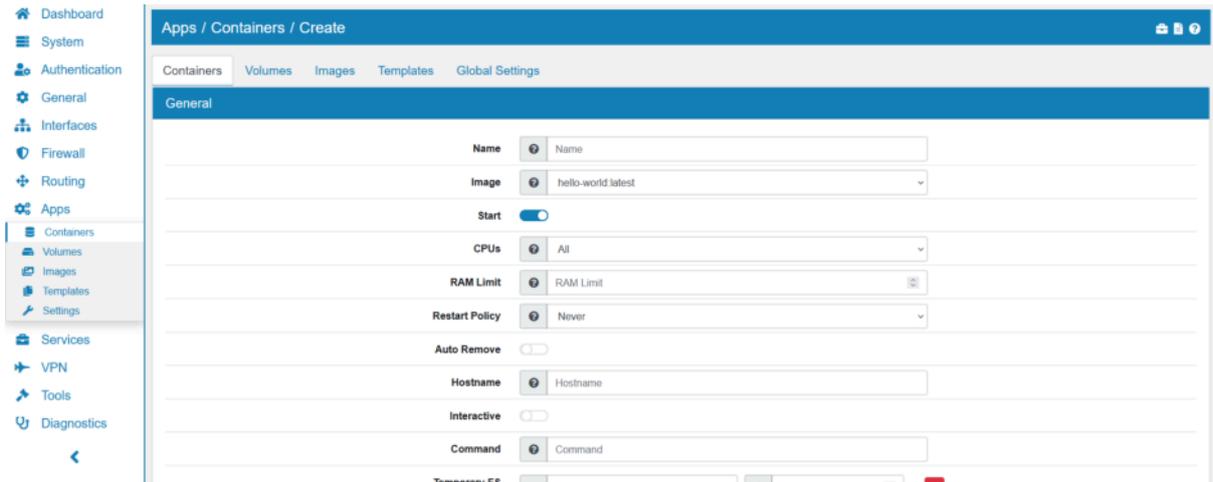
To create and run a new application you should follow these steps. First, load a new Image that either contains the operating system your app will run on or the app itself (refer to [Images](#) for more details).



If you require an external folder in your app, create a volume that you want to store your data on (refer to [Volumes](#) for more details). For most images this is not required or the image creates an external folder automatically.

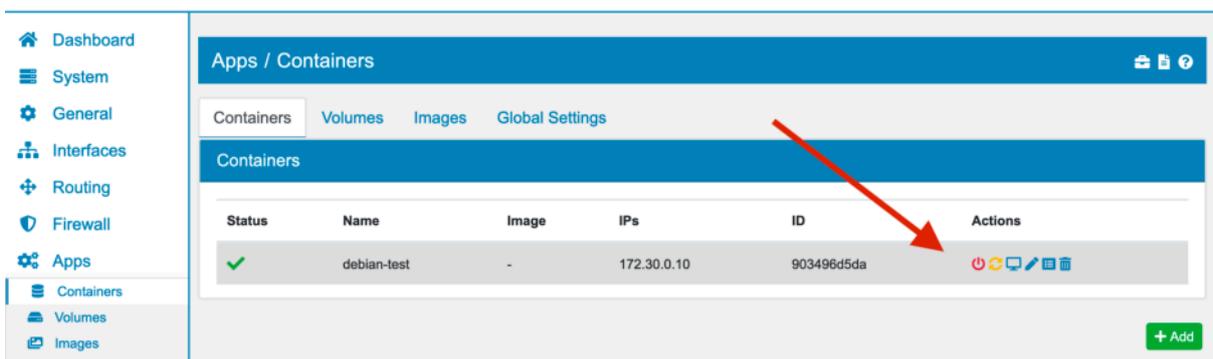


When creating a new Container you're given a few configuration options (refer to [Containers](#) for more details).



If you wish to enable the network connection for your Container you need to activate the network connection in its settings. If you leave the IP address field empty, it will be auto-assigned within the AppBridge **brapp**. The default Firewall rule allows access to all local and non-local networks on the AppBridge. However incoming traffic is blocked by default. If you wish to enable port-forwarding for example refer to [Firewall Rules \(Forward and Input\)](#) for more details.

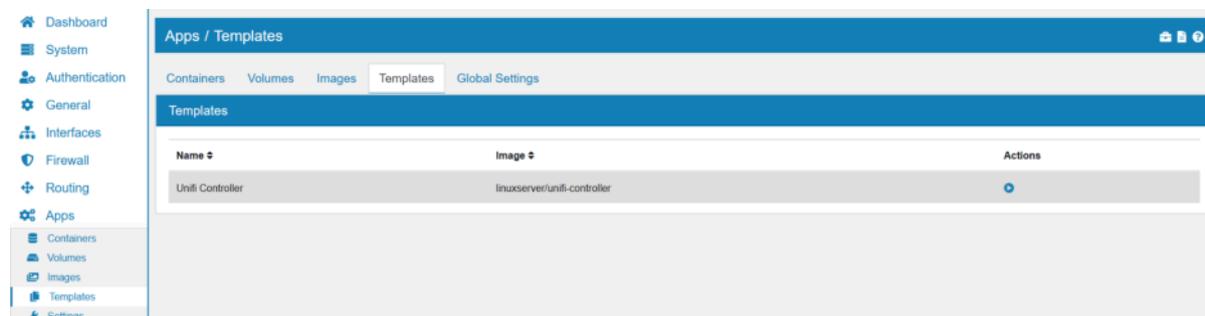
To access your newly created app, you need to run the Container. Click the play button to do so. You should now see a new stop and reload option as well as an option to start the console of your Container.



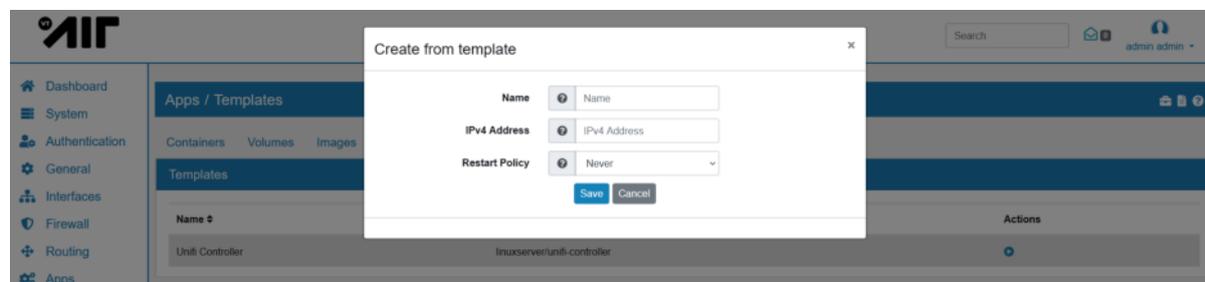
19.6 Templates

You can find the App Templates at **System** → **Apps** → **Templates**.

Templates are a convenient shortcut of creating a container and downloading the image.



On the overview page you can see all currently available templates. In the Actions column you can create and start a Container directly from a template.



When creating a Container from a template, you have to configure **Name**, **IPv4 Address** and **Restart Policy**.

19.7 Examples

19.7.1 UniFi Controller

If you want to install the UniFi Controller software on your TBF device you can do so via the Apps feature. Go to **System** → **Apps** → **Images** and click **Add**.

There is multiple images for the UniFi controller software available e.g. the image `jacobalberty/unifi`. Click **Save** and wait for the image to be installed. You do not need to create a volume for the UniFi Controller image since it automatically creates its own volume. Create a container based on your image. You do not need to activate **Interactive Mode**.

To access your UniFi controller go to <http://IP-ADDRESS:8080/> or <https://IP-ADDRESS:8443/> with the IP-ADDRESS being the one displayed in your Container overview panel.

The screenshot shows the Voleatech dashboard with the 'Apps / Containers' section. The 'Containers' tab is selected, and a table lists the installed containers. A red arrow points to the IP address '172.30.0.2' of the 'UniFI-Controller' container.

Status	Name	Image	IPs	ID	Actions
✓	UniFI-Controller	jacobalberty/unifi:latest	172.30.0.2	a452844a7e	🔌 🔄 🖨️ 🗑️

19.7.2 Debian

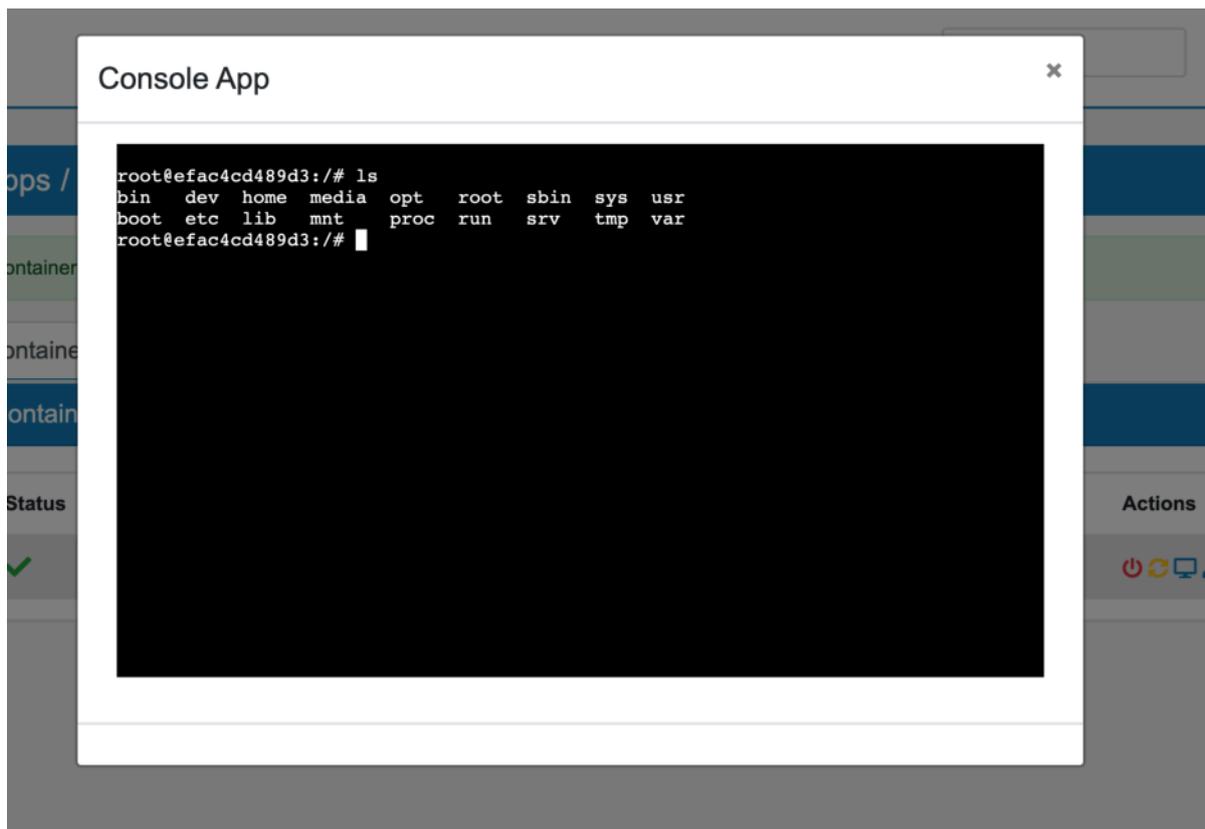
If you want to install the Debian Container on your TBF device you can do so via the Apps feature. Go to **System** → **Apps** → **Images** and click **Add**.

There is usually only the main Debian Image. Select it and click **Save** and wait for the image to be installed. You do not need to create a volume for the Debian image since it does not need a volume. Create a container based on your image. You do need to activate **Interactive Mode** and set the command to **/bin/bash**.

The screenshot shows the Voleatech dashboard with the 'Apps / Containers' section. The 'Containers' tab is selected, and a table lists the installed containers. The 'Debian' container is shown with IP address 172.30.0.2.

Status	Name	Image	IPs	ID	Actions
✓	Debian	debian:latest	172.30.0.2	efac4cd489	🔌 🔄 🖨️ 🗑️

In interactive mode you can also access the console of the Debian Image by clicking on the console icon.



19.7.3 MySQL

If you want to install the MySQL Container on your TBF device it is best to use the console so you can also pass along a default user, database and password. A MySQL container can be useful to store permanent data of the addon NtoPNG for example. The following command will create a MySQL container with user, password and database *ntopng*:

Note: `docker run --network brapp --name mysql-ntopng -e MYSQL_ROOT_PASSWORD=mysqlroot -e MYSQL_DATABASE=ntopng -e MYSQL_USER=ntopng -e MYSQL_PASSWORD=ntopng -d mysql:5.7-debian`

The container can be viewed and managed in the Webinterface afterwards.

HIGH AVAILABILITY

20.1 General High Availability

High Availability in TBF is composed of three different and *independent* settings:

- Configuration Synchronization
- States Synchronization
- VRRP Virtual IPs

Each of these settings can be enabled independent of each other and they do not influence the other settings. A complete HA setup though, only makes sense when all three parts are activated.

The High Availability Synchronization will only start, if both devices have the same TBF version running.

A High Availability Wizard is available for an easy onboarding of the secondary firewall.

20.1.1 Interface setup

The interfaces will only be synced if the two devices have the same TBF model. If that's not the case there is an interface requirement before you start the High Availability setup. Since two devices do not need to be the same make and model, you have to configure the interfaces individually first.

The synchronizations depend on stable internal interface names (WAN, LAN, INT1, INT2,). These names have to match on both ends of a sync master and client. The INTX numbers are set automatically by the system in the background and can be seen in **Interfaces** → **Assign** or on each interface settings page on the upper left corner.

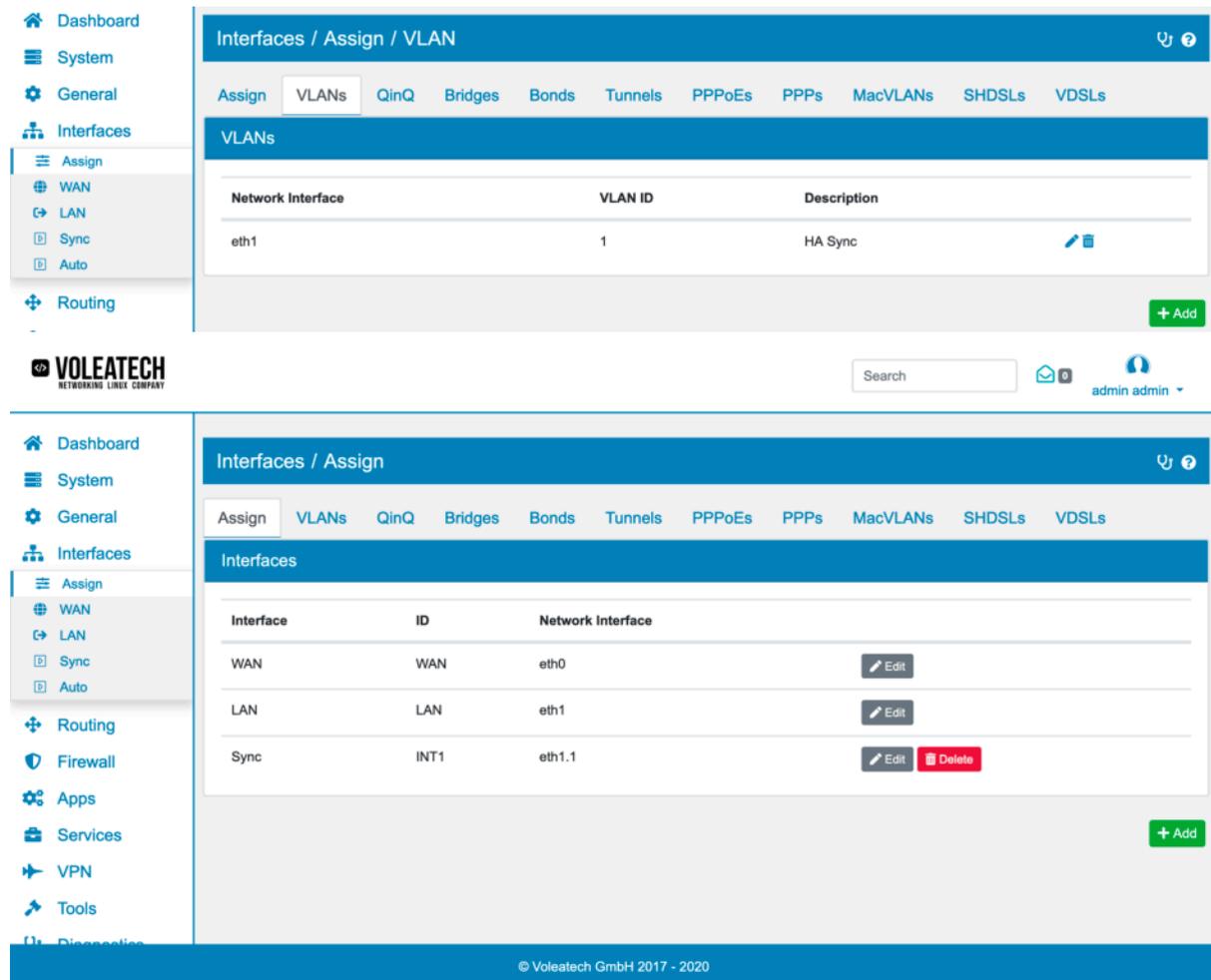
Please make sure to have the same amount of interfaces and that the names match up on both ends. Also make sure that the Interfaces IPs are different and do not conflict.

If you do not have the same amount of interfaces, please create dummy interfaces on the secondary firewall with hardware interface none. The interface can stay disabled.

20.1.2 Synchronization Interface

It is highly recommended to use a Synchronization Interface for all sync activities. The data are partially unencrypted and it is important that they arrive on each box in a timely and safe manner.

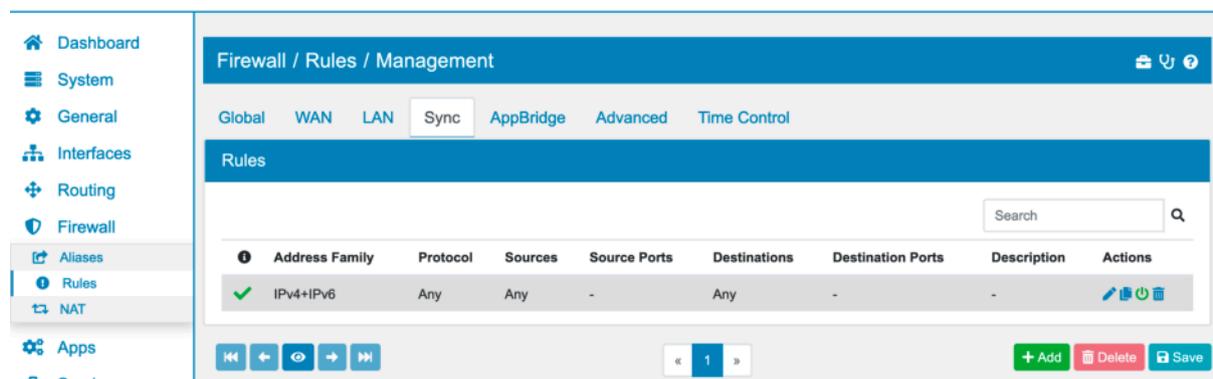
Use either a separate VLAN or a separate physical Interface.



Give all TBF a static IP Address in this network and do not enable the DHCP Server.



Make sure that there is a Firewall Rule to allow all Traffic to the Interface IP Address on the Sync Interface on each TBF.



Set the same password for the hasync user on each TBF.

Mode is *Multicast* by default. It allows for multiple Firewalls to exchange state information. If you have a

special requirement, you can change the mode to *Unicast* and send state information to one peer only. Please define the peer IP Address. This setting needs to be set on both `|prodname|s`.

20.1.3 VRRP Mode

The VRRP mode is Multicast by default. The exchange of VRRP state information is done on each Interface a VRRP IP is defined via Multicast. This also makes sure that a Layer 2 check is performed.

In certain cloud or virtual environments, there might not be a Layer 2 Multicast connection between firewalls. In that case, set the *Mode* to *Unicast* and a new option will show to also change the VRRP mode from *Multicast* to *Unicast*.

The *Unicast* mode will send **all** VRRP information on the Sync Interface to the Peer IP Address and not information on the interfaces the VRRP IP is defined. The Layer 2 check on each interface is also lost in this scenario.

System / High Availability

Firewall State Sync

States Sync	<input type="checkbox"/>
Syncinterface	<input type="text" value="WAN"/>
Mode	<input type="text" value="Unicast"/>
Peer	<input type="text" value="192.168.10.110"/>

VRRP

VRRP Mode	<input type="text" value="Unicast (Sync Interface)"/>
------------------	---

20.1.4 High Availability Nodes

There is no limit to the amount of nodes you can add to the HA setup. You can daisy chain nodes in TBF, you only need to have the *Configuration Sync* enabled on each node that should sync to the next one.

Some systems like DHCP do not support to have more than three members though.

20.1.5 Secondary Firewall

The secondary firewall will show a red sign in the upper right corner.



Note: Please do not make any configuration changes to the secondary firewall as they will be overridden by the master.

20.1.6 Onboarding Wizard

The master firewall will show an onboarding wizard on the first time you click on *High Availability* in the menu.

The screenshot shows the HASync Wizard configuration window. It includes the following fields and controls:

- States Sync:** A blue toggle switch that is turned on.
- DHCP HA:** A blue toggle switch that is turned on.
- Configuration Sync:** A blue toggle switch that is turned on.
- Sync Interface:** A dropdown menu with a question mark icon on the left and a downward arrow on the right, currently displaying 'LAN'.
- Remote Webgui:** A text input field with a question mark icon on the left, containing the text 'Remote Webgui'.
- Admin Username:** A text input field with a question mark icon on the left, containing the text 'Admin Username'.
- Password:** A text input field with a question mark icon on the left and an eye icon on the right, containing the text 'Password'.
- Buttons:** Two buttons at the bottom: a blue 'Save' button and a grey 'Cancel' button.

You can configure the main settings and the wizard will connect to the secondary firewall in order to set it up for High Availability.

States Sync enables the synchronization of states **DHCP HA** enables the HA mode for the DHCP Server **Configuration Sync** enables the configuration sync from the master to the Secondary

Sync Interface should be a separate Interface (or VLAN Interface) where the Master will synchronize data with the Secondary. **Remote Webgui** is the URL of the secondary firewall to enable the HA settings. It does not need to be the *Sync Interface* the Master Firewall only needs access to the Secondary Firewall on that interface to set it up for HA. **Admin User** for the secondary firewall for the onboarding operation. **Password** for the admin user.

The Wizard will setup the secondary firewall and configure it for the HA mode. The special user hasync will be used for the configuration sync. The password will be randomly generated.

20.2 Configuration Sync

You can find the High Availability Settings at **System** → **High Availability**.

It can be found starting with the **Configuration Sync Box**. You can enable or disable the entire sync.

Warning: The config sync only needs to be activated on the Master device. The Slave device will receive all settings from the Master. Do not attempt to enable the config sync from the Slave to the Master. The Master will transfer all settings to the Slave.

Master Device ID is a TBF device ID. If another TBF made an HASync to this TBF, its Device ID is saved here. This makes sure, that this TBF cannot make an HASync to that TBF and an endless loop will start.

Remote [prodname] is the URL of the TBF you want to sync to. It should be an URL on the syncinterface e.g. <https://10.10.20.2>. You will need to make sure to create a firewall rule on the sync interface to allow the access of the Webconsole. Also the API needs to be enabled, make sure to not disable it actively.

Username to login to the remote TBF. There is a default User for this called hasync which already has the hasync user permissions. The password is randomly generated on setup. You need to set one on the slave and master. Be aware that the initial sync will set the slaves user password to the masters hasync user. Make sure they are the same.

Password for the sync user.

You can also **select** or **unselect** all sync options with the appropriate button.

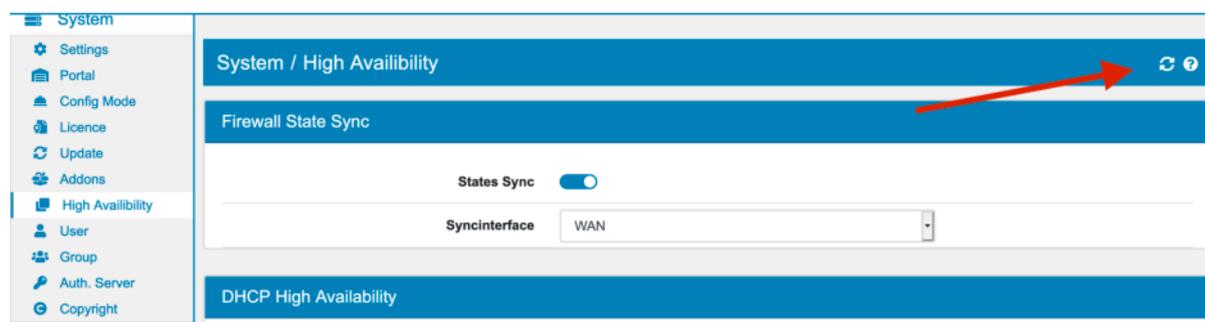
You have the option to enable the synchronization for the different systems. Be aware that if there are dependencies in the background, they will be synchronized even if the option is not set. For example firewall rules need QoS and RoutingTables.

The synchronization is triggered everytime you save or change a setting. There are a few exceptions. The follo

- DHCP
- Firewall and NAT
- VirtualIP

The interfaces synchronization only works from one TBF to another if both are the identical TBF hardware model.

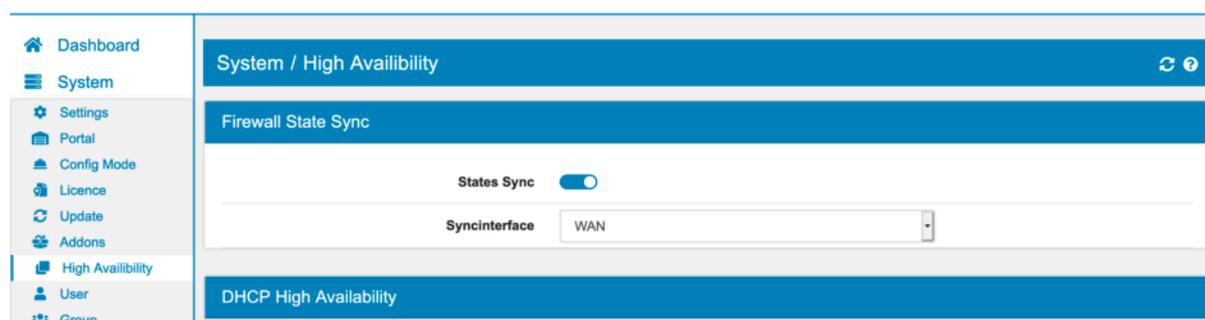
You can also trigger a manual synchronization on a page of a system where the sync is enabled in the upper right corner.



20.3 States Sync

You can find the High Availability Settings at **System** → **High Availability**.

It can be found starting with the **Firewall State Sync Box**. You can enable or disable the entire sync.



Syncinterface is the interface the states updates are published to. The states are sent as a multicast and received by all clients in that network. They are also unencrypted.

A firewall rule will automatically be generated when you enable this option. The **States Sync** must be enabled on all (master, slaves) TBF that participate in the HA Setup.

It contains all firewall state information and they will be automatically added to all TBF that have the option enabled.

States of the other firewall are first saved to a special external states cache and no directly applied to the state table. This allows for faster and easier Synchronization of the states as long as they are not used. As soon as a VRRP failover happens, all states are applied to the firewalls state table.

States and External States can be seen in the States Diagnostics at **Diagnostics** → **States**. External States can also be seen with the shell command `contrackd -e`.

20.4 VRRP Shared Virtual IP Address

VRRP Shared Virtual IP Address are configured on the **General** → **Virtual IPs** page.

On the master node, add a virtual IP address on each interface you want the failover to be active.

The virtual IP addresses must fall within the same subnet of an IP address defined on a real interface (WAN, LAN, INT1, etc.). A unique router ID must be used for each shared virtual IP address on a given interface. The highest priority will be master on each VRRP.

The configuration sync will automatically add -10 to each priority when synchronizing the VIPs to the next TBF. The default priority value is 100 and you can keep it.

The screenshot shows the configuration page for a VRRP Shared Virtual IP Address. The left sidebar contains navigation options: Dashboard, System, General, Certificates, Virtual IPs, DynDNS, Interfaces, Routing, Firewall, Apps, Services, VPN, Tools, and Diagnostics. The main content area is divided into two sections: 'General' and 'VRRP Settings'.

General Settings:

- Enabled:** A toggle switch is turned on.
- VIP Type:** Radio buttons for 'IP Alias' and 'VRRP' (selected).
- Interface:** A dropdown menu showing 'LAN'.
- Description:** A text input field containing 'Description'.

VRRP Settings:

- Router ID:** A text input field containing '1'.
- Priority:** A text input field containing '100'.
- VRRP Password:** A text input field containing '*****' with a visibility toggle.
- Track Interface:** A dropdown menu showing 'ens19'.

At the bottom of the page, there is a copyright notice: © Voleatech GmbH 2017 - 2020.

The screenshot shows the 'Virtual IPs' configuration page. The left sidebar is the same as in the previous screenshot. The main content area is titled 'General / Virtual IPs' and contains a table of configured virtual IP addresses.

Interface	Type	IPs	Priority	Description	Actions
WAN	VRRP (ID: 1)	1.2.3.4/32	100	-	[Edit] [Refresh] [Delete]
LAN	VRRP (ID: 2)	1.2.3.5/32	100	-	[Edit] [Refresh] [Delete]

At the bottom right of the table area, there is a '+ Add' button. Below the table, there is a pagination control showing '1'.

20.4.1 HA Outbound NAT

In order for the failover to work properly the Outbound NAT has to be changed to the VRRP Shared Virtual IP Address. On each WAN Interface that has a VRRP Shared Virtual IP Address defined, please create a SNAT rule at *SNAT (Postrouting)*.

Configure the rule on the Interface where the VRRP Shared Virtual IP Address is defined, set the appropriate Source IPs, if any, and select the VRRP Shared Virtual IP Address as the translation IP address.

This way, all traffic leaving the interface will be changed to come from the VRRP Shared Virtual IP Address. In case of a failover the next TBF can continue to send from this address and there will be no loss of traffic.

The screenshot shows the 'Firewall / NAT' configuration page. The left sidebar contains navigation options: Dashboard, System, General, Interfaces, Routing, Firewall, Aliases, Rules, NAT, Apps, Services, and VPN. The main content area is titled 'Firewall / NAT' and has tabs for 'Inbound (DNAT)', 'Outbound (SNAT)', and 'Both (BINAT)'. The 'Outbound (SNAT)' tab is selected.

Rules Table:

Interface	Address Family	Protocol	Sources	Source Ports	Destinations	Destination Ports	Translation IP	Translation Port	Description	Actions
WAN	IPv4+IPv6	Any	Any	-	Any	-	WAN VRRP (1.2.3.4)	-	-	[Edit] [Refresh] [Delete]

At the bottom of the page, there is a '+ Add', 'Delete', and 'Save' button. Below the table, there is a pagination control showing '1'.

20.4.2 Gateway IP Address

A VRRP Shared Virtual IP Address also needs to be the gateway address for the clients on the internal subnets/interfaces. Either set the gateway VRRP Shared Virtual IP Address manually or use the DHCP Server.

For the DHCP Server look at [DHCP & RA](#)

Set the default gateway to a VRRP Shared Virtual IP Address on each internal network (LAN, e.g. 192.168.1.3). Set the DNS server to the VRRP Shared Virtual IP Address on internal network (LAN, e.g. 192.168.1.3).

20.5 DHCP High Availability

You can find the High Availability Settings at **System** → **High Availability**.

It can be found starting with the **DHCP High Availability Box**. DHCP is an exception in the High Availability setup since it can only have up to three TBF in the setup. Each additional TBF needs to have DHCP disabled, which will be done automatically as long as the settings are enabled on each node.

You can enable or disable the entire DHCP HA Setup.

IP Type it is only supported to have either DHCPv4 or DHCPv6 HA enabled. This is a current limitation of the DHCP Daemon.

Role needs to be set to master on the initial master TBF. There is always only one slave and one backup. The configuration sync will automatically take care of setting the role on the next TBF, so you do not need to change the setting on each member. The role disable will disable DHCP of this type in order for the setup to work properly. Otherwise two DHCP servers will compete to give out leases.

Syncinterface should be the separate sync interface, as all information is synced unencrypted.

Max Unacked Specifies how many unacked clients are allowed before this server assumes that the partner is offline and transitions to the partner-down state. The special value of 0 is allowed for this parameter, which disables the failure-detection mechanism. In this case, a server that can't communicate with its partner over the control channel assumes that the partner server is down and transitions to the partner-down state immediately. The default value of this parameter is 3.

High Availability Mode can be either *Master/Backup* or *Load Balancing*.

Master Server is the IP Address of the master. On the master it will be filled automatically, there is no need to enter it.

Slave Server is the IP Address of the slave. On the slave it will be filled automatically, there is no need to enter it.

Backup Server is the IP Address of the backup. On the backup it will be filled automatically, there is no need to enter it.

Associate Firewall Rule will create the firewall rule to allow the connection between all TBF for the DHCP HA Setup. It is highly recommended to enable it.

20.6 Setup Examples

Your TBF's High Availability Feature can be configured and used based your needs. This page shows you different common example setups. The capabilities are not limited to these setups though. The three core components of TBF's High Availability Feature are *independent* of each other and can be configured and used individually.

- Configuration Synchronization
- States Synchronization
- VRRP Virtual IPs
- (DHCP High Availability)

20.6.1 Configuration Synchronization only

This section describes a setup in which your TBF devices synchronize their configuration but do not provide automatic failover protection. This is for example useful if you are able to swap in a second TBF manually in case of a fault with your primary device. The configuration synchronization feature ensures that your secondary device's configuration is always up to date.

Another scenario would be configuration synchronization in a common network across multiple sites. If you wish to keep parts of the configuration consistent across multiple sites without individually configuring each device, you can use the Configuration Synchronization Feature to do so.

Refer to [Configuration Sync](#) for setup details. In a typical setup where your local network is connected to the LAN Interface you would create a VLAN on top of your LAN Interface with static IP addresses for your TBF devices. The devices then share their configuration via this VLAN. Alternatively you can use a separate physical Interface for this.

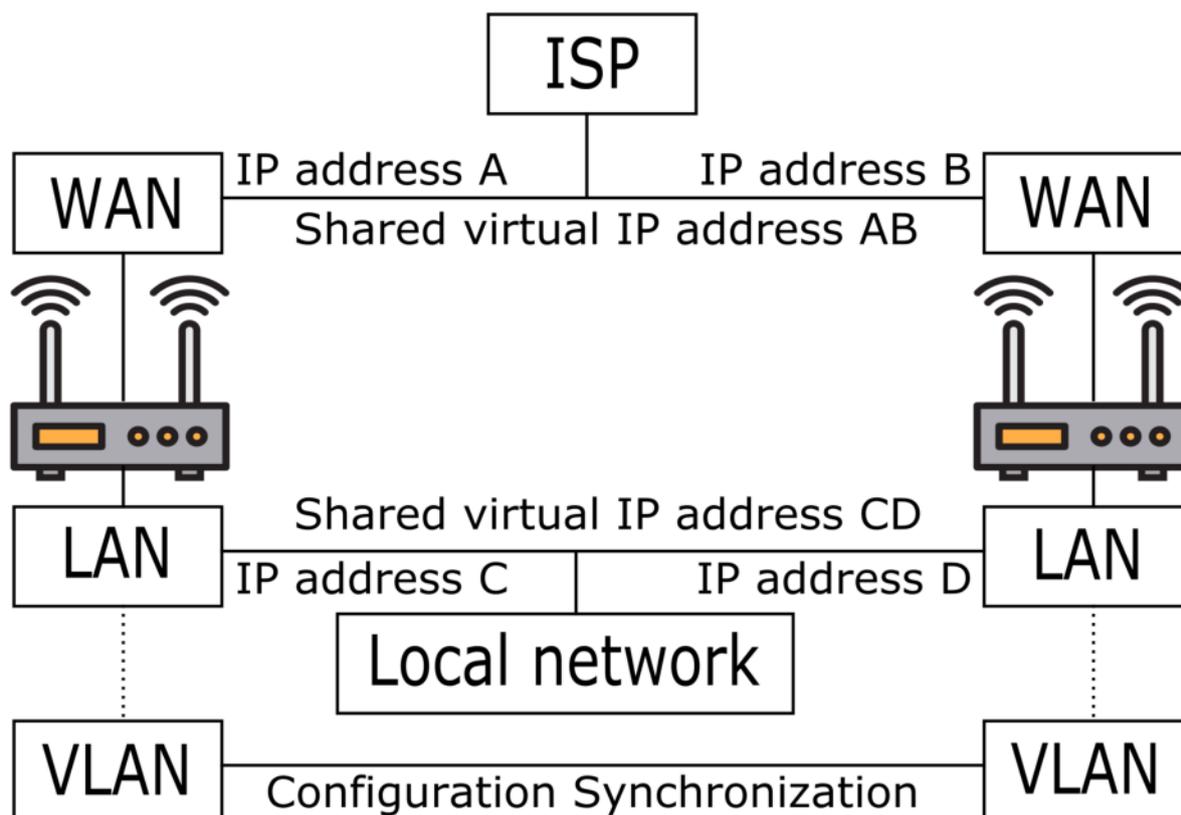
20.6.2 Full Failover Setup

If you wish to have full automatic failover support you can configure your TBF devices to automatically synchronize their configuration and automatically switch to a backup device in case of a fault. This is for example useful for critical networks in remote locations that do not allow for significant downtime.

Refer to the paragraph above for details on how to configure the Configuration Synchronization first. Also refer to [DHCP High Availability](#) if your TBF provides DHCP functionality to your network.

Each router gets its unique IP address in your local network. For an automatic failover setup the standard gateway and its IP address must not change suddenly during operation. Thus the standard gateway needs to be a virtual IP address that is shared between all the routers in your network. See [VRRP Shared Virtual IP Address](#) for configuration details. The same principle also applies to the WAN Interface. In case a secondary device continues operation for the primary device the IP address must not change.

Note: Your TBF's High Availability Feature might *not* be able to detect defective cables or causes outside of the device itself. It is only designed to register faulty devices and re-route traffic through a secondary device.



This image was created with icons by [srip](#) from [Flaticon](#).

DIAGNOSTICS

21.1 Diagnostics General

You can find the Diagnostics at **Diagnostics**.

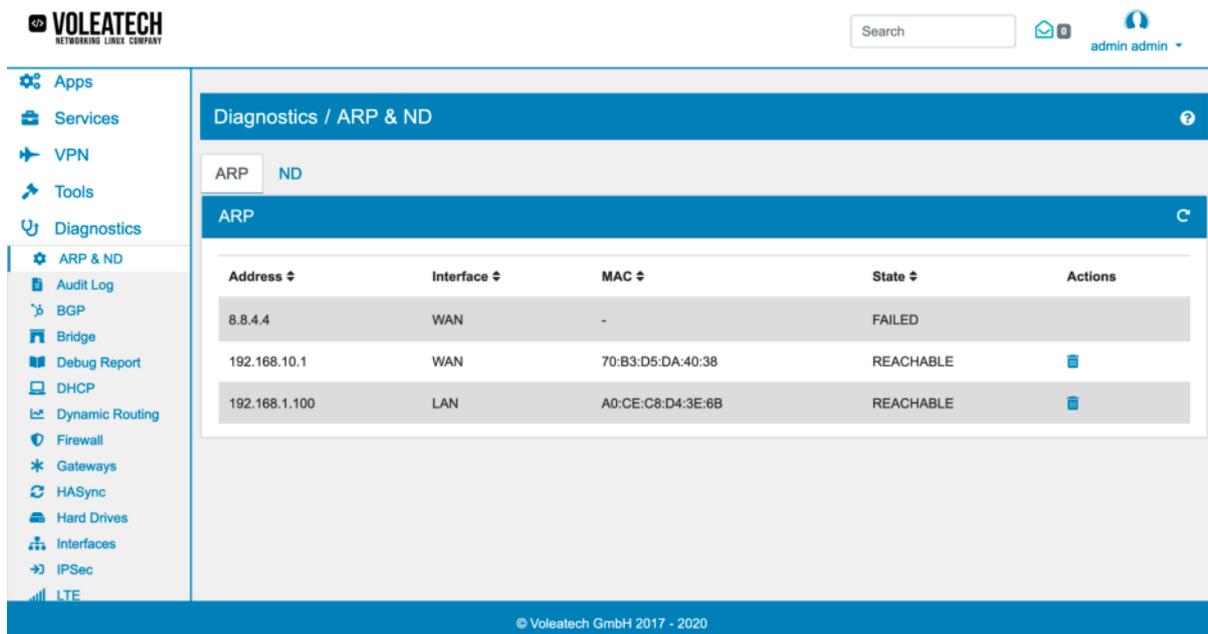
All TBF systems have a diagnostics page to give you the best output regarding all the services and software used. You can debug and find information to assist you in virtually any problem that might come up in your network setup.

All diagnostic pages auto refresh on their own and you can also trigger a refresh by pressing the symbol in the right upper corner.



21.2 ARP & ND

You can find the ARP & ND at **Diagnostics** → **ARP & ND**.



The screenshot shows the Voleatech network management interface. The top navigation bar includes the Voleatech logo, a search bar, and user information (admin admin). The left sidebar contains a list of navigation items: Apps, Services, VPN, Tools, Diagnostics, ARP & ND (selected), Audit Log, BGP, Bridge, Debug Report, DHCP, Dynamic Routing, Firewall, Gateways, HASync, Hard Drives, Interfaces, IPsec, and LTE. The main content area displays the 'Diagnostics / ARP & ND' page with the 'ARP' tab selected. Below the tab, there is a table with the following data:

Address ↕	Interface ↕	MAC ↕	State ↕	Actions
8.8.4.4	WAN	-	FAILED	
192.168.10.1	WAN	70:B3:D5:DA:40:38	REACHABLE	
192.168.1.100	LAN	A0:CE:C8:D4:3E:6B	REACHABLE	

Here you have an overview of all TBF **Address Resolution Protocol** and **Neighbor Discovery** entries. The first is used for the internet protocol v4, the second for v6.

Each entry shows the IP **Address**, the used **Interface**, the **MAC** Address and its **State**, for example *STALE*, *DELAY*, *REACHABLE*, *FAILED*.

On the right side of the entries you have the possibility to delete the entry and remove it from the system.

Address	Interface	MAC	State	Actions
fe80::6cea:bbff:fe6:3e52	WAN	6E:EA:BB:E6:3E:52	STALE	[Delete]
fe80::ae1f:6bff:fead:2850	WAN	AC:1F:6B:AD:28:50	STALE	[Delete]
fe80::205b:7dff:febe:55ac	WAN	22:5B:7D:BE:55:AC	STALE	[Delete]
fe80::1454:f95a:6afe:e581	LAN	A0:CE:C8:D4:3E:6B	STALE	[Delete]
fe80::250:43ff:fe02:201	WAN	00:50:43:02:02:01	STALE	[Delete]
fe80::8f7:f5ff:fe27:fa52	WAN	0A:F7:F5:27:FA:52	STALE	[Delete]
fe80::1ca4:b0ff:fe77:564b	WAN	1E:A4:B0:77:56:4B	STALE	[Delete]
fe80::54dc:edff:fe3d:41b8	WAN	56:DC:ED:3D:41:B8	STALE	[Delete]

21.3 Audit Log

You can find the Audit Log at **Diagnostics** → **Audit Log**.

Type	Object	Action	Changes	User	IP	Time
Alias Entry	fe80::9cf3:b1ff:fe1e:f151	Update	ipaddress: None → fe80::9cf3:b1ff:fe1e:f151	None	None	2020-11-10 14:09
Firewall Rule Port	Any	Create	id: None → 50 alias: None → Any uuid: None → 1e96bcef-3a43-4ce1-932b-1519b68e2fca	admin	192.168.1.100	2020-11-10 14:09
Firewall Rule Ip	Any	Create	id: None → 55 netmask: None → 128 alias: None → Any redirectip: None → False uuid: None → df346660-0692-41b1-8774-ce70f142ea30	admin	192.168.1.100	2020-11-10 14:09
Firewall Rule Port	Any	Create	id: None → 49 alias: None → Any uuid: None → e37abd4e-715c-45b5-8026-	admin	192.168.1.100	2020-11-10 14:09

This page shows all TBF changes made by users or the system itself.

The **Type** describes in which category the change was made and the **Object** refers to the name of the database object. **Action** can be create, update or delete. In **Changes** you can see a more detailed overview of what fields were changed from which value. **User** shows which TBF user made the change or none if the change was triggered by the system. The **IP** is only displayed if the change was made by

a user and shows from which network address he made the change. **Time** shows the date and time of the change.

You can also search for a change which will filter the changes by the search keywords in the name of the database object.

In the top left corner you can find a **XLSX Export** button which will let you download all Audit Log entries as a xlsx file to your computer.

If you want to log the Audit Log to Syslog, you can enable that in [Logging](#) and the logfile will be audit.log.

21.4 802.1X Authenticator

You can find the 802.1X Authenticator Diagnostics at **Diagnostics** → **Services** → **802.1X Authenticator**.

The screenshot shows the 'Diagnostics / Services / 802.1X Auth. / View' page. A 'WAN' tab is selected. Below the breadcrumb is a 'Connected Clients' section with a refresh icon. A table lists the following data:

MAC Address	Flags	Quiet Period	Server Timeout	Reauth Period	Session Time	Actions
70:b3:d5:da:30:1a	AUTHORIZED	60	30	3600	27	✕
70:b3:d5:da:30:04	AUTHORIZED	50	30	3600	45	✕

Here you have an overview of all authenticated clients, the timeouts and also the possibility to *disconnect* a client.

21.5 BFD

You can find the BFD Diagnostics at **Diagnostics** → **Routing** → **BFD**.

The screenshot shows the 'Diagnostics / Routing / BFD' page. A 'Peers' tab is selected. Below the breadcrumb is a 'BFD' section. The configuration for a peer is displayed as follows:

```

BFD Peers:
  peer 100.60.127.214 vrf default
    ID: 3469372006
    Remote ID: 0
    Active mode
    Status: shutdown
    Diagnostics: ok
    Remote diagnostics: ok
    Peer Type: configured
    Local timers:
      Detect-multiplier: 3
      Receive interval: 300ms
      Transmission interval: 300ms
      Echo transmission interval: 50ms
    Remote timers:
      Detect-multiplier: 3
      Receive interval: 1000ms
      Transmission interval: 1000ms
      Echo transmission interval: 0ms
  
```

Here you can see all information about your **Bidirectional Forwarding Detection** setup.

The information on the page are updated periodically without any user input.

To change your BFD setup please go to **Routing** → **BFD** and refer to the documentation at [BFD](#).

21.6 BGP

You can find the BGP Diagnostics at **Diagnostics** → **Routing** → **BGP**.

Here you can see all information about your **Border Gateway Protocol** setup. It's divided into *Summary*, *Neighbors*, *IPv4*, *IPv6*, *NextHop* and *Memory*.

The information on the page are updated periodically without any user input.

To change your BGP setup please go to **Routing** → **BGP** and refer to the documentation at [BGP](#).

21.7 Bond

You can find the Bond Diagnostics at **Diagnostics** → **Interfaces** → **Bond**.

Here you can see all **Bond** information.

You can select the desired Bond to get the information.

To revisit your Bond settings please go to **Interfaces** → **Assign** → **Bonds** and refer to the Bond documentation at [Bond](#).

The output for Bond could look like this:

```
Ethernet Channel Bonding Driver: v6.6.0-1-vtair-arm64
```

```
Bonding Mode: load balancing (xor)
Transmit Hash Policy: layer2+3 (2)
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 100
Down Delay (ms): 100
Peer Notification Delay (ms): 0
```

```
Slave Interface: eno4
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: c8:98:db:80:02:62
Slave queue ID: 0
```

```
Slave Interface: eno5
MII Status: up
Speed: 10000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: c8:98:db:80:02:63
Slave queue ID: 0
```

21.8 Bridge

You can find the Bridge Diagnostics at **Diagnostics** → **Interfaces** → **Bridge**.

bridge name	bridge id	STP enabled	interfaces
br0	8000.4e3f148858e6	yes	eth2 gretap1

Here you can see all **Bridge** information. It's divided into *Bridge* and *Mac*. You can select the desired bridge to get the information.

To revisit your Bridge settings please go to **Interfaces** → **Assign** → **Bridges** and refer to the Bridge documentation at [Bridge](#).

The output for Bridge could look like this:

```
bridge name      bridge id      STP enabled  interfaces
br0              8000.0008a20a8857  yes          enp0s20f2
```

And the output for Mac like this:

```
port no  mac addr      is local?  ageing timer
1        00:08:a2:0a:88:57  yes        0.00
1        00:08:a2:0a:88:57  yes        0.00
```

21.9 Captive Portal

You can find the Captive Portal Diagnostics at **Diagnostics** → **Services** → **Captive Portal**.

MAC	Username	IP	Inactivity Timeout	Packets	Bytes	Actions
12:34:56:78:9a:bc	smv_testlehrer	192.168.10.143	2024-06-13 13:00	0	0	
12:34:56:78:9a:bd	smv_testschueler	192.168.10.107	2024-06-13 13:00	2	14324	
a0:ce:c8:06:09:08	cpvouchercode	192.168.10.175	2024-06-13 12:25	13	8256	

Here you can see all information about your different **Captive Portal** setups. You can see the connected clients with their MAC Address, Username, IP Address and when their session is about to expire. You can remove clients manually by triggering the delete action.

21.10 DDoS

You can find the DDoS Diagnostics at **Diagnostics** → **Firewall** → **DDoS**.

The screenshot shows the 'Diagnostics / DDoS' interface. It contains two main sections:

DDoS Dynamic Blocker

IP	Blocker Expiration	Actions
81.7.16.52	2021-06-02 14:28:17	✕
172.217.18.99	2021-06-02 14:28:17	✕
216.58.210.3	2021-06-02 14:28:17	✕
216.58.232.144	2021-06-02 14:28:17	✕

DDoS Rules

IP	Counter Packets	Counter Bytes
1.2.3.4	0	0
1.2.3.4, 2.3.4.5	0	0

Here you can see all information about your **DDoS** blocked clients. It's divided into the blocked clients from Firewall DDoS Rules and the dynamic block entries. Both pages have a **Ranges** and **Leases** table.

To change the blocked clients from the Firewall DDoS Rules please go to **Firewall** → **Rules** and select DDoS. Please also refer to the documentation at [DDoS Rules](#).

The dynamic block entries can also be deleted manually by clicking on the corresponding action. The remaining block time is also displayed.

21.11 Debug Report

You can find the Debug Report at **Diagnostics** → **Debug** → **Debug Report**.

The screenshot shows the 'Diagnostics / Debug Report' interface. It features a sidebar menu on the left with the following items:

- Tools
- Diagnostics
 - ARP & ND
 - Audit Log
 - BGP
 - Bridge
 - Debug Report
 - DHCP
 - Dynamic Routing
 - Firewall
 - Gateways
 - HASync
 - Hard Drives
 - Interfaces
 - IPSec
 - LTE
 - Logfiles
 - MDRaid
 - NTP
 - OpenVPN

The main content area is titled 'Diagnostics / Debug Report' and contains a 'Debug' section with an 'Advanced' toggle switch. Below the toggle is a 'Download' button. The 'Overview' section lists the following items:

- OS Uptime
- Disk Space
- Memory
- BIOS
- Cron
- Interfaces
- Routes
- ARP Table
- Active Internet connections
- Firewall Rules
- Status DNS

© Voleatech GmbH 2017 - 2020

The screenshot shows the Voleatech management interface. The left sidebar contains a list of tools and services, with 'Debug Report' highlighted. The main content area is divided into three sections: 'OS Uptime', 'Disk Space', and 'Memory'. The 'OS Uptime' section shows the system has been up for 6 days, 22:30, with 2 users and a load average of 0.16, 0.86, and 0.65. The 'Disk Space' section displays a table of filesystem usage:

Filesystem	Size	Used	Avail	Use%	Mounted on
udev	985M	0	985M	0%	/dev
tmpfs	201M	21M	181M	11%	/run
/dev/mmcblk0p1	6.2G	2.1G	3.8G	36%	/
tmpfs	1005M	2.1M	1003M	1%	/dev/shm
tmpfs	5.0M	0	5.0M	0%	/run/lock
tmpfs	1005M	0	1005M	0%	/sys/fs/cgroup
log2ram	200M	28M	173M	14%	/var/log
tmpfs	201M	0	201M	0%	/run/user/0

The 'Memory' section is currently empty.

The debug report contains diagnostic and debugging information about your system. If you require support from Voleatech, you might be asked to supply a debug report. All passwords will be censored for the generated report.

The debug report contains logfiles, configurations and system reports so that a problem can be more easily diagnosed.

21.12 DHCP

You can find the DHCP Diagnostics at **Diagnostics** → **Services** → **DHCP**.

The screenshot shows the Voleatech management interface for DHCP diagnostics. The left sidebar contains a list of tools and services, with 'DHCP' highlighted. The main content area is divided into three sections: 'Diagnostics / DHCP', 'DHCP', and 'Leases (LAN)'. The 'Diagnostics / DHCP' section shows tabs for 'IPv4', 'IPv6', and 'Prefix Delegation'. The 'DHCP' section displays a table of interface ranges and IP usage:

Interface	Range	DHCP IPs	Used IPs	Available IPs
LAN	192.168.1.100 - 192.168.1.150	51	1	50
Total		51	1	50

The 'Leases (LAN)' section displays a table of active leases:

Address	Hardware Address	Valid Lifetime	Expire	Hostname	State	Actions
192.168.1.100	A0:CE:C8:E	4000 sec	2020-11-12 11:30:13	macbook-pro	default	

Here you can see all information about your **DHCP** server. It's divided into the IP protocol v4 and v6. Both pages have a **Ranges** and **Leases** table.

At Ranges you can see all **Interfaces** where the DHCP server is enabled and their configured **Pools**. At Leases you can see each lease with its IP **Address**, **Hardware Address** and **Hostname**. The **Valid Lifetime** and a timestamp at **Expire** show until when the lease is valid. Last but not least there is the **State** of the lease.

In the **Actions** column you have the ability to edit, create or delete static leases, as well as removing dynamic leases from the server.

To change the DHCP setup please go to **Services** → **DHCP & RA** and refer to the DHCP documentation at [DHCP & RA](#).

21.12.1 DHCP HA Modes

The DHCP Server are running in hot-standby mode during normal HA use. The master server is distributing the DHCP leases and the secondary server is in standby mode.

The following states are possible:

The following is the list of all possible server states:

backup - normal operation of the backup server. In this state it receives lease updates from the active servers.

hot-standby - normal operation of the active server running in the hot-standby mode; both the primary and the standby server are in this state during their normal operation. The primary server responds to DHCP queries and sends lease updates to the standby server and to any backup servers that are present.

in-maintenance - an active server transitions to this state as a result of being notified by its partner that the administrator requested maintenance of the HA setup. The administrator requests the maintenance by sending the ha-maintenance-start to the server which is supposed to take over the responsibility for responding to the DHCP clients while the other server is taken offline for maintenance. If the server is in the in-maintenance state it can be safely shut down. The partner is in the partner-in-maintenance state from which it will transition to the partner-down state immediately after it finds that the server in maintenance was shut down.

partner-down - an active server transitions to this state after detecting that its partner (another active server) is offline. The server does not transition to this state if only a backup server is unavailable. In the partner-down state the active server responds to all DHCP queries, including those queries which are normally handled by the server that is now unavailable.

partner-in-maintenance - an active server transitions to this state after receiving a ha-maintenance-start command from the administrator. The server in this state becomes responsible for responding to all DHCP requests. The server sends ha-maintenance-notify command to the partner which is supposed to enter the in-maintenance state. If that is the case, the server remaining in the partner-in-maintenance state keeps sending lease updates to the partner until it finds that the partner stops responding to those lease updates, heartbeats or any other commands. In this case, the server in the partner-in-maintenance state transitions to the partner-down state and keeps responding to the queries, but no longer sends lease updates.

passive-backup - a primary server running in the passive-backup HA mode transitions to this state immediately after it is booted up. The primary server being in this state responds to the entire DHCP traffic and sends lease updates to the backup servers it is connected to. By default, the primary server does not wait for the acknowledgments from the backup servers and responds to the DHCP query right after sending the lease updates to all backup servers. If any of the lease updates fails, a backup server misses such lease update but the DHCP client is still provisioned.

ready - an active server transitions to this state after synchronizing its lease database with an active partner. This state indicates to the partner - which may be in the partner-down state - that it should return to normal operation. If and when it does, the server in the ready state will also start normal operation.

syncing - an active server transitions to this state to fetch leases from the active partner and update the local lease database. When in this state, the server issues the dhcp-disable command to disable the DHCP service of the partner from which the leases are fetched. The DHCP service is disabled for a maximum time of 60 seconds, after which it is automatically re-enabled, in case the syncing partner was unable to re-enable the service. If the synchronization is completed, the syncing server issues the dhcp-enable command to re-enable the DHCP service of its partner. The syncing operation is synchronous; the server waits for an answer from the partner and does nothing else while the lease synchronization takes place. A server that is configured not to synchronize the lease database with its partner, i.e. when

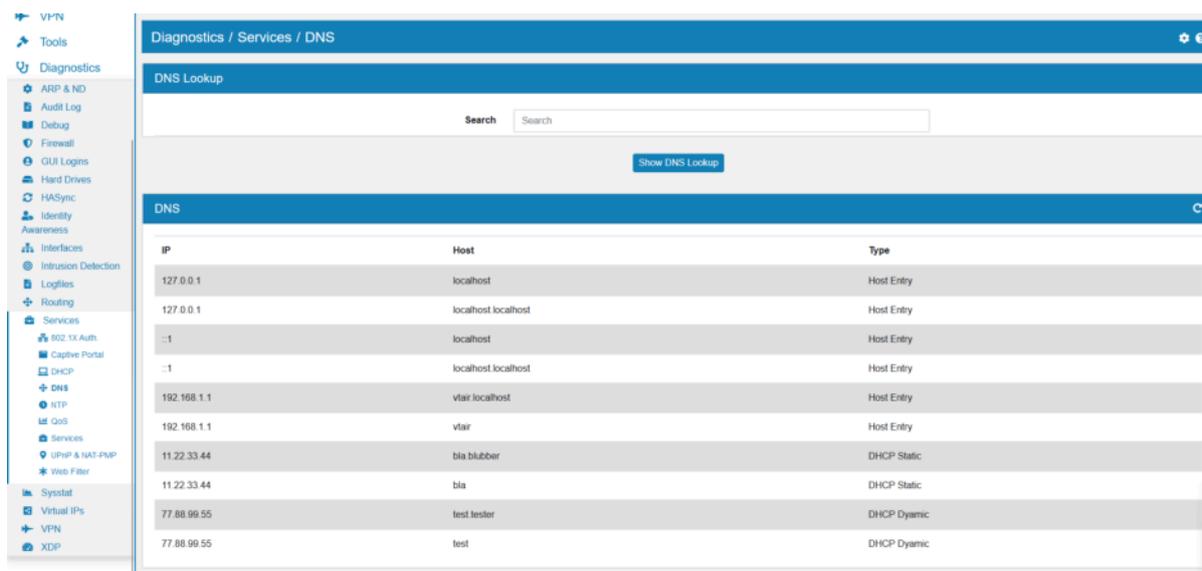
the sync-leases configuration parameter is set to false, will never transition to this state. Instead, it will transition directly from the waiting state to the ready state.

terminated - an active server transitions to this state when the High Availability hooks library is unable to further provide reliable service and a manual intervention of the administrator is required to correct the problem. Various issues with the HA setup may cause the server to transition to this state. While in this state, the server continues responding to DHCP clients based on the HA mode selected (load-balancing or hot-standby), but the lease updates are not exchanged and the heartbeats are not sent. Once a server has entered the “terminated” state, it will remain in this state until it is restarted. The administrator must correct the issue which caused this situation prior to restarting the server (e.g. synchronize the clocks); otherwise, the server will return to the “terminated” state once it finds that the issue persists.

waiting - each started server instance enters this state. The backup server transitions directly from this state to the backup state. An active server sends a heartbeat to its partner to check its state; if the partner appears to be unavailable, the server transitions to the partner-down state. If the partner is available, the server transitions to the syncing or ready state, depending on the setting of the sync-leases configuration parameter. If both servers appear to be in the waiting state (concurrent startup), the primary server transitions to the next state first. The secondary or standby server remains in the waiting state until the primary transitions to the ready state.

21.13 DNS

You can find the DNS Diagnostics at **Diagnostics** → **Services** → **DNS**.



IP	Host	Type
127.0.0.1	localhost	Host Entry
127.0.0.1	localhost localhost	Host Entry
::1	localhost	Host Entry
::1	localhost localhost	Host Entry
192.168.1.1	vitar localhost	Host Entry
192.168.1.1	vitar	Host Entry
11.22.33.44	bla blubber	DHCP Static
11.22.33.44	bla	DHCP Static
77.88.99.55	test testler	DHCP Dynamic
77.88.99.55	test	DHCP Dynamic

Here you can see all your current **DNS** entries. There are three different types listed: *DHCP Static*, *DHCP Dynamic* and *Host Entry*.

To change the DNS setup please go to **Services** → **DNS** and refer to the DNS documentation at [DNS](#).

On the top you can run a DNS Lookup on the firewall itself for a domain.

21.14 DNS Domain

You can find the DNS Domain Diagnostics at **Diagnostics** → **Firewall** → **DNS Domain**.

The screenshot shows the Mikrotik WinBox interface for DNS Domain diagnostics. The breadcrumb path is 'Diagnostics / Firewall / DNS Domain'. The main content area is titled 'DNS Wildcard Domain' and features a dropdown menu for selecting a domain, currently set to '*.wikipedia.org'. Below this, there are two sections: 'Entries v4' and 'Entries v6'. The 'Entries v4' section contains a table with the following data:

Value	Packets	Bytes
91.198.174.192	0	0

The 'Entries v6' section is currently empty.

Here you can select a *DNS Wildcard Domain* and see its v4 and v6 entries.

The information on the page are updated periodically without any user input.

To change your DNS Domain setup please go to **Firewall** → **Network Objects**.

21.15 Dynamic Routing

You can find the Dynamic Routing Diagnostics at **Diagnostics** → **Routing** → **Dynamic Routing**.

Here you can see all information about your **Dynamic Routing** setup. It's divided into *FFR Routes*, *FFR Routes v6*, *Access List*, *Access List v6*, *Prefix List*, *Prefix List v6* and *Route Map*.

The information on the page are updated periodically without any user input.

To change your Dynamic Routing setup please go to **Routing** → **Dynamic** and refer to the documentation at [Dynamic](#).

21.16 Firewall

You can find the Firewall Diagnostics at **Diagnostics** → **Firewall** → **Firewall**.

The screenshot shows the Firewall Diagnostics interface. The top navigation bar includes 'Tools', 'Diagnostics', and 'Firewall'. The left sidebar lists various system components, with 'Firewall' selected. The main content area is divided into two tabs: 'Log' and 'Ruleset'. The 'Log' tab is active, displaying a table of firewall log entries.

Firewall Configuration:

- Number of Lines: 50
- Interface: All
- Protocol: Any
- Source Address: Source Address
- Source Port: Source Port
- Destination Address: Destination Address
- Destination Port: Destination Port
- Action: Any

Log Table:

Time	Interface	Source	Destination	Protocol	Comment	Result	Actions
Aug 28 15:44:32	WAN (enp0s20f0)	192.168.10.116.65471	239.255.255.250.1900	UDP	Input (Default Block Rule)	drop	
Aug 28 15:41:07	WAN (enp0s20f0)	192.168.10.30.138	192.168.10.255.138	UDP	Input (Default Block Rule)	drop	
Aug 28 15:40:28	WAN (enp0s20f0)	192.168.10.106.68	255.255.255.255.67	UDP	Input (Default Block Rule)	drop	
Aug 28 15:39:27	WAN (enp0s20f0)	192.168.10.116.54261	239.255.255.250.1900	UDP	Input (Default Block Rule)	drop	
Aug 28 15:34:22	WAN (enp0s20f0)	192.168.10.116.65482	239.255.255.250.1900	UDP	Input (Default Block Rule)	drop	
Aug 28 15:29:17	WAN (enp0s20f0)	192.168.10.116.37723	239.255.255.250.1900	UDP	Input (Default Block Rule)	drop	
Aug 28 15:29:05	WAN (enp0s20f0)	192.168.10.30.138	192.168.10.255.138	UDP	Input (Default Block Rule)	drop	
Aug 28 15:28:37	WAN (enp0s20f0)	192.168.10.30.58856	224.0.0.252.5355	UDP	Input (Default Block Rule)	drop	
Aug 28 15:28:37	WAN (enp0s20f0)	192.168.10.30.58856	224.0.0.252.5355	UDP	Input (Default Block Rule)	drop	

There are three tabs. In the **Log** tab you can browse, search and parse the current firewall log. Each log entry comes from the firewall log.

Be aware that by default only deny entries are logged. If you need more logging, turn it one in each firewall rule *Firewall Rules (Forward and Input)*.

You can also *create a firewall rule* directly from a log entry by hitting the action symbol on the right.

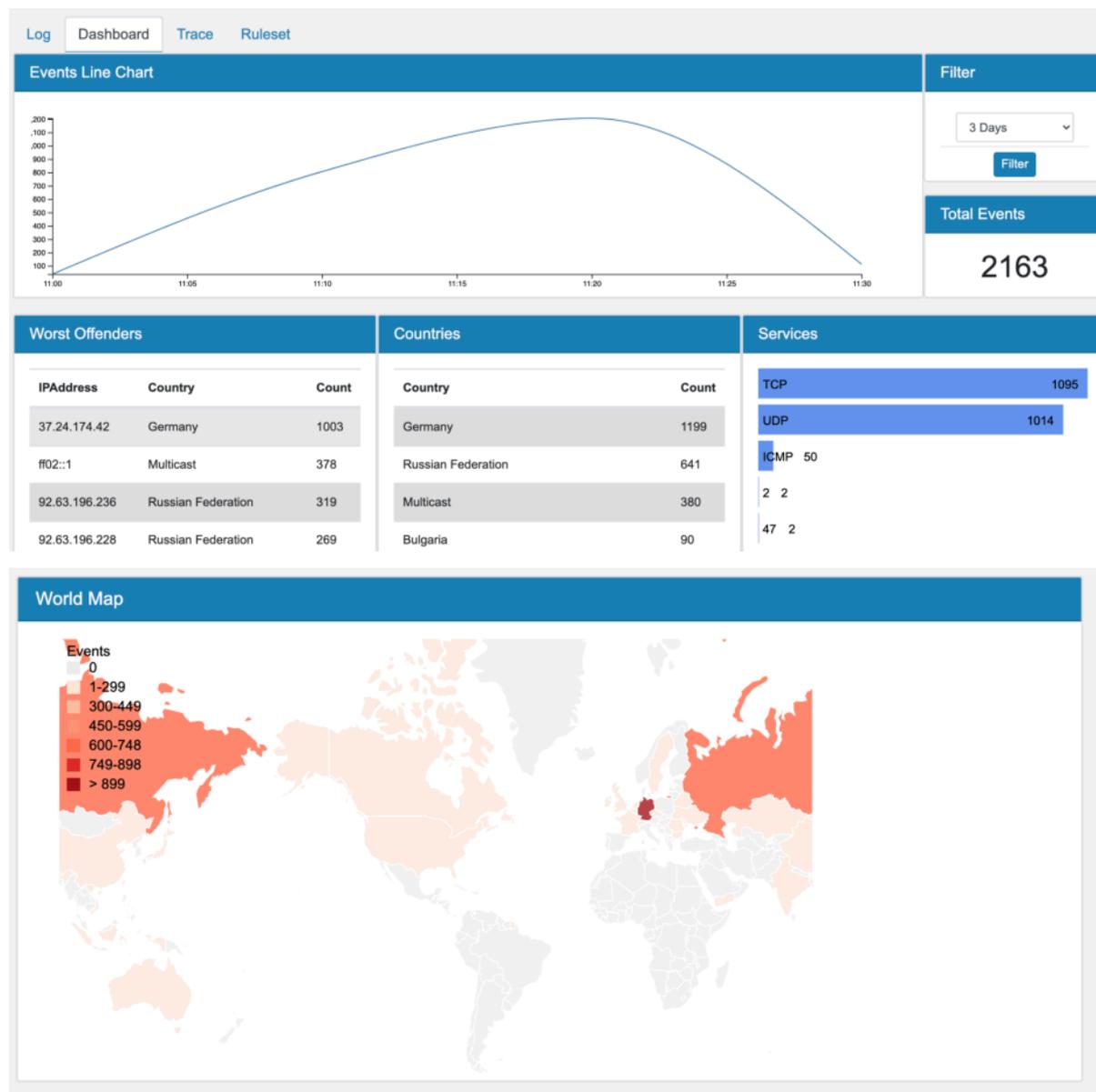
Source and destination IPs can show reverse DNS entry on hover, as long as the TBF can resolve the IP.

In the **Ruleset** tab you can see the current system firewall ruleset.

The **Dashboard** tab provides an interactive view of the collected data from log events.

21.16.1 Firewall Dashboard

The dashboard shows you firewall information by country and origin. The dashboard is a convenient way of visualising the event data.



Note: Logfile Analysis needs to be enabled to see data in the Dashboard. It is disabled by default as it costs performance. It can be enabled at [Settings](#).

21.16.2 Ruleset

The ruleset tabs shows you the current firewall rules in the system.

```

table inet nat {
  chain prerouting {
    type nat hook prerouting priority dstnat; policy accept;
    jump prerouting_minipnpd
  }

  chain postrouting {
    type nat hook postrouting priority srcnat; policy accept;
    meta l4proto vrrp accept comment "No NAT for VRRP"
    ipsec out reqid 0-2147483647 accept comment "No NAT for IPsec Policy"
    oifname "enp0s20fe" ip saddr { 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 } counter packets 507 bytes 30546 masquerade fully-random comment "SNAT WAN (Private Networks)"
    oifname "enp0s20fe" ip6 saddr fc00::/7 counter packets 0 bytes 0 masquerade fully-random comment "SNAT WAN (Private Networks)"
    jump postrouting_minipnpd
  }

  chain prerouting_captiveportal {
  }
}

```

21.16.3 Trace

If you enabled the trace option on one or more firewall rules, matching traffic can be seen here. This is a good tool to debug your firewall rules. The packet will be followed through the firewall from DNAT to rule until SNAT.

21.17 Gateways

You can find the Gateways Diagnostics at **Diagnostics** → **Routing** → **Gateways**.

Name	Gateway	Monitor IP	RTT	RTTsd	Loss	Status	Description
WAN_IPv4_DHCP	192.168.10.1 (DHCP)	192.168.10.1	0.422ms	0.035ms	0%	Online	WAN DHCP IPv4 Gateway
WAN_IPv6_DHCP	DHCP	-	-	-	-	Unknown	WAN DHCP IPv6 Gateway

Here you have an overview of all TBF **gateways** and if configured their monitoring status.

To create your own gateways or edit existing ones please go to **Routing** → **Gateways** and refer to the documentation at [Gateway](#).

21.17.1 Routing Tables

Two additional tabs show **Routing Tables v4** and **Routing Tables v6**. Here you have all routing tables and their associated gateways, ordered by priority.

To create additional routing tables or add gateways to existing ones please go to **Routing** → **Routes** → **Routing Tables** and refer to the documentation at [Routes](#).

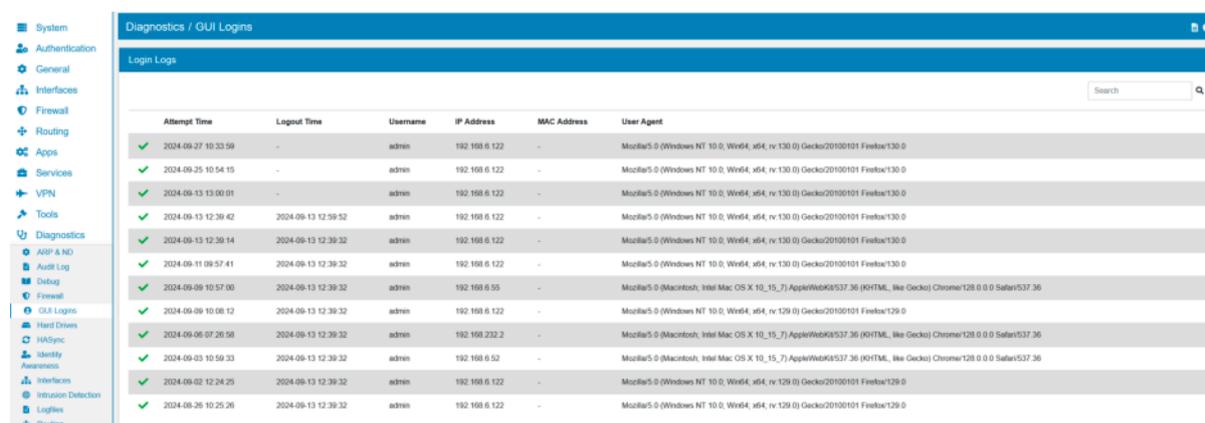
21.17.2 RRD Graphs

The last tab is **RRD Graphs**. Here you can see historical data of TBF gateway checks.

You can select a gateway, *from date* and *to date*. There will be three graphs generated, one for *latency*, *stddev* and *loss*.

21.18 GUI Logins

You can find the GUI Logins Diagnostics at **Diagnostics** → **GUI Logins**.



The screenshot shows the 'Diagnostics / GUI Logins' page. It features a search bar and a table with the following columns: Attempt Time, Logout Time, Username, IP Address, MAC Address, and User Agent. The table contains 10 rows of data, all with a green checkmark in the first column indicating successful logins.

Attempt Time	Logout Time	Username	IP Address	MAC Address	User Agent
2024-09-27 10:33:59	-	admin	192.168.6.122	-	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
2024-09-25 10:54:15	-	admin	192.168.6.122	-	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
2024-09-13 13:00:01	-	admin	192.168.6.122	-	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
2024-09-13 12:39:42	2024-09-13 12:59:52	admin	192.168.6.122	-	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
2024-09-13 12:39:14	2024-09-13 12:39:32	admin	192.168.6.122	-	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
2024-09-11 09:57:41	2024-09-13 12:39:32	admin	192.168.6.122	-	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
2024-09-09 10:57:00	2024-09-13 12:39:32	admin	192.168.6.55	-	Mozilla/5.0 (Macintosh; Intel Mac; OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
2024-09-09 10:08:12	2024-09-13 12:39:32	admin	192.168.6.122	-	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0
2024-09-06 07:28:58	2024-09-13 12:39:32	admin	192.168.232.2	-	Mozilla/5.0 (Macintosh; Intel Mac; OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
2024-09-03 10:59:33	2024-09-13 12:39:32	admin	192.168.6.52	-	Mozilla/5.0 (Macintosh; Intel Mac; OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
2024-09-02 12:24:25	2024-09-13 12:39:32	admin	192.168.6.122	-	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0
2024-08-28 10:25:26	2024-09-13 12:39:32	admin	192.168.6.122	-	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0

Here you can see all TBF GUI Login attempts, successful or failed. Each login shows the *Status*, *Attempt Time*, *Logout Time*, *Username*, *IP Address*, *MAC Address* and *User Agent*. The first column shows if the login was successful or not.

21.19 Hard Drives

You can find the Hard Drives Diagnostics at **Diagnostics** → **Hard Drives** → **Hard Drives** (this is not available on TBF 100/300 devices due to the eMMC drive type).

Diagnostics / Hard Drives

Info Test **Log** Capabilities

Hard Drives

Hard Drive

Result

```
smartctl 6.6 2017-11-05 r4594 [x86_64-linux-5.4.0-4-vtair-amd64] (local build)
Copyright (C) 2002-17, Bruce Allen, Christian Franke, www.smartmontools.org

=== START OF READ SMART DATA SECTION ===
General SMART Values:
Offline data collection status: (0x02) Offline data collection activity
was completed without error.
Auto Offline Data Collection: Disabled.
Self-test execution status:      (  0) The previous self-test routine completed
without error or no self-test has ever
been run.
Total time to complete Offline
data collection:                ( 120) seconds.
Offline data collection
capabilities:                    (0x11) SMART execute Offline immediate.
No Auto Offline data collection support.
```

Here you can see *S.M.A.R.T* (Self-Monitoring, Analysis and Reporting Technology) information of your hard drives.

It's divided into *Info*, *Test*, *Log* and *Capabilities*. At *Test* you can start a *short* or *long* test of a specific hard drive and the result can be seen at *Log* after a few minutes.

Diagnostics / Hard Drives

Info **Test** Log Capabilities

Hard Drives

Hard Drive

Test

Start Test

The *Info* could look like this:

```
=== START OF INFORMATION SECTION ===
Device Model:          TS128GMTS400S
Serial Number:         7612325CE35121310830
Firmware Version:     Q0926B
User Capacity:         128,035,676,160 bytes [128 GB]
Sector Size:           512 bytes logical/physical
Rotation Rate:        Solid State Device
Form Factor:           M.2
Device is:             Not in smartctl database [for details use: -P showall]
ATA Version is:       ACS-2 (minor revision not indicated)
SATA Version is:      SATA 3.1, 6.0 Gb/s (current: 3.0 Gb/s)
Local Time is:        Mon May 20 15:06:44 2019 CEST
```

(continues on next page)

(continued from previous page)

```
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
```

Info Test Log Capabilities

Hard Drives

Hard Drive /dev/sda

Result

```
smartctl 6.6 2017-11-05 r4594 [x86_64-linux-5.4.0-4-vtair-amd64] (local build)
Copyright (C) 2002-17, Bruce Allen, Christian Franke, www.smartmontools.org

=== START OF INFORMATION SECTION ===
Device Model:     OSC M.2 256GB
Serial Number:   05C20030200000000034
LU WWN Device Id: 0 000000 0000000000
Firmware Version: 00927A
User Capacity:   256,060,514,304 bytes [256 GB]
Sector Size:     512 bytes logical/physical
Rotation Rate:   Solid State Device
Form Factor:     M.2
Device is:       Not in smartctl database [for details use: -P showall]
ATA Version is:  ACS-2 (minor revision not indicated)
SATA Version is: SATA 3.1, 6.0 Gb/s (current: 6.0 Gb/s)
Local Time is:   Thu Nov 12 18:07:55 2020 CET
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
```

and the Log like this:

```
=== START OF READ SMART DATA SECTION ===
SMART Self-test log structure revision number 1
Num Test_Description      Status                    Remaining  LifeTime(hours)  LBA_of_first_error
# 1 Short captive          Completed without error   00%        3327              -
# 2 Short offline         Completed without error   00%        3325              -
# 3 Extended offline      Completed without error   00%        3324              -
# 4 Short offline         Completed without error   00%        3324              -
# 5 Short offline         Completed without error   00%        3251              -
```

Info Test Log Capabilities

Hard Drives

Hard Drive /dev/sda

Result

```
smartctl 6.6 2017-11-05 r4594 [x86_64-linux-5.4.0-4-vtair-amd64] (local build)
Copyright (C) 2002-17, Bruce Allen, Christian Franke, www.smartmontools.org

=== START OF READ SMART DATA SECTION ===
Warning! SMART Self-Test Log Structure error: invalid SMART checksum.
SMART Self-test log structure revision number 1
Num Test_Description      Status                    Remaining  LifeTime(hours)  LBA_of_first_error
# 1 Short offline         Completed without error   00%         0                 -
```

21.20 HASync

You can find the HASync Diagnostics at **Diagnostics** → **HASync**.

Name	Last Sync	Status	Action
BGP	-	Disabled	
Certificate	-	Pending	↻
Cron	-	Disabled	
DHCP	-	Disabled	
DNS	-	Disabled	
DynDNS	-	Disabled	
Dynamic	-	Disabled	
Firewall	-	Disabled	
Gateway	-	Disabled	

Here you have an overview of all TBF **hasync** status. In the first column you can see the hasync name, the status and the last sync date.

21.20.1 Actions

You can trigger a manual resync if hasync is enabled. On the top right corner you can also trigger a hasync for all enabled hasyncs.

Be aware that a sync starts with a slight delay and you might need to wait up to a minute to see the result.

21.21 Host Connections

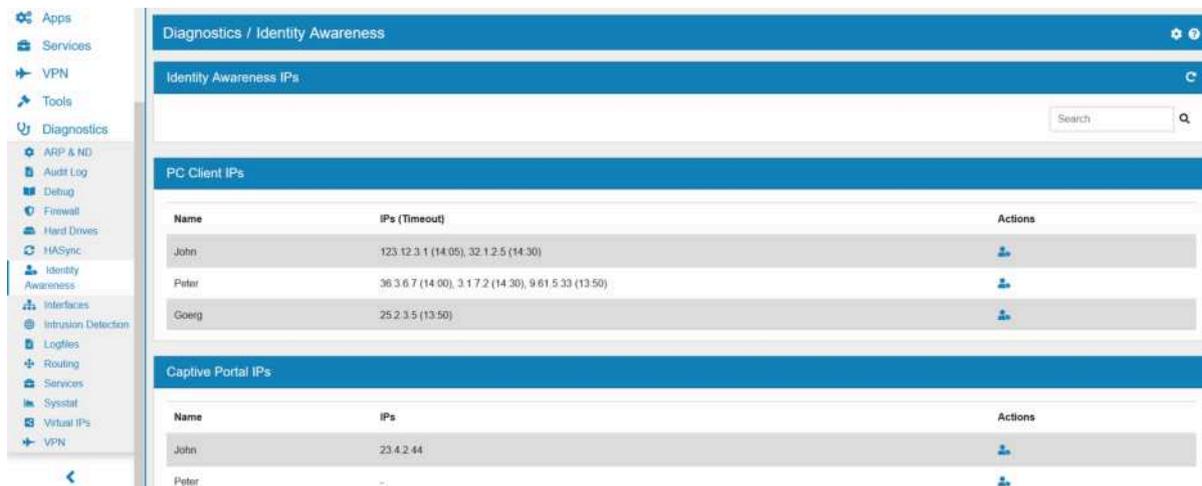
You can find the Host Connections Diagnostics at **Diagnostics** → **Firewall** → **Host Connections**.

Family	Type	VT AIR	Remote	Status
IPv4	TCP	192.168.10.110:22	192.168.6.122:59018	ESTABLISHED
IPv6	UTP	:::4500	-	NONE
IPv4	UTP	192.168.1.1:123	-	NONE
IPv6	TCP	:::53	-	LISTEN
IPv4	UTP	127.0.0.1:53001	-	NONE
IPv6	UTP	:::500	-	NONE
IPv6	TCP	:::443	-	LISTEN
IPv4	TCP	0.0.0.0:80	-	LISTEN
IPv4	TCP	0.0.0.0:53	-	LISTEN
IPv6	TCP	:::53	-	LISTEN

Here you can see all open connections to the TBF itself. Each connection shows the *IP Family*, *Type*, *TBF IP address**, *Remote IP address* and *Status*.

21.22 Identity Awareness

You can find the Identity Awareness Diagnostics at **Diagnostics** → **Identity Awareness**.



The screenshot displays the 'Diagnostics / Identity Awareness' page. It features a left-hand navigation menu with categories like Apps, Services, VPN, Tools, and Diagnostics. Under Diagnostics, various sub-items are listed, including ARP & ND, Audit Log, Debug, Firewall, Hard Drives, HASync, Identity Awareness (highlighted), Interfaces, Intrusion Detection, Logfiles, Routing, Services, Sysstat, Virtual IPs, and VPN. The main content area is titled 'Identity Awareness IPs' and includes a search bar. Below this, there are two sections: 'PC Client IPs' and 'Captive Portal IPs'. Each section contains a table with columns for Name, IPs (with timeout information), and Actions.

Name	IPs (Timeout)	Actions
John	123.12.3.1 (14:05), 32.1.2.5 (14:30)	[User Icon]
Peter	36.3.6.7 (14:00), 3.1.7.2 (14:30), 9.6.1.5.33 (13:50)	[User Icon]
Goetg	25.2.3.5 (13:50)	[User Icon]

Name	IPs	Actions
John	23.4.2.44	[User Icon]
Peter	-	[User Icon]

Here you can see all Identity Awareness IPs:

- PC Client IPs
- Captive Portal IPs
- AD IPs
- DHCP IPs

To change your Identity Awareness setup please go to **Authentication** → **Identity Awareness** and refer to the documentation at [Identity Awareness](#).

21.23 Interfaces

You can find the Interfaces Diagnostics at **Diagnostics** → **Interfaces** → **Interfaces**.

21.23.1 Interfaces



Diagnostics / Interfaces / Interfaces

Interfaces Usage

WAN (enp0s20f0)

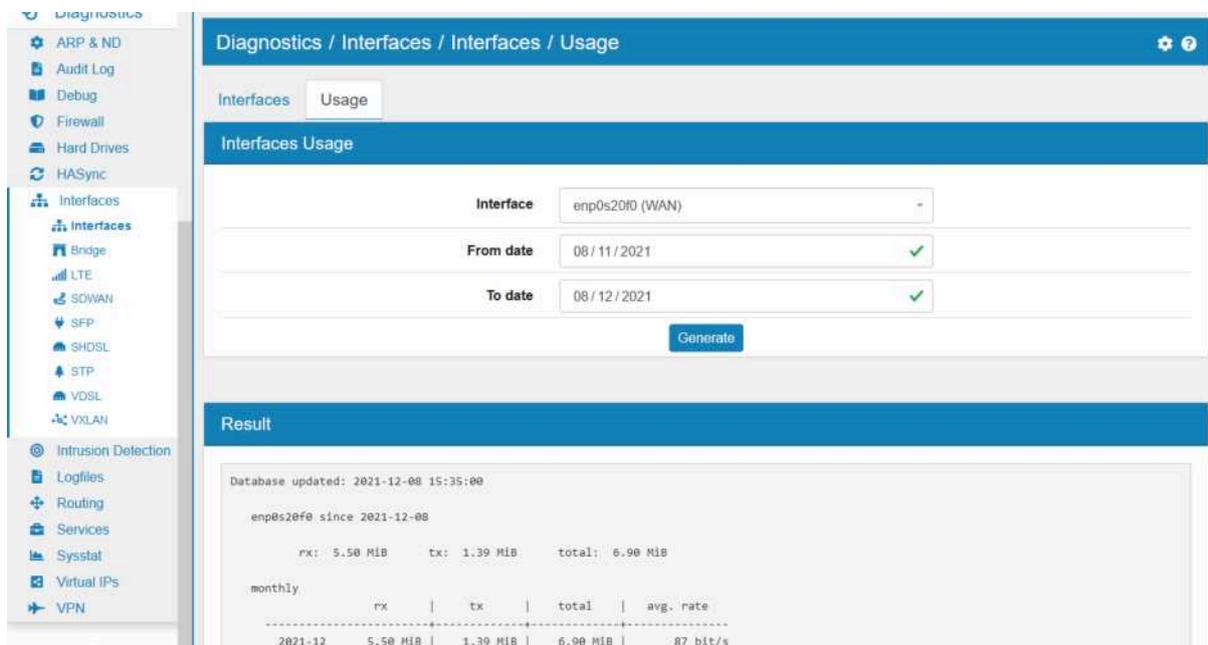
Status	UP
MAC Address	00:08:a2:09:c2:9a
IPv4 Address	192.168.10.110/24
IPv6 Address	fe80::208:a2ff:fe09:c29a:64
Broadcast Address	ff:ff:ff:ff:ff:ff
MTU	1500
In / out (bytes)	5823055 / 1839653 (5.55 MB / 1.75 MB)

Here you can see each interface with its current status, MAC address, IPv4 address, IPV6 address, broadcast Address, MTU and traffic.

The traffic is divided into *In* and *Out* as well as into bytes, packets, errors and drops.

To assign Interfaces please go to **Interfaces** → **Assign** and refer to the documentation at [Assign Interfaces](#).

21.23.2 Usage



Diagnostics / Interfaces / Interfaces / Usage

Interfaces Usage

Interface: enp0s20f0 (WAN)

From date: 08/11/2021 ✓

To date: 08/12/2021 ✓

Generate

Result

Database updated: 2021-12-08 15:35:00

enp0s20f0 since 2021-12-08

rx: 5.50 MiB tx: 1.39 MiB total: 6.90 MiB

monthly

	rx	tx	total	avg. rate
2021-12	5.50 MiB	1.39 MiB	6.90 MiB	87 bit/s

Here you can see the usage of each interface. Select an *Interface*, *From date* and *To date* and click on **Generate** to see the usage data.

The *Usage data* could look like this:

Database updated: 2021-12-08 15:35:00

enp0s20f0 since 2021-12-08

(continues on next page)

(continued from previous page)

	rx: 5.50 MiB	tx: 1.39 MiB	total: 6.90 MiB	
monthly				
	rx	tx	total	avg. rate
2021-12	5.50 MiB	1.39 MiB	6.90 MiB	87 bit/s
estimated	20.43 MiB	5.11 MiB	25.54 MiB	
daily				
	rx	tx	total	avg. rate
today	5.50 MiB	1.39 MiB	6.90 MiB	1.03 kbit/s
estimated	8.48 MiB	2.14 MiB	10.62 MiB	

21.24 Intrusion Detection

The diagnostics provide three tabs.

The *Overview* tab provides general information about memory usage and packet statistics.

The *Dashboard* tab provides an interactive view of the collected data from alerts and block events.

The *Security Logs* tab shows fast log matches for drop/reject events.

Note: The IDS engine might drop packets if they are too broken. In that case no rule id is present in the drop message.

The *Audit Logs* tab shows fast log matches for audit events.

The *Event Log* shows detailed information for each matched flow with protocol and application data associated with a flow or event. Source and destination IPs can show reverse DNS entry on hover, as long as the TBF can resolve the IP.

Diagnostics / Intrusion Detection				
Intrusion Detection				
Running Mode	Capture Mode	Uptime	Version	
workers	NFLOG	4714	4.1.2 RELEASE	
Work Queues				
Name	Packets	Drop	Bypassed	Invalid Cheksums
10	0	0	0	0

Work Queues

Name	Packets	Drop	Bypassed	Invalid Cheksums
10	0	0	0	0

Memcap

Stream	Stream-reassembly	Flow	Applayer-proto-http	Defrag	Ippair	Host
64mb	256mb	128mb	unlimited	32mb	16mb	32mb

Diagnostics / Intrusion Detection / Logs

Overview **Logs** Event Logs

Filter

Lines

Filter

Filter

Log

Time	Message	Classification	Source	Destination	Protocol	SID	Actions
07/03/2019-10:20:54	BAD TRAFFIC Non-Standard IP protocol	Detection of a non-standard protocol or event	81.7.16.52:123	192.168.10.130:53	UDP	1620	

Diagnostics / Intrusion Detection / Event Logs

Overview **Logs** Event Logs

Filter

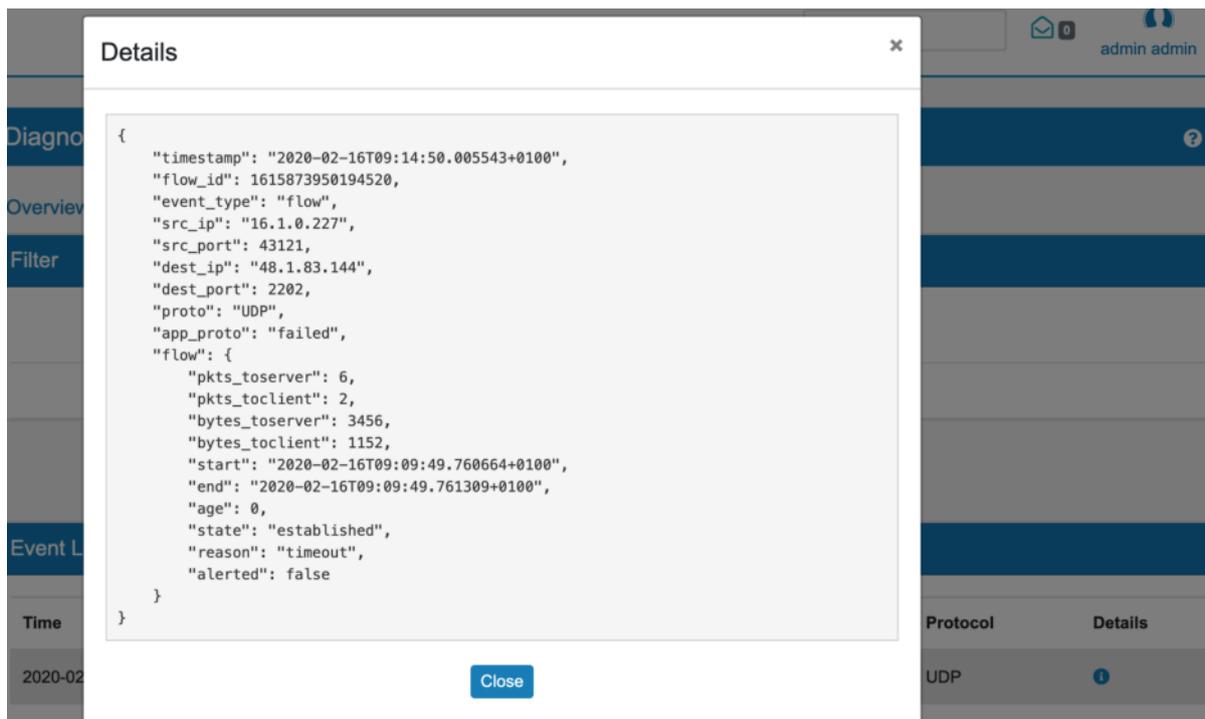
Lines

Filter

Filter

Event Log

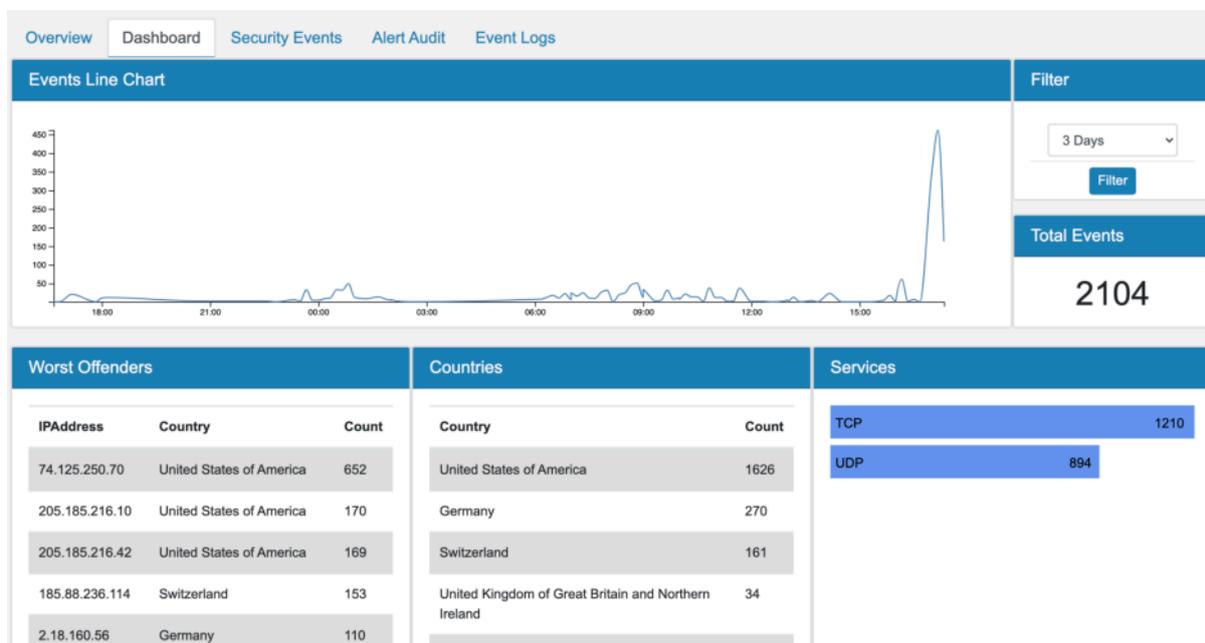
Time	Type	Source	Destination	Protocol	Details
2020-02-16 09:14:50	flow	16.1.0.227:43121	48.1.83.144:2202	UDP	

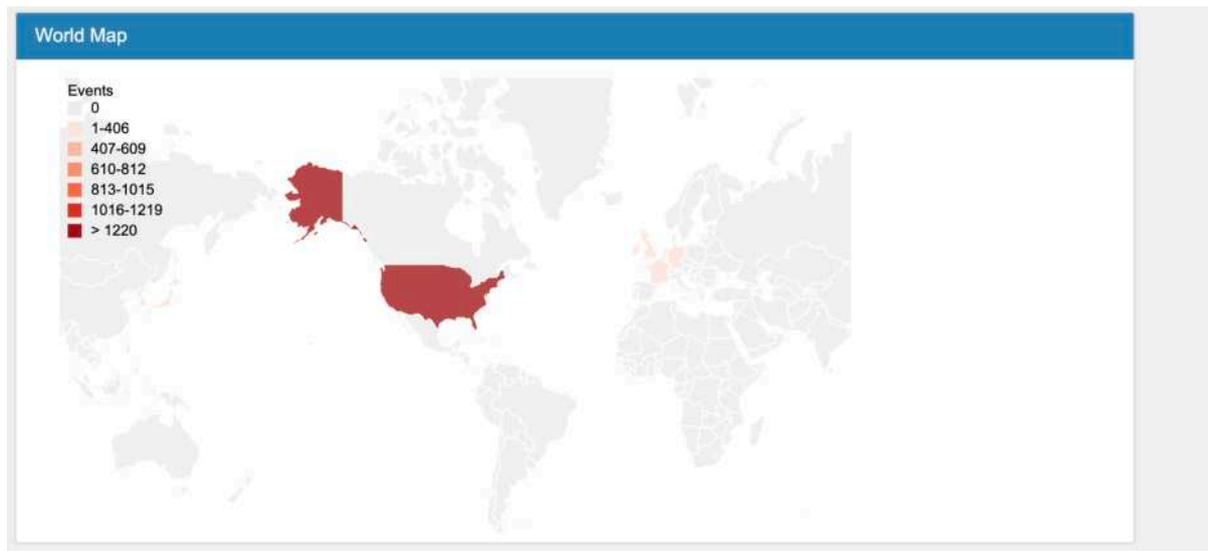


21.24.1 Intrusion Detection Dashboard

The dashboard shows you alert and block information by country and origin.

The dashboard is a convenient way of visualising the event data.





Note: Logfile Analysis needs to be enabled to see data in the Dashboard. It is disabled by default as it costs performance. It can be enabled at [Settings](#).

Security and Alert Notifications can be downloaded at the bottom of the Dashboard. They are also included in the Report Email.

21.25 IPsec

You can find the IPsec Diagnostics at **Diagnostics** → **VPN** → **IPsec**.

Name	Local	Remote	Algorithm	State	Established	Rekey	Actions
✓ West-Side (con1)	192.168.10.104	192.168.10.138	AES_CBC 128 / HMAC_SHA2_256_128 / MODP_4096	ESTABLISHED	4s ago	in 28603s	

Name	SPIs	Local	Remote	Algorithm	State	Installed	Rekey	Bytes In/Out	Actions
con1	Local: ce1423d Remote: cc80495c	10.10.112.1/32	10.10.111.1/32	AES_CBC 256 / HMAC_SHA2_256_128	INSTALLED	4s ago	in 3241s	0 B / 0 B	

Here you can see connection information about your **IPsec** setup. There is one **All** tab with all IPsec setups and each IPsec entry has also its own tab. The connection information is split up into **Phase1** and **Phase2**.

21.25.1 Phase1

The first column shows whether the entry is enabled or not.

Local and **Remote** display their corresponding IP addresses.

Reauth shows, when the next reauthentication is planned.

Algo lists the used encryption algorithms.

Status will be *Connected* or *Disconnected*.

At **Actions**, it's possible to manually start the connection or disconnect it, depending on the current status. There is also a **Log** symbol. When clicked, a window opens with detailed log information of the sepecific connection.

21.25.2 Phase2

All setup Phase2 will be listed here.

Local and **Remote** display their corresponding IP addresses.

SPIs shows a Security Parameter Index, which is an identification tag helpul for the kernel.

Rekey shows when a new key is negotiated.

Algo displays the used encryption algorithm. **Bytes In/Out** show the traffic.

At **Actions**, it's possible the manually disconnect the connection. There is also a **Log** symbol. When clicked, a window opens with detailed log information of the sepecific connection.

To change the IPsec setup please go to **VPN** → **IPSec** and refer to the documentation at [IPSec Phase 1](#).

21.25.3 IKEv2

There is one important aspect that affects IKEv2. The keys for the CHILD_SA that's implicitly created with the IKE_AUTH exchange will always be derived from the IKE keys even if PFS is configured. So if the peers disagree on whether to use PFS or not (or on the DH groups) it will not be known until the CHILD_SA is first rekeyed with a CREATE_CHILD_SA exchange (and fails). This is also the reason why you won't see a DH group in the status of the phase 2 until the SA is first rekeyed.

21.26 ISIS

You can find the ISIS Diagnostics at **Diagnostics** → **Routing** → **ISIS**.

The screenshot shows the 'Diagnostics / Routing / ISIS' page in a network management interface. The left sidebar contains a navigation menu with categories like Audit Log, Debug, Firewall, Hard Drives, HASync, Interfaces, Intrusion Detection, Logfiles, Routing (expanded), Services, Sysstat, and Virtual IPs. Under 'Routing', options include Gateways, Routes, MPLS, Dynamic, BFD, BGP, ISIS (selected), OSPF, and OSPFv6. The main content area has tabs for 'Summary' and 'Interfaces', with 'Summary' selected. The 'ISIS' section displays the following text:

```

vrf          : default
Process Id   : 37231
Up time     : 00:00:19 ago
Number of areas : 1
Area vtair:
TX counters per PDU type:
  LSP RXMT: 0
RX counters per PDU type:
Level-1:
  LSP0 regenerated: 0
  LSPs purged: 0
SPF:
  minimum interval : 1
IPv4 route computation:
  last run elapsed : 49w3d14h ago
  last run duration : 0 usec
  run count       : 0
  
```



Here you can see all information about your **Intermediate System to Intermediate System** setup.

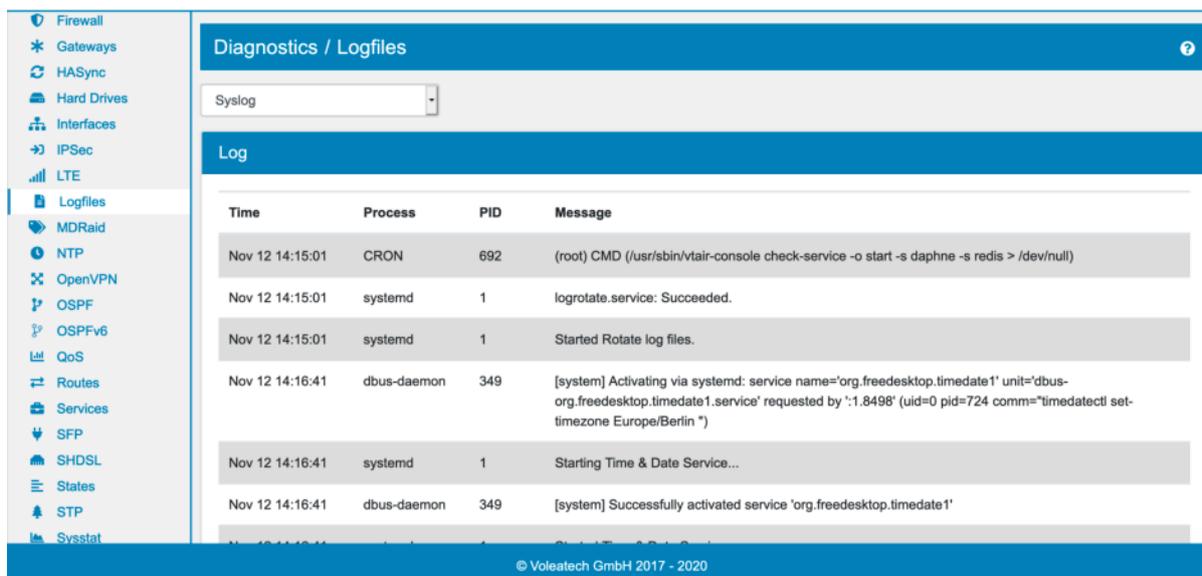
There are two tabs, one for a *ISIS Summary* and one for the *ISIS Interfaces*.

The information on the page are updated periodically without any user input.

To change your ISIS setup please go to **Routing** → **ISIS** and refer to the documentation at *ISIS*.

21.27 Logging

You can find the Logging Diagnostics at **Diagnostics** → **Logfiles**.



Here you can see all system logs divided into their service or category.

By default the last 50 entries of the logfile are displayed. If you click on **Realtime** you can see the latest log entries written into the log file in realtime.

21.27.1 Settings

At general settings the **Maximum Logfile Size in MB** for each file can be specified. The default is 5 MB and the number shouldn't be too high, else it could fill up the hard drive. The **Logfile Rotation** specifies the number of logfiles to keep before they get deleted.

Under **GUI Logging** the logging detail level of each TBF category can be adjusted. This will only affect the TBF GUI and Management logs.

You can also **Enable Auditlog Syslog** which will log all audit events to audit.log.

It's also possible to **Enable Remote Logging**. Multiple Syslog servers can be added with their ip address, port and protocol.

For TLS you need to set the **Certificate Authority** to use for checking the TLS connection to the Syslog server.

21.28 Cellular

You can find the Cellular Diagnostics at **Diagnostics** → **Interfaces** → **Cellular**.

Here you can see the current settings and status of your **Cellular** setup.

To change your Cellular setup please go to the Interface page of your Cellular at **Interfaces**.

Reception shows you data about the Cellular modems reception to the cell tower.

System Status shows you the current status of the Cellular modem.

The screenshot displays the Mikrotik WinBox interface for Cellular diagnostics. At the top, the breadcrumb is 'Diagnostics / Interfaces / Cellular'. Below this, the 'Cellular' section shows the interface 'ens22' selected. A 'Reconnect Cellular' button is visible. The 'Reception' section shows a red progress bar with the label 'Poor RA'. The 'System Status' section contains the following text:

```

IP Family: IPv4
IPv4 address: 10.153.168.145
IPv4 subnet mask: 255.255.255.252
IPv4 gateway address: 10.153.168.146
IPv4 primary DNS: 10.74.210.210
IPv4 secondary DNS: 10.74.210.211
MTU: 1500
Domains: none

HSDPA service:
  Status: 'limited'
  True Status: 'limited'
  Preferred data path: 'no'
  Domain: 'none'
  Service capability: 'cs-ps'
  Roaming status: 'on'
  Forbidden: 'yes'
  Location Area Code: '7318'
  Cell ID: '198145161'
  MCC: '262'
  MNC: '02'
  HS call status: 'hspa-hspa-unsupported'
  HS service: 'hspa-hspa-supported'
  Primary scrambling code: '095'
  Call broadcast support: 'off'
  Call barring status (CS): 'all-calls'
  Call barring status (PS): 'all-calls'
  Cipher Domain: 'none'

LTE service:
  Status: 'none'
  True Status: 'none'
  Preferred data path: 'no'
  SIM reject info: 'available'

Current:
  Network 'umts': '-108 dBm'
  RSSI:
  Network 'umts': '-108 dBm'
  ECID:
  Network 'umts': '-14.0 dBm'
  IO: '-106 dBm'
  SINR (R): '9.8 dB'
  
```

SIM Status shows the status of the SIM card and if it is locked.

```

SIM Status

Provisioning applications:
  Primary GW: slot '1', application '1'
  Primary IX: session doesn't exist
  Secondary GW: session doesn't exist
  Secondary IX: session doesn't exist
Slot [1]:
  Card state: 'present'
  UPIN state: 'not-initialized'
  UPIN retries: '0'
  UPUK retries: '0'
  Application [1]:
    Application type: 'usim (2)'
    Application state: 'ready'
    Application ID:
      A0:00:00:00:87:10:02:FF:49:94
    Personalization state: 'ready'
    UPIN replaces PIN1: 'no'
    PIN1 state: 'disabled'
    PIN1 retries: '3'
    PUK1 retries: '10'
    PIN2 state: 'enabled-not-verified'
    PIN2 retries: '3'
    PUK2 retries: '10'
Slot [2]:
  Card state: 'absent'
  UPIN state: 'not-initialized'
  UPIN retries: '0'
  UPUK retries: '0'

```

Channel Rates shows the theoretical maximum speed and the speed the Cellular modem negotiated with your provider.

```

Channel Rates

Current TX rate: 4294967295bps
Current RX rate: 4294967295bps
Max TX rate: 500000000bps
Max RX rate: 300000000bps

Packet

Connection status: 'connected'

TX packets OK: 113
RX packets OK: 113
TX packets dropped: 0
RX packets dropped: 0
TX bytes OK: 3164
RX bytes OK: 3164

```

Packet shows the statistics about the current open Cellular connection.

```

Current:
  Network 'lte': '-77 dBm'
RSSI:
  Network 'lte': '-77 dBm'
ECIO:
  Network 'lte': '-2.5 dBm'
IO: '-106 dBm'
SINR (8): '9.0 dB'
RSRQ:
  Network 'lte': '-10 dB'
SNR:
  Network 'lte': '6.6 dB'
RSRP:
  Network 'lte': '-106 dBm'

```

Cell Location Info.

```

Cell Location Info

Intrafrequency LTE Info
UE In Idle: 'no'
PLMN: '26201'
Tracking Area Code: '25510'
Global Cell ID: '28035538'
EUTRA Absolute RF Channel Number: '1300' (E-UTRA band 3; 1800+)
Serving Cell ID: '471'
Cell [0]:
  Physical Cell ID: '471'
  RSRQ: '-9.3' dB
  RSRP: '-108.1' dBm
  RSSI: '-69.3' dBm
Cell [1]:
  Physical Cell ID: '128'
  RSRQ: '-20.0' dB
  RSRP: '-113.9' dBm
  RSSI: '-82.7' dBm
Cell [2]:
  Physical Cell ID: '284'
  RSRQ: '-20.0' dB
  RSRP: '-112.7' dBm
  RSSI: '-82.8' dBm
Cell [3]:
  Physical Cell ID: '199'
  RSRQ: '-20.0' dB
  RSRP: '-115.4' dBm
  RSSI: '-82.7' dBm
Cell [4]:
  Physical Cell ID: '244'
  RSRQ: '-19.9' dB
  RSRP: '-113.8' dBm
  RSSI: '-82.7' dBm

```

21.28.1 LTE RSSI

Signal Quality	RSSI
Excellent	> -65
Good	-65 to -75
Fair	-75 to -85
Poor	< -85

21.28.2 LTE SINR

Signal Quality	SINR (db)
Excellent	> 12,5
Good	10 to 12,5
Fair	7 to 10
Poor	< 7

21.29 MDRaid

You can find the MDRaid Diagnostics at **Diagnostics** → **Hard Drives** → **MDRaid**.

MDRaid is the Software Raid used by TBF if you have two equal drives in your device at installation time. If you want to get email updates on drive failures please setup the email notification at [Notifications](#).

21.29.1 Info

This tab will print out the information about all mdraid disks and partitions and gives an overview of the current functionality.

21.29.2 Disks

This tab allows you to have a closer look at each disk and disk array. You can see the available partitions in each disk array and their health status as well as a general result of the disk array.

You have the ability to set partitions to faulty and/or to add a new disk in case of failure.

21.29.3 Copy Disk (Repair)

This tab is necessary if you need to replace a disk. The new disk needs the exact same disk layout as the old disk.

With this tool you can copy the disk layout from the working to the new disk.

21.29.4 Replace a disk

In case of a disk failure, you need to replace the faulty drive. Please go to **Disks** and make sure that the partitions on the faulty drive are set to faulty on all mdraid arrays.

Still on **Disks** remove the faulty partitions from all mdraid arrays.

The faulty drive is now properly removed from all mdraid arrays.

You now can shutdown the TBF and replace the disk with a new one. In case of a hot swap case, you can do this operation without shutting down TBF.

You now need to go to **Copy Disk (Repair)** and copy the partition table of the working disk onto the new disk. After this operation succeeded, you can go back to **Disks**.

You now need to add the corresponding partition on the new disk back to each mdraid array.

A resync operation will start after the adding was successful to sync all data to the new disk.

21.30 MPLS

You can find the MPLS Diagnostics at **Diagnostics** → **Routing** → **MPLS**.

Here you have an overview of all TBF **MPLS** as well as **LDP** diagnostics. They are all in the MPLS table that is shown here.

You can see the **lables** of each route, the **Gateway** it's using and whether it's using a **gateway**. The interface of the **MPLS** is shown as well.

To create your own MPLS routes please go to **Routing** → **MPLS** and refer to the documentation at [MPLS](#).

21.30.1 LDP

AF	Destination	Nextthop	Local Label	Remote Label	In Use
ipv4	192.168.1.0/24	0.0.0.0	imp-null	-	no
ipv4	192.168.10.0/24	0.0.0.0	imp-null	-	no

Here you have an overview of all four different **LDP** diagnostics:

- LDP Interface
- LDP Binding
- LDP Neighbor
- LDP Discovery

21.31 NTP

You can find the NTP Diagnostics at **Diagnostics** → **Services** → **NTP**.

remote	refid	st	t	when	poll	reach	delay	offset	jitter
212.18.3.18	.XFAC.	16	u	26h	512	0	0.000	0.000	0.000
129.70.132.32	.XFAC.	16	u	32h	512	0	0.000	0.000	0.000

To change the NTP setup please go to **Services** → **NTP** and refer to the NTP documentation at [NTP](#).

The output could look like this:

remote	refid	st	t	when	poll	reach	delay	offset	jitter
94.16.115.123	.XFAC.	16	u	11h	512	0	0.000	0.000	0.000
176.221.42.125	.XFAC.	16	u	6d	512	0	0.000	0.000	0.000

21.32 OpenVPN

You can find the OpenVPN Diagnostics at **Diagnostics** → **VPN** → **OpenVPN**.

The top screenshot shows the 'Server' tab for 'ovpn1'. The table below is as follows:

Name	State	Virtual Address	Service
ovpn1	CONNECTED	192.168.222.1	active

The bottom screenshot shows the 'Router Clients' tab. The table below is as follows:

Name	OVPN interface	State	Virtual Address	Local Address	Remote Host	Bytes Sent/Received	Service	Actions
client1	OVPN_test (ovpnc1)	CONNECTED	192.168.22.2	192.168.10.104.60721	192.168.10.138.1194	1488 B / 3392 B	active	Log

Here you can see information about your **OpenVPN** setup. All **OpenVPN Router Clients** are listed on one page while each **OpenVPN Servers** has its own separate page.

To change the OpenVPN setup please go to **VPN** → **OpenVPN** and refer to the documentation at [OpenVPN General](#).

21.32.1 Router Clients

All router clients configured in the TBF are listed here. The **State** shows whether a connection is established or not. The **Local Address** and **Virtual Address** display more information about the client, while the **Remote Host** displays the OpenVPN server the client is connected to. If a connection is successful, **Bytes Sent/Received** will show the traffic. In the **Service** column it's possible to start, stop or reload the service, depending on its current state. The **Actions** column has a **Log** symbol. When clicked, a window opens with detailed log information of the client.

21.32.2 Servers

All servers configured in the TBF are listed here. The **state** shows whether a connection is established or not and the **Virtual Address** displays the servers current IP address. In the **Service** column it's possible to start, stop or reload the service, depending on its current state.

The next table shows all to the server connected clients. At **Connected Since** you can see, whether they are connected or not. **Real address** shows their IP address and **Bytes Sent/Received** displays the traffic. **Cipher** shows which encryption algorithm is used. The **Actions** allow you to disconnect clients manually.

There is also a **Log** symbol. When clicked, a window opens with detailed log information of the server.

21.33 OSPF

You can find the OSPF Diagnostics at **Diagnostics** → **Routing** → **OSPF**.

Here you can see all information about your **Open Shortest Path First** setup. It's divided into *Summary*, *Routes*, *Neighbors*, *Database* and *Interfaces*.

The information on the page are updated periodically without any user input.

To change your OSPF setup please go to **Routing** → **OSPF** and refer to the documentation at [OSPF](#).

21.34 OSPFv6

You can find the OSPFv6 Diagnostics at **Diagnostics** → **Routing** → **OSPFv6**.

Here you can see all information about your **Open Shortest Path First v6** setup. It's divided into *Summary*, *Routes*, *Neighbors*, *Database* and *Interfaces*.

The information on the page are updated periodically without any user input.

To change your OSPF setup please go to **Routing** → **OSPFv6** and refer to the documentation at [OSPFv6](#).

21.35 QoS

You can find the QoS Diagnostics at **Diagnostics** → **Services** → **QoS**.

The screenshot displays the QoS configuration for the 'gretap1-out' interface. The configuration is as follows:

```

FireQoS 3.1.6
(C) 2013-2014 Costa Tsaousis, GPL

gretap1-out: gretap1 output => gretap1, type: , overhead:
Rate: 100000Kbit/s, min: 1000Kbit/s
Values in Kbit/s

CLASS synacks default
CLASSID 1:11 1:8000
COMMIT 1000 10000
MAX 100000 100000

PRIORIT 2 3
QDISC fq_code fq_code

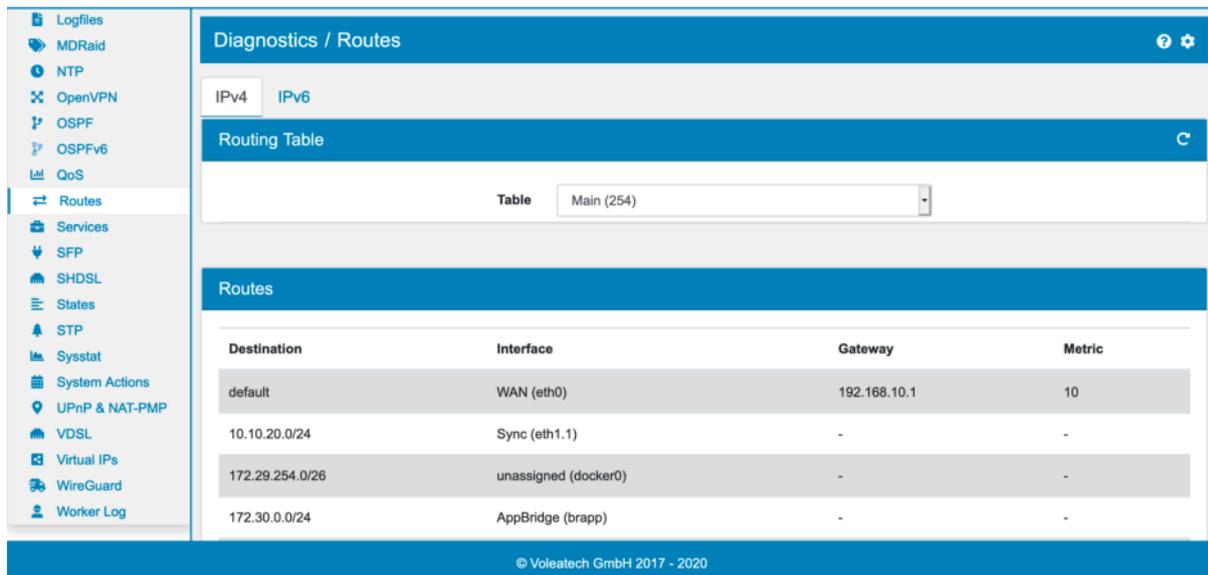
color code (packets): backlog | dropped | delayed | requested
Class Utilization on gretap1-out (gretap1 output => gretap1) - values in Kbit/s
TOTAL synacks default
0 - 0
- - -
0 - 0
  
```

Here you can see the current settings and status of your **QoS** setup. It is organized by Interface an Input or Output. You can only view one at a time.

To change your QoS setup please go to **Services** → **QoS** and refer to the documentation at [QoS](#).

21.36 Routes

You can find the Routes Diagnostics at **Diagnostics** → **Routing** → **Routes**.



Destination	Interface	Gateway	Metric
default	WAN (eth0)	192.168.10.1	10
10.10.20.0/24	Sync (eth1.1)	-	-
172.29.254.0/26	unassigned (docker0)	-	-
172.30.0.0/24	AppBridge (brapp)	-	-

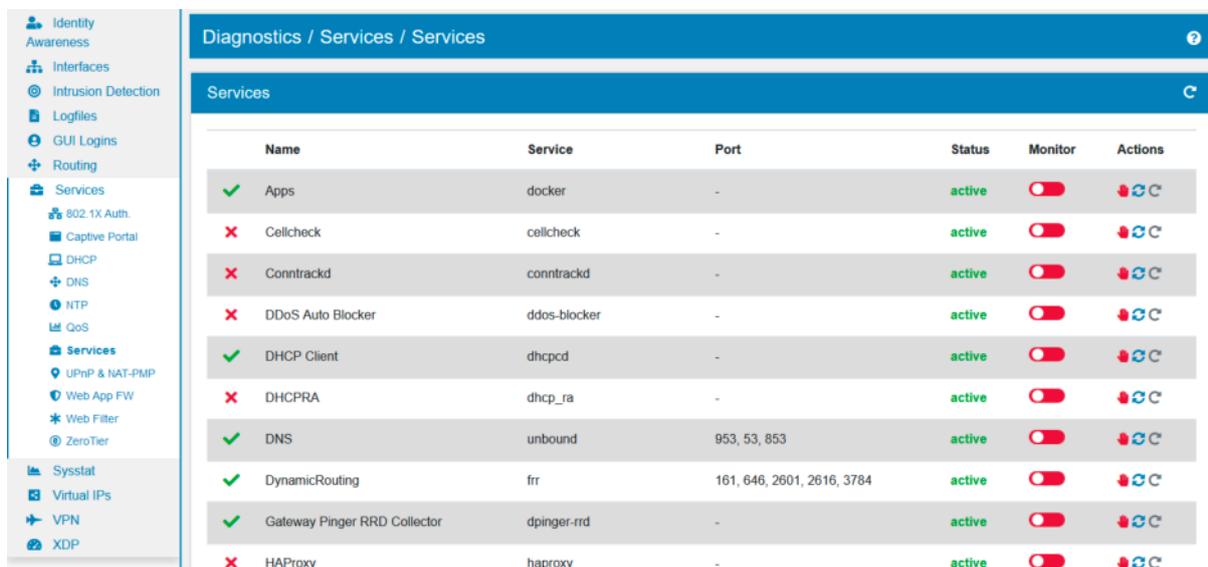
Here you have an overview of all TBF **routes**, divided into internet protocol v4 and v6. A **routing table** dropdown menu lets you display only the routes assigned to a selected routing table. By default the already existing system routes are listed.

You can see the **destination** of each route, the **interface** it's using and whether it's using a **gateway**. The **MTU** describes the *Maximum Transmission Unit* which is the size of the largest protocol data unit that can be communicated in a single network transaction. Some routes also have a numeric **priority**. The **Type** shows where the route is coming from, usual options are Static, OSPF, BGP.

To create your own routes please go to **Routing** → **Routes** and refer to the documentation at [Routes](#).

21.37 Services

You can find the Services Diagnostics at **Diagnostics** → **Services** → **Services**.



Name	Service	Port	Status	Monitor	Actions
✓ Apps	docker	-	active	<input checked="" type="checkbox"/>	
✗ Cellcheck	cellcheck	-	active	<input checked="" type="checkbox"/>	
✗ Conntrackd	conntrackd	-	active	<input checked="" type="checkbox"/>	
✗ DDoS Auto Blocker	ddos-blocker	-	active	<input checked="" type="checkbox"/>	
✓ DHCP Client	dhcpcd	-	active	<input checked="" type="checkbox"/>	
✗ DHCPRA	dhcp_ra	-	active	<input checked="" type="checkbox"/>	
✓ DNS	unbound	953, 53, 853	active	<input checked="" type="checkbox"/>	
✓ DynamicRouting	frr	161, 646, 2601, 2616, 3784	active	<input checked="" type="checkbox"/>	
✓ Gateway Pinger RRD Collector	dpinger-rrd	-	active	<input checked="" type="checkbox"/>	
✗ HAProxy	haproxy	-	active	<input checked="" type="checkbox"/>	

Here you have an overview of all TBF **services**. In the first column you can see if the service itself is **enabled** or **disabled**. The next columns show the TBF service name, the system name as well which ports are used by the service. Be aware that the ports are not open to the world unless there is a firewall rule defined.

21.37.1 Status

The status can be one of the following:

- active
- reloading
- inactive
- failed
- activating
- deactivating

21.37.2 Monitor

Here you can check a service if you want, the service to get monitored by the system. The system will then check on a regular basis the status of the service and restarts it if it's not running.

21.37.3 Actions

You can do different actions, depending on the status of the service. If the service status is inactive or failed, you have the ability to **start** the service. If the status is active, reloading, activating or deactivating, you can **stop** or **reload** the service.

21.38 SFP

You can find the SFP Diagnostics at **Diagnostics** → **Interfaces** → **SFP**.

The screenshot shows the SFP diagnostics interface. On the left is a navigation menu with options like Logfiles, MDRAID, NTP, OpenVPN, OSPF, OSPFv6, QoS, Routes, Services, SFP, SHDSL, States, STP, Sysstat, System Actions, UPnP & NAT-PMP, VDSL, Virtual IPs, WireGuard, and Worker Log. The main content area is titled 'SFP' and has a dropdown menu for 'Interface' set to 'eth2'. Below this is a 'Result' section containing a list of SFP parameters and their values:

```

Identifier : 0x03 (SFP)
Extended identifier : 0x04 (GBIC/SFP defined by 2-wire interface ID)
Connector : 0x07 (LC)
Transceiver codes : 0x00 0x00 0x00 0x01 0x20 0x40 0x0c 0x00 0x00
Transceiver type : Ethernet: 1000BASE-SX
Transceiver type : FC: intermediate distance (I)
Transceiver type : FC: Shortwave laser w/o OFC (SN)
Transceiver type : FC: Multimode, 62.5um (M6)
Transceiver type : FC: Multimode, 50um (M5)
Encoding : 0x03 (NRZ)
BR, Nominal : 1300MBd
Rate identifier : 0x00 (unspecified)
Length (SMF,km) : 0km
Length (SMF) : 0m
Length (50um) : 550m
Length (62.5um) : 270m
Length (Copper) : 0m

```

At the bottom of the interface, there is a copyright notice: © Voleatech GmbH 2017 - 2020.

Here you can see all **Small Form-factor Pluggable** information. You can select the desired interface to get the information.

There is pre filtering for the interfaces. Please make sure you select the correct SFP interface to see the information.

21.39 SHDSL

You can find the SHDSL Diagnostics at **Diagnostics** → **Interfaces** → **SHDSL**.

Here you can see the current settings and status of your **SHDSL** setup.

To change your SHDSL setup please go to **Interfaces** → **Assign** → **SHDSL** and refer to the documentation at [SHDSL](#).

21.39.1 Output

You can see the current *configuration* that is active, the *status* if the modem is connected and the connection data (PAM/Speed/SNRM/LATN).

The screenshot shows a web interface for SHDSL diagnostics. At the top, there is a blue header with the text "Diagnostics / SHDSL / View". Below this, there is a tab labeled "dsl1". Underneath the tab is another blue header with the text "Current Settings". The main content area displays a table of settings and their status.

	configured	active
- enabled:	yes	yes
- line:	1	1
- master line:	1	1
- mode:	C0	C0
- tclayer:	EFM	EFM
- pam:	auto	auto
- rate:	auto	auto
- ratemode:	extended	extended
- snrm:	6 dB	6 dB
- threshold:	4 dB	4 dB
- annex:	ANNEX_A	ANNEX_A
- ef:	on	on
- testmode:	off	off
- iop:	0x00000000	0x00000000

You can also see all performance counter like CRC errors. NE is always the local errors and FE the foreign errors if available.

The different counters are:

- SNRM – Signal to Noise Margin
- LATN – Line Attenuation
- PBO – Power Back-off
- ES – Errored Seconds

- SES – Severe ES
- AUS – UnAvailable Seconds
- LOSW – Loss Of SyncWord
- CRCa – Cyclic Redundancy Check

Clear Stats allows you to reset the performance counter.

Status

Linestate: DOWN_NOT_READY
 Mode: STU-C (CO)

SHDSL performance counter of line #1

SNRM(NE):	0 dB	SNRM(FE):	0 dB
LATN(NE):	0 dB	LATN(FE):	0 dB
PBO (NE):	0 dB	PBO (FE):	0 dB
ES (NE):	0	ES (FE):	0
SES (NE):	0	SES (FE):	0
UAS (NE):	0	UAS (FE):	0
LOSW(NE):	0	LOSW(FE):	0
CRCa(NE):	0	CRCa(FE):	0

Clear Stats

21.40 States

You can find the States Diagnostics at **Diagnostics** → **Firewall** → **States**.

- VPN
- Tools
- Diagnostics
 - ARP & ND
 - Audit Log
 - Debug
 - Firewall
 - Firewall
 - DDoS
 - DNS Domain
 - States**
 - Host Connections
 - Hard Drives
 - HASync
 - Identity Awareness
 - Interfaces
 - Intrusion Detection
 - Logfiles
 - GUI Logins
 - Routing
 - Services
 - Sysstat
 - Virtual IPs
 - VPN

Diagnostics / Firewall / States

States
External States
Reset States

States

Number of States

State Direction

Protocol

Source Address

Destination Address

Filter

States (48/48)

Protocol	TTL (Age)	Source (Original) → Destination (Original)	Packets Src/Dst	Bytes Src/Dst	Status	
TCP (SYN SENT)	91 sec	192.168.10.110:45937 → 1.3.3.124:80	1 / 0	60.0 B / 0B	UNREPLIED	✕
TCP (SYN SENT)	89 sec	192.168.10.110:51116 → 1.3.3.124:80	1 / 0	60.0 B / 0B	UNREPLIED	✕

Here you can see all current network **States**. If you have *States Sync of High Availability* enabled, you can also see the **External States**.

External States are the states that were synchronized from the other firewalls. They will stay in the **External States** status until the firewall assumes the Master role on all VIPs. The states will then be merged into the normal **States**.

Each entry shows which **Protocol** it uses, for example *TCP*, *UDP* or *ICMP*. The **TTL** is the *Time to Live* and limits the lifespan of the state. The **Source** and **Destination** column shows the IP address. If some kind of address translation was used, like NAT for example, the **Original** address is displayed in parenthesis.

You can see how many packets are processed within a state by **Packets Src/Dst** and **Bytes Src/Dst**. It allows you to see how many data are going through an open state.

Last but not least the **Status**. A button lets you also delete the network state from the system.

You can filter the states by port and ipaddress in the original or replt direction. By default the first 10.000 states are shown. You can select to show more states. Be aware, that it might take a long time to show all states if you have more than 100.000 state entries.

It's also possible to **Reset all States**. This will break all open connections! They will have to be re-established, which can take some time. This may also cause the browser session to appear hung. In this case, please refresh the page to continue.

21.40.1 State Actions

Each state has actions connected to it on the right side of the state entry. You can always *delete* a state.

If a state can be associated with a firewall rule, you have the option to go to the rule directly via the rule symbol.

States (29/29)						
Protocol	TTL (Age)	Source (Original) → Destination (Original)	Packets Src/Dst	Bytes Src/Dst	Status	
TCP (TIME WAIT)	65 sec	192.168.10.112:36338 → 18.195.174.247:443	16 / 14	2.13 KB / 6.29 KB	ASSURED	
TCP (TIME WAIT)	40 sec	192.168.10.112:50846 → 192.168.10.26:443	16 / 12	2.42 KB / 5.55 KB	ASSURED	
ICMP	29 sec	192.168.10.112 → 192.168.10.1	854956 / 854956	22.83 MB / 22.83 MB	-	
TCP (TIME WAIT)	84 sec	192.168.10.112:36340 → 18.195.174.247:443	16 / 13	2.13 KB / 6.25 KB	ASSURED	
TCP (ESTABLISHED)	431967 sec	192.168.232.2:56439 → 192.168.10.112:22	428 / 310	30.68 KB / 66.34 KB	ASSURED	 

21.41 STP

You can find the STP Diagnostics at **Diagnostics** → **Interfaces** → **STP**.

The screenshot shows the 'Diagnostics / STP' page. The left sidebar contains a navigation menu with items like Logfiles, MDRaid, NTP, OpenVPN, OSPF, OSPFv6, QoS, Routes, Services, SFP, SHDSL, States, STP, Sysstat, System Actions, UPnP & NAT-PMP, VDSL, Virtual IPs, WireGuard, and Worker Log. The main content area has tabs for Bridge, Tree, Port, MSTIs, MST Conf. ID, VID-to-FID, and FID-to-MSTID. The 'Bridge' tab is selected, and a dropdown menu shows 'br0'. Below this is a 'Result' section displaying the following STP information for bridge br0:

```
br0 CIST info
enabled          yes
bridge id       7.000.4E:3F:14:88:58:E6
designated root 7.000.4E:3F:14:88:58:E6
regional root  7.000.4E:3F:14:88:58:E6
root port      none
path cost      0          internal path cost  0
max age        20          bridge max age      20
forward delay  15          bridge forward delay 15
tx hold count  6          max hops             20
hello time     2          ageing time          300
force protocol version rstp
```

© Voleatech GmbH 2017 - 2020

Here you can see all **Spanning Tree Protocol** information. It's divided into *Bridge*, *Tree*, *Port*, *MSTIs*, *MST Conf. ID*, *VID-to-FID* and *FID-to-MSTID*. You can select the desired bridge to get the information.

To revisit your bridges STP settings please go to **Interfaces** → **Assign** → **Bridges** and refer to the Bridge documentation at [Bridge](#).

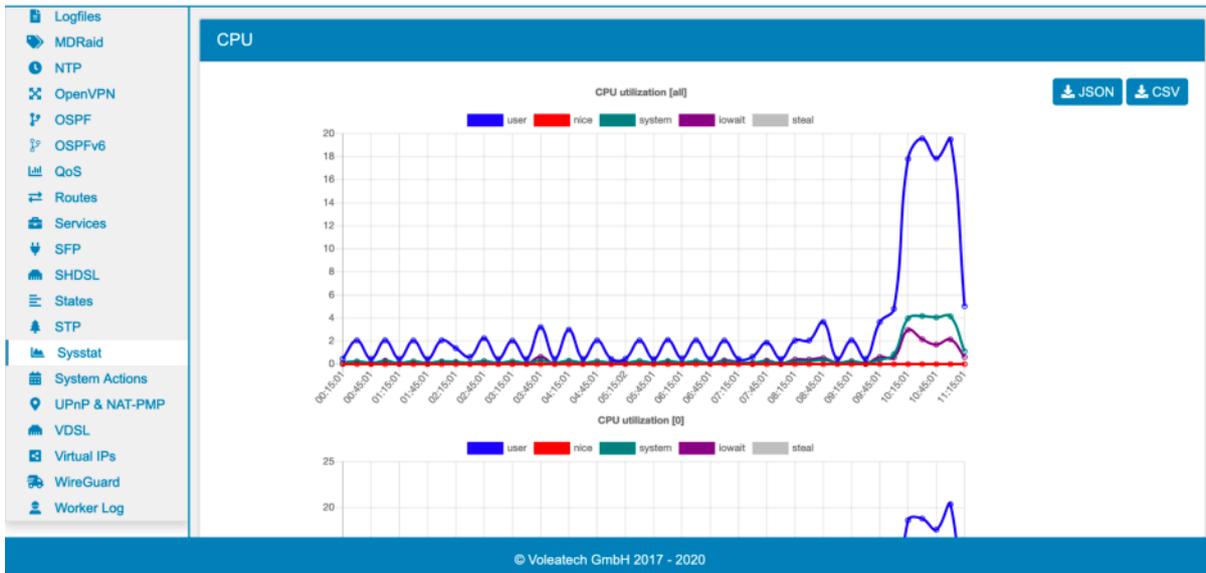
21.42 Sysstat

You can find the Sysstat Diagnostics at **Diagnostics** → **Sysstat**.

The screenshot shows the 'Diagnostics / Sysstat' page. The left sidebar is the same as in the previous screenshot. The main content area has tabs for System and Network. The 'System' tab is selected. Below the tabs is an 'Options' section with a 'Date' field set to '12' and 'Save' and 'Cancel' buttons. Below this is a 'Memory' section with a line graph titled 'Memory utilization' showing '% Memory used' over time. The y-axis ranges from 66.0 to 67.0. The graph shows a fluctuating line that generally trends upwards. There are 'JSON' and 'CSV' download buttons in the top right corner of the graph area. © Voleatech GmbH 2017 - 2020

Here you can see information graphics about your *CPU*, *Memory*, *I/O* and *Network* usage.

The data of each category can be downloaded as *JSON* or *CSV* format.



You can choose a **date** to show for the graphs. The data is kept in a rotation for a month per date. You can always choose between the 1st and the last day of the month and if the current month has not reached a day it is filled with data from the previous month.

On the *Network* tab you can also choose to show data for **all** or a **single** interface.

21.43 System Actions

You can find the System Actions Diagnostics at **Diagnostics** → **Debug** → **System Actions**.

The screenshot shows the 'System Actions' page with a table listing various actions. The table has four columns: Name, Last Run, Next Run, and Actions. The data is as follows:

Name	Last Run	Next Run	Actions
copyright	2020-11-11 20:08	2020-11-12 19:08	▶
letsencrypt	2020-11-12 02:08	2020-11-13 02:00	▶
licence	2020-11-12 02:08	2020-11-13 02:00	▶
auditlog_clear	2020-11-12 02:08	2020-11-13 02:00	▶
dyndns	2020-11-12 02:08	2020-11-13 02:00	▶
squidproxysalla	2020-11-11 19:08	2020-11-12 18:08	▶

System Actions are like cron jobs but executed in the management process of the TBF. You can trigger them manually on this page or see their last and next runtime.

21.44 UPNP NAT

You can find the UPNP NAT Diagnostics at **Diagnostics** → **Services** → **UPNP NAT**.

Here you can see all UPNP NAT entries that are added to the firewall. Each entry represents a port forward to a client.

The entries are split between **IPv4** and **IPv6**

21.45 VDSL

You can find the VDSL Diagnostics at **Diagnostics** → **Interfaces** → **VDSL**.

Current Settings

```

version=1.1
state=running
multiplex=0
vci=32
vpi=1
dsl_startmode=1
lan_ipv4=10.10.10.1
lan_vlan=0
revision=00
type=00
annex=A

```

Status

Line State	UP
Line Uptime	125 seconds
Profile	17a
Power Mode	L0 - Synchronized
Temperature (max. 125C)	81.0 C

The screenshot displays the VDSL configuration interface. On the left is a navigation menu with various system settings. The main content area is divided into two sections: 'Line Data' and 'Errors'.

Line Data section:

	Down	Up
Data Rate	63.67 Mb/s	12.73 Mb/s
Latency (Interleave Delay)	13 ms	0 ms
Line Attenuation (LATN)	15.6 dB	16.4 dB
Signal Attenuation (SATN)	15.6 dB	16.3 dB
Noise Margin (SNR)	18.5 dB	27.6 dB
Aggregate Transmit Power (ACTATP)	8.4 dB	5.0 dB
Max. Attainable Data Rate (ATTNDR)	108.0 Mb/s	40.53 Mb/s

Errors section:

	Near	Far
Forward Error Correction Seconds (FECS)	0	16
Errored seconds (ES)	0	2
Severely Errored Seconds (SES)	0	0
Loss of Signal Seconds (LOSS)	0	0
Unavailable Seconds (UAS)	162	162
Header Error Code Errors (HEC)	0	0
Non Preemptive CRC errors (CRC_P)	0	0
Preemptive CRC errors (CRCP_P)	0	0

Here you can see the current settings and status of your **VDSL** setup.

To change your VDSL setup please go to **Interfaces** → **Assign** → **VDSL** and refer to the documentation at [VDSL](#).

Current Settings shows you the current setup of the VDSL modem.

Status shows the *Line State*, *Line Uptime*, *Profile*, *Power Mode* and *Temperature*.

Line Data shows the *Data Rate*, *Latency (Interleave Delay)*, *Line Attenuation (LATN)*, *Signal Attenuation (SATN)*, *Noise Margin (SNR)*, *Aggregate Transmit Power (ACTATP)* and *Max. Attainable Data Rate (ATTNDR)*.

Errors shows the *Forward Error Correction Seconds (FECS)*, *Errored seconds (ES)*, *Severely Errored Seconds (SES)*, *Loss of Signal Seconds (LOSS)*, *Unavailable Seconds (UAS)*, *Header Error Code Errors (HEC)*, *Non Preemptive CRC errors (CRC_P)* and *Preemptive CRC errors (CRCP_P)*.

21.46 Virtual IPs

You can find the Virtual IPs Diagnostics at **Diagnostics** → **Virtual IPs**.

The screenshot shows the 'Diagnostics / Virtual IPs' page. The left sidebar contains a navigation menu with items like Logfiles, MDRaid, NTP, OpenVPN, OSPF, OSPFv6, QoS, Routes, Services, SFP, SHDSL, States, STP, Sysstat, System Actions, UPnP & NAT-PMP, VDSL, Virtual IPs, WireGuard, and Worker Log. The main content area is divided into three sections:

- VRRP Status:** Shows the current state as 'master' in green. Below it are two buttons: 'Enable Maintenance Mode' and 'Enable Force Master'.
- VRRP Virtual IPs:** A table with columns: Interface, IP Address, Priority, Description, and State.

Interface	IP Address	Priority	Description	State
WAN	1.2.3.4/32	100	-	active
- Alias Virtual IPs:** This section is currently empty.

At the bottom of the page, there is a copyright notice: © Voleatech GmbH 2017 - 2020.

Here you can see the current settings and status of your **Virtual IPs** setup.

At the top the **VRRP Status** is displayed. There are two buttons, one to enable or disable *Maintenance Mode* and one to enable or disable *Force Master*. You can only have *Maintenance Mode* or *Force Master* enabled at any time.

You can also see the **VRRP Virtual IPs** and **Alias Virtual IPs** with their current system state.

To change your Virtual IPs setup please go to **General** → **Virtual IPs** and refer to the documentation at [VRRP](#).

21.46.1 Maintenance Mode

If you activate the maintenance mode the VRRP ID of all IPs is set to 1, the lowest ID possible. In turn the TBF will become Slave if any other device is available in the network that also has the VRRP IPs configured. This though also means that the TBF will still be master if it is the **ONLY** device left that has the VRRP IPs configured.

The maintenance mode option will be persistent also after reboots until you turn it back off manually.

Use it to do maintenance on the TBF, test the High Availability failover or do updates.

21.46.2 Force Master

If you activate the force master mode the VRRP ID of all IPs is set to 255, the highest ID possible. In turn the TBF will become Master if any other device is available in the network that also has the VRRP IPs configured.

The force master mode option will be persistent also after reboots until you turn it back off manually.

Use it to take over the Master role on the TBF, in case of emergencies or problems.

21.47 VRF

You can find the VRF Diagnostics at **Diagnostics** → **Interfaces** → **VRF**.

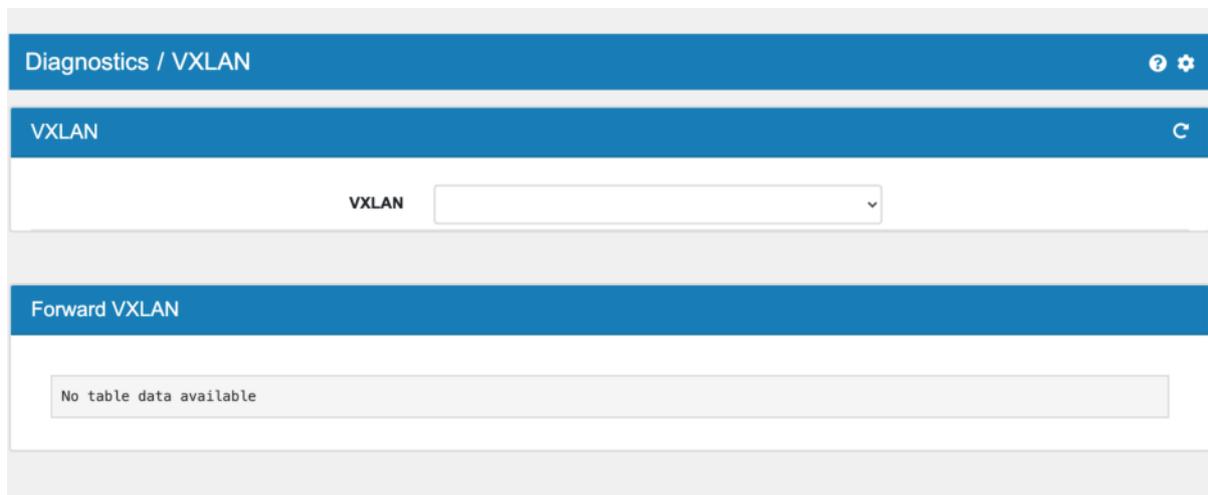


Here you can see all **VRF** information. You can select the desired VRF to get the information.

To revisit your VRF settings please go to **Interfaces** → **Assign** → **VRF** and refer to the VRF documentation at [VRF](#).

21.48 VXLAN

You can find the VXLAN Diagnostics at **Diagnostics** → **Interfaces** → **VXLAN**.



Here you can see all **VXLAN** Forward entry information. You can select the desired vxlan to get the information.

To revisit your VXLAN settings please go to **Interfaces** → **Assign** → **VXLAN** and refer to the VXLAN documentation at [VXLAN](#).

21.49 Web Filter

You can find the Web Filter Diagnostics at **Diagnostics** → **Services** → **Web Filter**.

Here you can see all information about your **Web Filter** setup. It's divided into *Access Log*, *Clamav Log*, *I-Cap Log* and *I-Cap Stats*.

The information on the page are updated periodically without any user input.

To change your Web Filter setup please go to **Services** → **Web Filter** and refer to the documentation at *Web Filter*.

Access Log shows the live information about who is accessing the proxy server as well as related information about the status of requests and replies. You can filter the access log via the search field.

Clamav Log shows the clamav anti virus log file content.

Diagnostics / Web Filter / Clamav Log	
Access Log	Clamav Log
I-Cap Log	I-Cap Stats
Clamav Log	
Time	Message
Wed Nov 4 10:35:27 2020	+++ Started at Wed Nov 4 10:35:27 2020
Wed Nov 4 10:35:27 2020	Received 0 file descriptor(s) from systemd.
Wed Nov 4 10:35:27 2020	clamd daemon 0.102.4 (OS: linux-gnu, ARCH: aarch64, CPU: aarch64)
Wed Nov 4 10:35:27 2020	Running as user clamav (UID 117, GID 124)
Wed Nov 4 10:35:27 2020	Log file size limited to 4294967295 bytes.
Wed Nov 4 10:35:27 2020	Reading databases from /var/lib/clamav
Wed Nov 4 10:35:27 2020	Not loading PUA signatures.

I-Cap Log shows the I-Cap log file content which also shows found Virus alerts.

Diagnostics / Web Filter / I-Cap Log

Access Log Clamav Log **I-Cap Log** I-Cap Stats

I-Cap Log

Time	Message
Wed Nov 4 12:23:25 2020	Error opening control socket Permission denied: /var/run/c-icap/c-icapctl. Fatal error exiting!
Wed Nov 4 12:24:05 2020	Create shared mem qsize=20 stat_block_size=560 childshared data:1120
Wed Nov 4 12:24:05 2020	Command stop registered
Wed Nov 4 12:24:05 2020	Command reconfigure registered
Wed Nov 4 12:24:05 2020	Command dump_statistics registered
Wed Nov 4 12:24:05 2020	pool hits:0 allocations: 3
Wed Nov 4 12:24:05 2020	Geting buffer from pool 992:15

I-Cap Stats shows the I-Cap stats. Including *Running Servers Statistics*, *General Statistics*, *Service info Statistics*, *Service echo Statistics* and *Service squidclamav Statistics*.

Diagnostics / Web Filter / I-Cap Stats

Access Log Clamav Log I-Cap Log **I-Cap Stats**

I-Cap Stats

```
ICAP server:127.0.0.1, ip:127.0.0.1, port:1344

Running Servers Statistics
=====
Children number: 3
Free Servers: 29
Used Servers: 1
Started Processes: 3
Closed Processes: 0
Crashed Processes: 0
Closing Processes: 0

Child pids: 3411 3412 3413
Closing children pids:
Semaphores in use
  file:/tmp/icap_lock_accept.yg2XJx
  file:/tmp/icap_lock_children-queue.6RpJhV
```

21.50 Web Application Firewall

You can find the Web Application Firewall Diagnostics at **Diagnostics** → **Services** → **Web App FW**.

Time	Client	Host	Message	URI	Details
2023-08-25 06:33	192.168.232.2	192.168.10.116	Path Traversal Attack (/./) or (/../)	/login/?next=/_./etc/passwd	Details
2023-08-25 06:33	192.168.232.2	192.168.10.116	OS File Access Attempt	/login/?next=/_./etc/passwd	Details

The diagnostics provide two tabs.

The *Overview* tab provides general information like the used rules version.

The *Audit Log* shows detailed information for each triggered rule. Each log entry has Time, Client, Host, Message and URI as well as a details button the right side to show even more pieces of information.

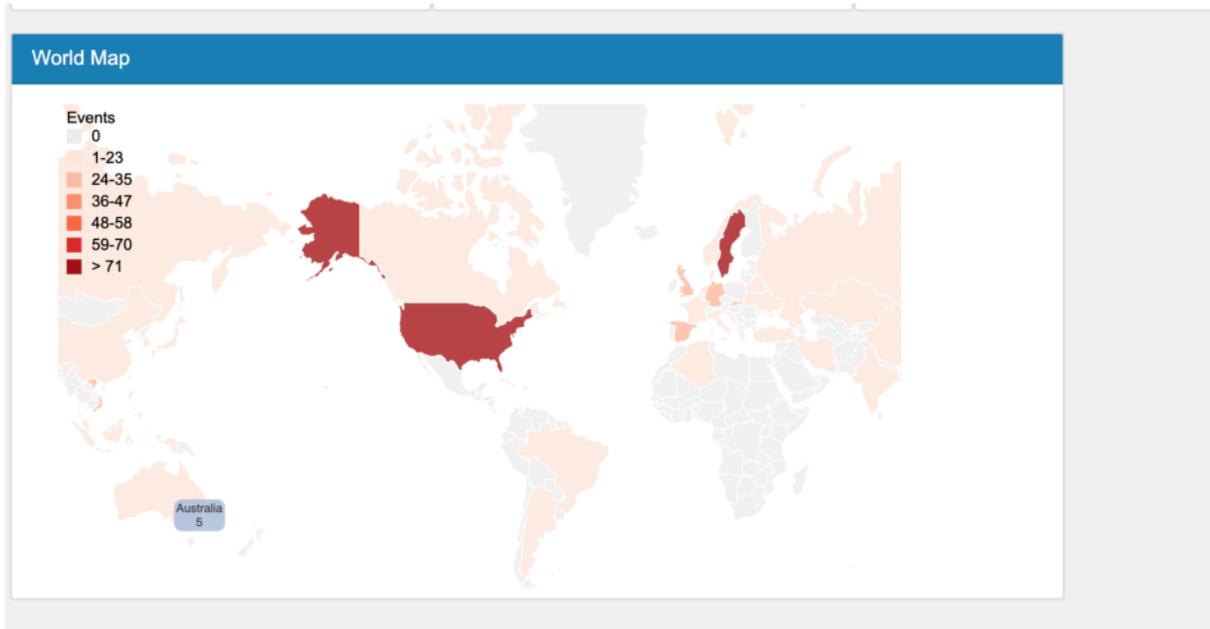
21.50.1 WAF Dashboard

The dashboard shows you web application firewall information by country and origin.

The dashboard is a convenient way of visualising the event data.

IPAddress	Country	Count
165.231.130.135	Sweden	28
196.196.148.182	Spain	13
165.231.133.12	Sweden	12
196.245.186.182	Norway	12
196.245.186.189	Norway	11

Country	Count
United States of America	95
Sweden	84
Slovakia	33
Viet Nam	28
Spain	27



Note: Logfile Analysis needs to be enabled to see data in the Dashboard. It is disabled by default as it costs performance. It can be enabled at [Settings](#).

21.51 WireGuard

You can find the WireGuard Diagnostics at **Diagnostics** → **VPN** → **WireGuard**.

Diagnostics / WireGuard / View

WireGuard

Name	Listening Port	Public Key	State
✓ WireGuard	-	-	failed

Peers

Name	IPs	Transfer	Keep Alive Time	Public Key
✗ Site2Site	192.168.100.2/32, 192.168.1.0/24	-	30 seconds	qDUQEUn4DvkzgXHWIPwXgAA+hbVgSQou4P/ITDxOLDo=

© Voleatech GmbH 2017 - 2020

Here you can see information about your **WireGuard** setup.

To change the WireGuard setup please go to **VPN** → **WireGuard** and refer to the documentation at [WireGuard](#).

All *WireGuards* configured in the TBF are listed here.

Name shows the configured name of the selected *WireGuard*. **Listening Port** is the port on which connections are received. **Public Key** is a shortened string of the public key. **State** shows the current state of the service.

The next table shows all to the peers.

The first column shows a symbol, whether the peer is **Connected** or **Not Connected**. **IPs** are all allowed IPs by the peer. **Transfer** shows how much data was received and sent by this peer. **Keep Alive Time** shows in seconds how long the connection is kept alive. **Public Key** is a shortened string of the public key.

21.52 Worker Log

You can find the Worker Log at **Diagnostics** → **Debug** → **Worker Log**.

The screenshot shows the 'Diagnostics / Debug / Worker Log' page. The left sidebar contains navigation options like 'Main', 'GUI', and 'HASync'. The main content area is divided into three sections:

- Worker:** A table listing worker identifiers and their function names.

Identifier	Function Name
ManiWorker (139934371235584)	-
ManiWorker (139934362942980)	-
ManiWorker (139934354450176)	-
ManiWorker (139934346057472)	-
- Queue:** A table showing function names, arguments, KW arguments, and scheduled times.

Function Name	Arguments	KW Arguments	Scheduled Time
sysconfd utils run_systemaction_jobs	-	-	2023-12-22 12:09:30
tools utils patch get_patches_vtair_call	-	-	2023-12-22 14:56:29
- Worker Log (Total 590):** A detailed log table with columns for Identifier, Function Name, Arguments, KW Arguments, and Time. A search bar is present above the table.

Identifier	Function Name	Arguments	KW Arguments	Time
ManiWorker	utils.files.execute_custom_scripts_folder		{ folder: '/etc/scripts/syschange_env_data', 'event': 'NEWADDR', 'script_family': '2', 'script_prefixid': '24', 'script_flags': '0', 'script_scope': '0', 'script_index': '2', 'script_event': 'RTM_NEWADDR', 'script_ifa_address': '192.168.10.138', 'script_ifa_local': '192.168.10.138', 'script_ifa_broadcast': '192.168.10.255', 'script_ifa_label': 'ens18', 'script_ifa_flags': 'S12', 'script_ifa_cacheinfo': '{file_preferred: 3500, file_valid: 4000, timestamp: 6370359, timestamp: 6970380}}'	2023-12-22 12:32:46 -> 2023-12-22 12:32:46

The Worker Log contains information about the background worker process that processes functions and informations in the system. It shows all the functions it calls and provides information for debugging of TBF.

21.53 XDP

You can find the XDP Diagnostics at **Diagnostics** → **XDP**.

The screenshot shows the 'Diagnostics / XDP' page. The left sidebar contains navigation options like 'Services', 'VPN', 'Tools', and 'Diagnostics'. The main content area shows the XDP status:

- Status:** active
- State:** enabled
- Action:** Disable XDP (button)

Here you can see the current status of your **XDP** setup and enable or disable it temporarily. This will keep the general **XDP** setting but allows for testing or debugging when disabling it.

To activate or deactivate your XDP setup please go to **System** → **Settings** → **Advanced** and refer to the documentation at [XDP](#).

21.53.1 XDP Interfaces

The screenshot shows the 'Diagnostics / XDP' interface. The 'Interfaces' tab is active, and the selected interface is 'enp0s20i0'. A 'Stats' button is visible. The 'Result' section displays the following data:

```

XDP-action      0 pkts ( 0 pps)      0 Kbytes ( 0 Mbits/
XDP_ABORTED    0 pkts ( 0 pps)      0 Kbytes ( 0 Mbits/
XDP_DROP       0 pkts ( 0 pps)      0 Kbytes ( 0 Mbits/
XDP_PASS       755 pkts ( 4 pps)    48 Kbytes ( 0 Mbits/
XDP_TX         0 pkts ( 0 pps)      0 Kbytes ( 0 Mbits/
XDP_REDIRECT   0 pkts ( 0 pps)      0 Kbytes ( 0 Mbits/
XDP-action      0 pkts ( 0 pps)      0 Kbytes ( 0 Mbits/
XDP_ABORTED    0 pkts ( 0 pps)      0 Kbytes ( 0 Mbits/
XDP_DROP       0 pkts ( 0 pps)      0 Kbytes ( 0 Mbits/
XDP_PASS       743 pkts ( 3 pps)    48 Kbytes ( 0 Mbits/
XDP_REDIRECT   0 pkts ( 0 pps)      0 Kbytes ( 0 Mbits/
  
```

Here you can see stats about your interfaces supporting XDP. It will show you how many packets are forwarded or passed on to the normal firewall.

21.53.2 XDP DDoS

The screenshot shows the 'Diagnostics / XDP / DDoS' interface. The 'DDoS' tab is active. The page displays the following information:

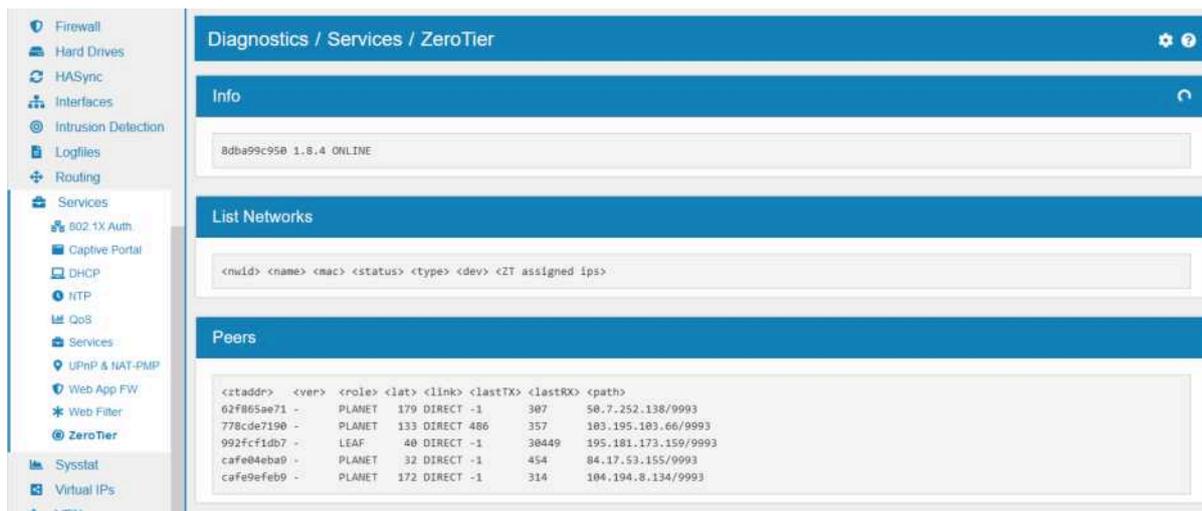
```

Collecting stats from BPF map
- BPF map (bpf_map_type:10) id:4 name:blacklist_v4_st key_size:8 value_size:16 max_entries:10000
- BPF map (bpf_map_type:10) id:5 name:blacklist_v6_st key_size:20 value_size:16 max_entries:10000
Blacklist
Blacklist      1.2.3.4/32      0 pkts ( 0 pps)      0 Kbytes ( 0 Mbits/s) period:0.251337
Blacklist      1.2.3.4/32      0 pkts ( 0 pps)      0 Kbytes ( 0 Mbits/s) period:2.000627
Blacklist      1.2.3.4/32      0 pkts ( 0 pps)      0 Kbytes ( 0 Mbits/s) period:2.000753
Blacklist      1.2.3.4/32      0 pkts ( 0 pps)      0 Kbytes ( 0 Mbits/s) period:2.000548
  
```

Here you can see stats about the XDP DDoS protection. XDP DDoS allows for efficient and fast dropping of packets at near line rate and therefore protects the firewall from getting overwhelmed by requests. The Firewall DDoS rules will be loaded automatically.

21.54 ZeroTier

You can find the ZeroTier Diagnostics at **Diagnostics** → **Services** → **ZeroTier**.



The screenshot displays the Mikrotik WinBox interface for the ZeroTier service. The left sidebar shows the navigation menu with 'ZeroTier' selected under the 'Services' category. The main content area is titled 'Diagnostics / Services / ZeroTier' and is divided into three sections:

- Info:** Shows the device ID '8dba99c950', version '1.8.4', and status 'ONLINE'.
- List Networks:** Shows a table with columns for network ID, name, MAC, status, type, device, and assigned IPs.
- Peers:** Shows a table with columns for address, version, role, latency, link, last TX, last RX, and path.

<nwid>	<name>	<mac>	<status>	<type>	<dev>	<ZT assigned ips>
<nwid>	<name>	<mac>	<status>	<type>	<dev>	<ZT assigned ips>

<ztaddr>	<ver>	<role>	<lat>	<link>	<lastTX>	<lastRX>	<path>
62f885ae71	-	PLANET	179	DIRECT	-1	307	50.7.252.138/9993
778cde7190	-	PLANET	133	DIRECT	486	357	103.195.103.66/9993
992fcf1db7	-	LEAF	40	DIRECT	-1	30449	195.101.173.159/9993
cafe04eba9	-	PLANET	32	DIRECT	-1	454	84.17.53.155/9993
cafe9efeb9	-	PLANET	172	DIRECT	-1	314	104.194.8.134/9993

Here you can see the general *Info*, *Networks* and *Peers*.

To change the ZeroTier setup please go to **Services** → **ZeroTier** and refer to the ZeroTier documentation at [ZeroTier](#).

22.1 ARPing

You can find the ARPing Tool at **Tools** → **ARPing**.

The information is shown in real time in your browser.

With this tool you can test the reachability of a host via a MAC address. It will send an arp message from this system to the entire L2 and will get an answer if the MAC address is reachable.

Enter the MAC address of the destination and click on **ARPing** to start. You can specify the **number of pings** and which **source** interface shall be used, which uses auto by default.

22.2 Backup & Restore

You can find the Backup & Restore Settings at **Tools** → **Backup & Restore**.

Here you can backup and restore all data of the TBF.

22.2.1 Backup

The backup functionality lets you download a file with the name **backup.json** to your computer. This file is in the JSON format and contains all data of the TBF. Optionally you can enter a password before you create a backup. This password is also needed for the restore process.

A TBF backup is automatically created every day at 02:00 and can be found in the folder **/var/lib/vtair/backup/**.

Note: Beware that all passwords which are displayed unencrypted in the web interface are also stored unencrypted in the backup. The user passwords are stored encrypted in the system and in the backup as well.

22.2.2 Restore

The restore functionality lets you restore a backup which was previously created with the TBF. If you entered a password for the backup, you need to enter it here as well.

Note: Please do not modify the backup file to ensure a working restore of the backup.

The restore process will be displayed in the GUI after the backup file has been uploaded. You can watch the restore process until the end and will be redirected to the GUI afterwards. When the restore is finished, the backup settings are not yet applied. You might need to map the interfaces of the restored device to your backup and apply all settings.

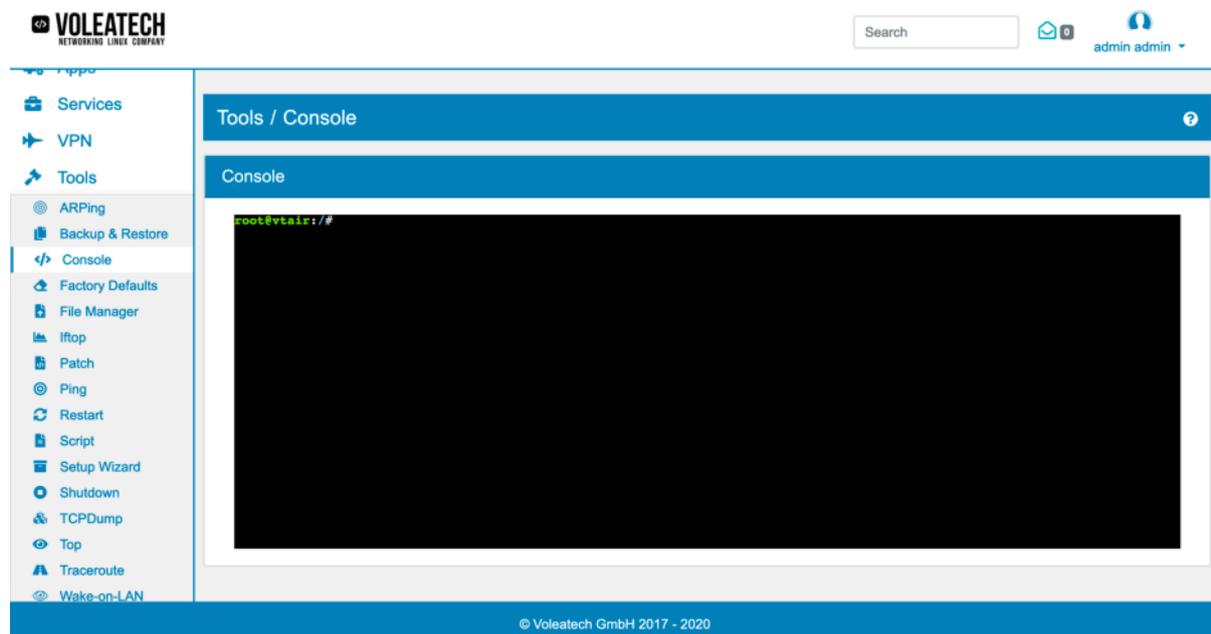
Before applying all restored settings, no backup settings are applied to the TBF. Passwords are already used from the restored backup to sign into the Webgui.

22.3 Web Console

You can find the Web Console at **Tools** → **Console**.

This tool opens an interactive system console which lets you operate directly on the system itself in the browser. You will have root access in the shell on the screen.

Warning: The web console is a linux bash with admin rights and should be used with caution.



You can use standard UNIX commands to navigate and control the web console of your TBF device.

22.4 Factory Defaults

You can find the Factory Defaults Option at **Tools** → **Factory Defaults**.

This tool lets you reset the TBF and restores all default settings and puts it into a factory new state.

Warning: It's highly recommended to create a backup before. All created and modified data in the TBF will be lost. The browser connection will also be reset after the restore is completed. The LAN interface will be accessible again at the default IP 192.168.1.1.

22.5 File Manager

You can find the File Manager Tool at **Tools** → **File Manager**.

This tool lets you upload and download files from the TBF.

You can browse through all directories by clicking on a folder. When you click on the **Upload** button and select a file, it will be uploaded in the currently opened directory.

If you click on a file it is downloaded to your computer.

22.6 lftop

You can find the lftop Tool at **Tools** → **lftop**.

The information is shown in real time in your browser.

This tool displays a consistently updated list of network connections. The network traffic will be monitored and a list of bandwidth usage displayed. You can specify the interface which will be used.

22.7 LLDP

You can find the LLDP Tool at **Tools** → **LLDP**.

Enabled can be changed to enable or disable LLDP. It's disabled by default.

The screenshot shows the 'Tools / LLDP' configuration page. At the top, there is a blue header with 'Tools / LLDP' and a help icon. Below the header, the 'LLDP' section has a toggle switch labeled 'Enabled' which is currently turned on. There are 'Save' and 'Cancel' buttons below the toggle. The 'LLDP Neighbors' section displays a list of discovered neighbors. The first neighbor is connected via interface 'emp82098, via: LLDP, RID: 1' at 'Time: 0 day, 00:41:00'. Its details include: ChassisID: mac 00:50:c2:04:d2:6c, SystemName: vtair-internal, SysDescr: Debian GNU/Linux 11 (bullseye) Linux 6.6.0-1-vtair-arm64 #1 SMP Debian 6.6.22-2-vtair (2024-04-29) aarch64, MgmtIP: 10.10.11.2, MgmtFace: 5, MgmtIP: fd00:7371:7569:0470:726f:7879:0:1, MgmtFace: 1, Capabilities: Bridge, on; Router, on; Mlan, off; Station, off. The second neighbor is connected via interface 'emp82098, via: LLDP, RID: 2' at 'Time: 0 day, 00:41:07'. Its details include: ChassisID: mac 04:a1:51:33:03:34, SystemName: XS712T ProSafe 12-Port 10 Gigabit Ethernet (10GbE) Smart Switch, 6.1.0.36, 06.1.0.3, MgmtIP: 192.168.10.40, MgmtFace: 13, Capabilities: Bridge, on.

LLDP shows you information about other devices on your network that also use the LLDP protocol.

22.8 Patch

You can find the Patch Tool at **Tools** → **Patch**.

The **Patch** tool lets you apply patches to specific parts of the system without the necessity of a complete system software update.

When creating a new patch, there are several options:

Description is a description of the patch.

Patch Content is the content of the patch.

Path Strip Count is the number of leading components from the patch file name.

Base Directory is the base directory for the patch. By default / is used.

Ignore Whitespace lets whitespaces be ignored in the patch content.

On the Patch screen you can **apply** and **delete** patches.

The status can be one of the following:

- Not applied yet
- Failed to applied
- Successfully applied

22.8.1 Patches

In the * TBF Patches** tab you can find TBF system patches.

They will be automatically pulled from the TBF Portal and cannot be changed or deleted.

On a system start the TBF will automatically apply all available patches.

Some patches have a dependency which means another patch has to be applied before this patch.

On the Patch screen you can **apply** and **unapply** patches.

22.9 Ping

You can find the Ping Tool at **Tools** → **Ping**.

The information is shown in real time in your browser.

With this tool you can test the reachability of a host. It will send messages from this system to the destination which will be echoed back if it's reachable.

Enter the hostname or IP address of the destination and click on **Ping** to start. You can specify the IP Protocol, v4 or v6, the **number of pings** and which **source** address shall be used, which uses auto by default.

A successful result could look like this:

```
PING www.wikipedia.com (91.198.174.192) 56(84) bytes of data.  
64 bytes from text-lb.esams.wikimedia.org (91.198.174.192): icmp_seq=1 ttl=56  
↔time=27.9 ms  
64 bytes from text-lb.esams.wikimedia.org (91.198.174.192): icmp_seq=2 ttl=56  
↔time=30.6 ms
```

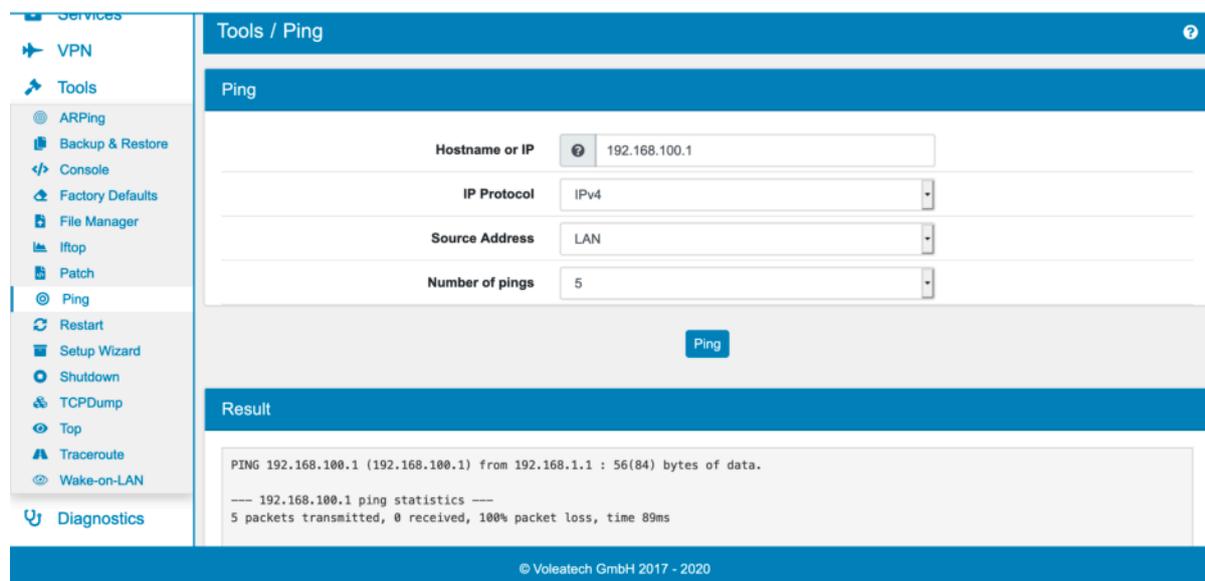
(continues on next page)

(continued from previous page)

```
64 bytes from text-lb.esams.wikimedia.org (91.198.174.192): icmp_seq=3 ttl=56
↳time=24.4 ms
```

```
--- www.wikipedia.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 24.441/27.682/30.699/2.566 ms
```

An unsuccessful result would look like this:



Ping helps you in determining the reachability of a specific host/IP address. If you have a new rule configured that is supposed to block a specific website for example you can test the reachability (and thus the effectiveness of your rule) with ping. There is no need to actually visit the website to confirm that a rule is operational.

22.10 Restart

You can find the Restart Option at **Tools** → **Restart**.

Here you can restart the TBF. The web interface won't work for the time being.

If you want to stop the TBF entirely, you can use the *Shutdown* functionality instead.

22.11 Script

You can find the Script Tool at **Tools** → **Script**.

The **Script** tool lets you save the code of a script to a specific file on the system. This way, the script will be included in the TBF backup.

When creating a new script, there are several options:

File Path is the absolute file path of the script. It is not possible to overwrite an existing file by choosing a file path which already exists in the system.

Script Content is the content of the script.

Description is a description of the script.

22.12 Setup Wizard

You can find the Setup Wizard at **Tools** → **Setup Wizard**.

Here you can configure the TBF with the same setup wizard, which is shown the first time you log into the TBF.

It consists of several pages, where you can configure general options, the WAN and LAN interfaces and set a new admin password. You can always cancel the dialog and revisit it later.

All options can always be changed on the [Settings](#) page and corresponding interface pages.

22.13 Shutdown

You can find the Shutdown Option at **Tools** → **Shutdown**.

Here you can shutdown the TBF. The web interface won't work for the time being.

If you want to restart the TBF instead, you can use the [Restart](#) functionality instead.

22.14 TCPDump

You can find the TCPDump Tool at **Tools** → **TCPDump**.

This tool is a **packet analyzer** that displays TCP/IP and other packets which are transmitted and received over the network.

The information is shown in real time in your browser.

You can specify the interface and the IP Protocol, v4 or v6. The **count** determines, after how many packets it stops. With **packet length** you can specify the number of bytes it will capture for each package. The default is 0 which will capture everything. A **detail level** can also be configured, which is set to normal by default.

If you don't use the IPSec interface, there is also the possibility to add additional filters by protocol, IP address, port or mac address. Those filters can be connected via logical operators like **and**, **or** and **not**.

You can also download the trace afterwards if you enable the **Save to File** option **before** you start tcpump.

The output could look like this:

```
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144,
↳ bytes
12:51:21.060482 IP (tos 0x0, ttl 64, id 3784, offset 0, flags [DF], proto TCP (6),
↳ length 162)
    vtair.localhost.hq.voleatech.com.8000 > IT1.hq.voleatech.com.57318: Flags [P.],
↳ cksum 0x92ec (incorrect -> 0xbd6a), seq 2584698705:2584698827, ack 1786006290,
↳ win 120, length 122
12:51:21.100800 IP (tos 0x0, ttl 127, id 26583, offset 0, flags [DF], proto TCP
↳ (6), length 40)
    IT1.hq.voleatech.com.57318 > vtair.localhost.hq.voleatech.com.8000: Flags [.],
↳ cksum 0x66f0 (correct), seq 1, ack 122, win 2052, length 0
12:51:21.365874 IP (tos 0x0, ttl 64, id 46612, offset 0, flags [DF], proto ICMP
↳ (1), length 28)
    vtair.localhost.hq.voleatech.com > 192.168.10.1: ICMP echo request, id 0, seq
↳ 17114, length 8
12:51:21.365959 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto ICMP (1),
↳ length 28)
```

(continues on next page)

(continued from previous page)

```

192.168.10.1 > vtair.localhost.hq.voleatech.com: ICMP echo reply, id 0, seq_
↳17114, length 8
12:51:21.384065 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.10.
↳143 tell pfSensedev.dev.hq.voleatech.com, length 46
12:51:21.396593 IP (tos 0x0, ttl 64, id 14672, offset 0, flags [DF], proto TCP (6),
↳ length 91)

```

With TCPDump you can analyze the communication on your network in great detail. If you're only interested in the communication of a specific host you can specify its IP address in the filter section. This way you're given all the packets that are sent and received by this host.

If you're only interested in the traffic of a specific host relating to a specific port/protocol you can also specify the port number in the filtering section. This way you can customize your TCPDump request and get a much cleaner result that is a lot easier to interpret.

22.14.1 Troubleshooting via TCPDump

You can also access the TCPDump feature via the Console. To do this, log in to your TBF device via SSH or via a serial connection (see [Console Access](#) for more details). Once you are logged in, type *shell* to access the Shell.

Type the command

```
nohup tcpdump -i INT -w /var/tmp/packetcapture.pcap -W 3 -C 10 -n host IPADDRESS and port PORT &
```

with *INT* being the physical interface (for example eth1), *IPADDRESS* being the IP address of the host you want to observe the connection with and *PORT* being the port of the connection you want to observe. This creates a maximum of three files with 10MB (rotating). You can analyze the files later on.

Type

```
pskill tcpdump
```

to end the process. Afterwards you can look at the results by loading the file into Wireshark or by typing

```
tcpdump -r /var/tmp/packetcapture.pcap0 -n -vvvv -XX
```

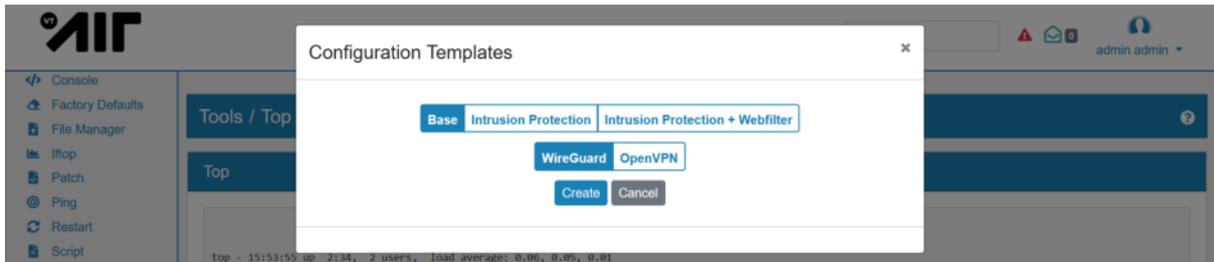
```

root@vtair:~# nohup tcpdump -i eth1 -w /var/tmp/packetcapture.pcap -W 3 -C 10 -n -n host 192.168.1.100 and port 443 &
[1] 837
root@vtair:~# nohup: ignoring input and appending output to 'nohup.out'
kill1 tcpdump
root@vtair:~# tcpdump -r /var/tmp/packetcapture.pcap0 -n -vvvv -XX
reading from file /var/tmp/packetcapture.pcap0, link-type EN10MB (Ethernet)
14:21:46.881707 IP (tos 0x2,ECT(0), ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 153)
 192.168.1.100.68116 > 192.168.1.1.443: Flags [P.], cksum 0x5ffa (correct), seq 4054295435:4054295536, ack 3885006685, win 2319, options [nop,nop,TS val 883098782 ecr 507780121], length 101
 0x0000: 163b 1de8 4f5c a8ce c8d4 3e6b 0808 4502  ....>K...D...E.
 0x0010: 0099 0000 4000 4006 b5a7 c0a8 0164 c0a8  ...@.....d...
 0x0020: 0101 ead4 01bb f1a7 a38b 1728 0ccd 8018  .....{....
 0x0030: 090f 5ffa 0000 0101 080a 3a43 0a9e 1e44  .....A....D
 0x0040: 1c19 1703 0300 000c 0041 089e 0002 500c  ....1BA...0P
 0x0050: c2d6 9083 02c8 6255 7687 643e 16ba 2afe  ....BMA.d...*
 0x0060: 78a7 1e79 0da4 2038 4d26 c800 da78 67f4  p..y.J.BMA...xg.
 0x0070: 78d1 d61f 5251 047a 3c49 377d f44c 5708  x...RQ.z<17>.LW.
 0x0080: 77c7 0e35 0190 0703 000a 4065 b0f6 a2bb  w...5a....0e....
 0x0090: e88b 0e96 c391 ab08 41b9 470d a0da 08c7  @.....A.0....
 0x00a0: 2281 7edc c3f5 8a  ....*.....
14:21:46.881791 IP (tos 0x0, ttl 64, id 65809, offset 0, flags [DF], proto TCP (6), length 52)
 192.168.1.1.443 > 192.168.1.100.68116: Flags [P.], cksum 0x83dc (incorrect -> 0x2331), seq 1, ack 101, win 252, options [nop,nop,TS val 507826487 ecr 883098782], length 0
 0x0000: a0ce c8d4 3e6b 163b 1de8 4f5c 0808 4502  ....>K...D...E.
 0x0010: 0034 fe23 4000 4006 b08a c0a8 0101 c0a8  .A.#@.....
 0x0020: 0164 01bb ead4 1728 0ccd f1a7 a3f0 8010  .d.....{.....
 0x0030: 00fc 83dc 0000 0101 080a 1e44 d137 34a3  .....D.74.
 0x0040: 040e  ....
14:21:48.742676 IP (tos 0x2,ECT(0), ttl 64, id 65860, offset 0, flags [DF], proto TCP (6), length 7292)
 192.168.1.1.443 > 192.168.1.100.68116: Flags [P.], cksum 0xa024 (incorrect -> 0xae09), seq 1:7241, ack 101, win 252, options [nop,nop,TS val 507828348 ecr 883098782], length 7240
 0x0000: a0ce c8d4 3e6b 163b 1de8 4f5c 0808 4502  ....>K...D...E.
 0x0010: 1c7c fe24 4000 4006 9c9f c0a8 0101 c0a8  .J.#@.....
 0x0020: 0164 01bb ead4 1728 0ccd f1a7 a3f0 8018  .d.....{.....
 0x0030: 00fc a024 0000 0101 080a 1e44 d07c 34a3  ...$......D.|4.
 0x0040: 049e 1703 0340 11f7 e20c 9664 425b 98c5  ....@.....dBl..
 0x0050: 052b 99bd 9710 22f4 371b a5f9 3ad1 18cf  +.....*7...l...
 0x0060: 0b42 2f44 f0bc a392 c32c 099f 752f 3f0f  kB/D.....u/?.
 0x0070: eec1 2cd7 1683 5f79 8df3 819c 7020 080e  .....}....0...
 0x0080: 0826 bab0 c338 fba7 57b1 9c05 922f 00e7  .&...B.W...../..
 0x0090: 001a 5853 b15d d0c6 eaf4 0f1d 53bf c8a4  .X5.].....S...
 0x00a0: a192 3af5 c7cb 0a52 0107 f3ff 3bde 0d3c  ..:...b.g...<
 0x00b0: 7504 0c76 f21a ea7a 8508 0603 01ff 7f48  udV...U.F.O..H
 0x00c0: 4aa4 c742 e20d 40a1 1240 08fd 844b b052  J..B..@...K.R
 0x00d0: 7ced 1b05 4d25 2230 ea09 e055 aaff 0370  [...M*0...U..p
 0x00e0: 96c7 2083 cb18 c197 52b4 4938 5b79 64bc  +.....R.l8|yd.
 0x00f0: 4aa4 2c7f 0710 c19a c4cd 96d8 9a2c 60e3  .D.....f...
 0x0100: 3aed 26c2 a123 c82c 8a46 8d71 448e 0bf3  .&...&.F.gD...
 0x0110: 09ef b31f 01ab b331 6400 45c5 fee6 5cad  ....l.d.E...\.
 0x0120: b1cf 7b56 0610 6755 2b03 62b4 67a0 c8b8  ..{V..gU+.b.g...
 0x0130: ff9c a54f 8572 c056 4e08 0522 d0d7 b0b3  <.0.rM.V.e*...
 0x0140: f109 c100 bba9 905b 77db 0700 1f0b b7b6  .....E.....
 0x0150: b25a 2c10 f35a f718 f487 ac4f 2c14 b1d2  .Z...Z.....0...
 0x0160: 8ff7 2eaf e2ca 95aa 8a8d 081a d8c0 c92b  .....+.....
 0x0170: 410f 0171 d0c3 c053 a087 1645 0056 b08d  Ao.q.c.S...E.V..
 0x0180: 7009 0396 f10b 071c 0ba6 c00e 040c 3409  Z.....JL...4.
 0x0190: 8c00 c07f c7a3 fc0c fff5 594c 1655 7400  .....YL.Ut.
 0x01a0: 49bc fa1e 95b2 7930 0009 488d 0d45 9a50  I.....y0".H..E.P
 0x01b0: c868 0409 0c7e bda4 f945 9e89 23b2 3377  .h.....E.#.3w
 0x01c0: a453 20c3 f97b c0f0 25cd 4f0c e18c 263b  +.....NmDL.A.
 0x01d0: 4022 eaef ff7a 0815 009c cc21 2077 0d04  0".....z..0.l1.w.
 0x01e0: 19f2 51c2 d371 8e60 d791 72a1 3b90 fe21  .Q..q...r...!
 0x01f0: bcde 9101 0f31 51b6 a3c4 5743 f409 a96c  ....lQ...WC...l
    
```

This is very helpful to find sporadic connection or network problems that can not be reproduced right away.

22.15 Templates

You can find the Templates Tool at **Tools** → **Templates**.



This tool helps you create a TBF setup. You can chose between one of the options *Base*, *Intrusion Detection* and *Intrusion Protection + Webfilter*. Additionally you can choose a VPN setup being *WireGuard* or *OpenVPN* or both. The system will then automatically create a rudimentary setup in those categories. If you want to revert this setup, you can use this tool again and deselect what you want to have removed.

22.16 Top

You can find the Top Tool at **Tools** → **Top**.

This tool displays information about the CPU and memory utilization. The result is a ordered list of running processes which get updated consistently.

22.17 Traceroute

You can find the Traceroute Tool at **Tools** → **Traceroute**.

The information is shown in real time in your browser.

With this tool you can display the route and and measure the delay across a network.

Enter the hostname or IP address of the destination and click on **Traceroute** to start. You can specify the IP Protocol, v4 or v6 and which **source** address shall be used, which uses auto by default. The **max. TTL** is the time-to-live and represents the maximum number of network hops. You can also use **ICMP ECHO** instead of UDP datagrams.

A successful result could look like this:

```

traceroute to www.wikipedia.de (134.119.24.29), 30 hops max, 60 byte packets
 1 HSI-KBW-46-237-206-193.hsi.kabel-badenwuerttemberg.de (46.237.206.193)  5.683
   ↪ms 10.471 ms 10.579 ms
 2 ip-81-210-148-240.hsi17.unitymediagroup.de (81.210.148.240)  10.256 ms 10.266
   ↪ms 10.228 ms
 3 de-fra01b-rc1-ae37-0.aorta.net (84.116.191.173)  16.927 ms 17.086 ms 17.079 ms
 4 de-fra01b-ri2-ae30-0.aorta.net (84.116.134.166)  16.781 ms de-fra01b-ri2-ae29-0.
   ↪aorta.net (84.116.134.162)  16.956 ms 16.722 ms
 5 213.46.177.10 (213.46.177.10)  16.767 ms 28.383 ms 26.085 ms
 6 ffm-bb3-link.telia.net (62.115.120.1)  26.078 ms ffm-bb4-link.telia.net (62.115.
   ↪120.7)  20.464 ms 16.672 ms
 7 koln-b1-link.telia.net (80.91.247.247)  19.419 ms 104.602 ms 104.479 ms
 8 ae0.cr-nashira.cgn4.core.heg.com (62.115.33.242)  39.964 ms 21.363 ms 21.355
   ↪ms
 9 ae0.sr-jake.cgn1.dcn.heg.com (87.230.114.222)  21.317 ms 21.275 ms 21.227 ms
10 wikipedia.de (134.119.24.29)  22.021 ms 21.997 ms 20.675 ms

```

22.18 Wake-on-LAN

You can find the Wake on LAN Tool at **Tools** → **Wake-on-LAN**.

With this tool you can turn on or awake a host by a network message.

Enter the *MAC Address* or the destination and click on **Wake-on-LAN** to start. The *IP Address* is optional and its default value is 255.255.255.255. It's needed, if the destination is on another network.

22.18.1 Wake-on-LAN Devices

You can also save devices with their *MAC Address*, *IP Address* and a *Description*. At **Actions**, it's possible to manually start the *Wake-on-LAN* for each saved device.

CONFIGURATION EXAMPLES

23.1 Windows Updates

To only allow Windows Updates you can use a DNS Network Object. Create the Network Object with the following DNS Names:

- windowsupdate.microsoft.com (Exact Match)
- *.windowsupdate.microsoft.com (Direct Subdomains)
- *.update.microsoft.com (Direct Subdomains)
- *.windowsupdate.com (Direct Subdomains)
- download.windowsupdate.com (Exact Match)
- download.microsoft.com (Exact Match)
- *.download.windowsupdate.com (Direct Subdomains)
- wustat.windows.com (Exact Match)
- ntservicepack.microsoft.com (Exact Match)
- go.microsoft.com (Exact Match)
- dl.delivery.mp.microsoft.com (Exact Match)

You can use the Network Object in a Firewall Rule as Destination. Please also make sure to disable IPS in the rule under the advanced settings.

23.2 IPv6 Multi WAN

IPv6 Multi WAN can be configured if TBF is connected to multiple ISPs which each provide an IPv6 address or IPv6 network address range.

23.2.1 Network Prefix Translation (NPTv6)

IPv6-to-IPv6 Network Prefix Translation (NPTv6) is a specification for IPv6 to achieve address-independence, similar to network address translation (NAT) in Internet Protocol version 4 (IPv4).

The setup for IPv6 Multi-WAN is very similar to IPv4. The main difference is that you need to define a Network Range in SNAT to achieve NPT.

Firewall / NAT / Create

General Settings

Enabled

Add Rule To Top Bottom

Interface

NAT Type

No NAT

Address Family

Protocol

Description

Sources

Invert IP Match

Source IPs /

Destinations

NAT Settings

Translation IP /

Static Port(s)

Create a second SNAT Rule for WAN2.

Additionally you need to add the WAN2 Gateway to the main routing table in *Routing Tables* for a Multi-Gateway Setup *Multi-Gateway Setup*.

23.3 Custom Scripts

TBF calls custom scripts on events happening on the system to execute custom actions.

23.3.1 System Notification

System notifications are new or deleted routes, ipaddresses or link up an down events. All scripts in the folder */etc/scripts/syschange* are called and the event data are passed along as environment variables.

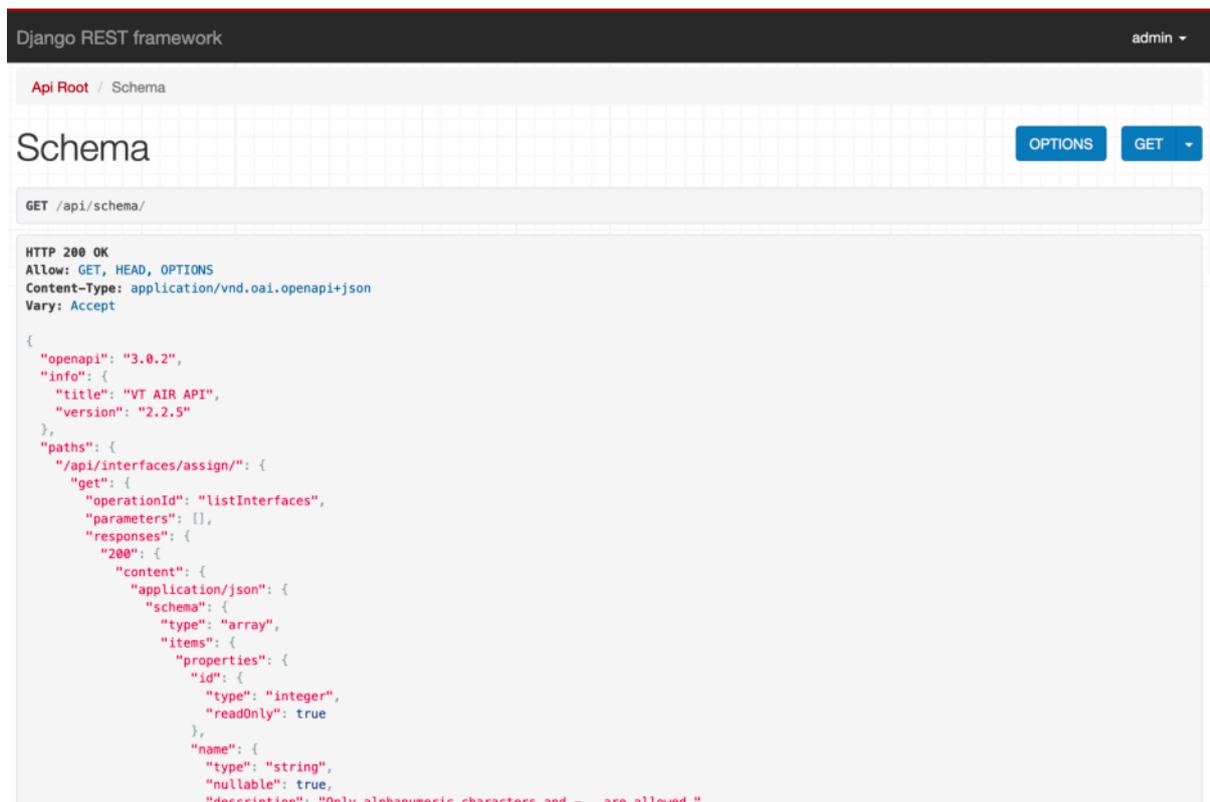
23.3.2 Gateway Change Notification

The Gateway Change Notification calls all scripts in the folder */etc/scripts/gatewaychange* and the event data are passed along as environment variables.

24.1 General

Your TBF device comes with a REST API so you can automate configuration changes in very large networks and save time. Instead of accessing the web GUI of potentially hundreds of devices you can enter the configuration changes once and send them to a whole list of IP addresses.

The REST API gives you the same configuration options as the web GUI in a text-based form. The API can be accessed via the command line, your web browser or specialized programs that read and write to REST APIs.

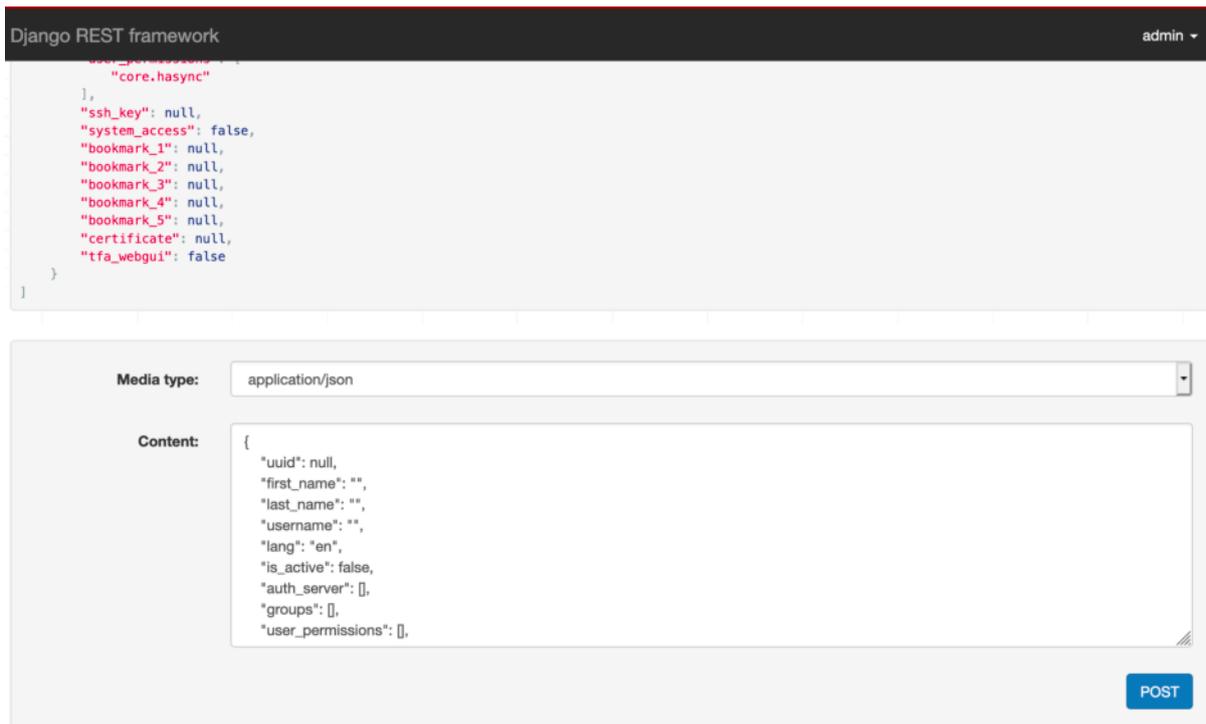


```
HTTP 200 OK
Allow: GET, HEAD, OPTIONS
Content-Type: application/vnd.oai.openapi+json
Vary: Accept

{
  "openapi": "3.0.2",
  "info": {
    "title": "VT AIR API",
    "version": "2.2.5"
  },
  "paths": {
    "/api/interfaces/assign/": {
      "get": {
        "operationId": "listInterfaces",
        "parameters": [],
        "responses": {
          "200": {
            "content": {
              "application/json": {
                "schema": {
                  "type": "array",
                  "items": {
                    "properties": {
                      "id": {
                        "type": "integer",
                        "readOnly": true
                      },
                      "name": {
                        "type": "string",
                        "nullable": true,
                        "description": "Only alphanumeric characters and - . are allowed."
                      }
                    }
                  }
                }
              }
            }
          }
        }
      }
    }
  }
}
```

Via GET, POST and DELETE commands you can alter the contents of the individual fields. You can execute a GET request to load all the fields within that endpoint. For example you can display your TBF's users with the request GET /api/user/.

When accessing the API via your web browser you can execute POST commands directly from your browser window.



```
Django REST framework admin ▾  
"core.hasync"  
},  
"ssh_key": null,  
"system_access": false,  
"bookmark_1": null,  
"bookmark_2": null,  
"bookmark_3": null,  
"bookmark_4": null,  
"bookmark_5": null,  
"certificate": null,  
"tfa_webgui": false  
}  
1
```

Media type: application/json

Content:

```
{  
  "uuid": null,  
  "first_name": "",  
  "last_name": "",  
  "username": "",  
  "lang": "en",  
  "is_active": false,  
  "auth_server": [],  
  "groups": [],  
  "user_permissions": []  
}
```

POST

24.1.1 Accessing the API via a Console

GET requests

On your Mac or Linux device type

```
curl -k -u USER:PASSWORD https://IPADDRESS/api/user/
```

to access the user data of your TBF device reachable under IPADDRESS with the user credentials USER and PASSWORD. This reads back the configuration string of all the users currently configured on your system.

The `-k` option makes your command line ignore that your system does not trust the SSL connection to your device.

The screenshot shows a web browser interface for the Django REST framework. At the top, it says "Django REST framework" and "admin" with a dropdown arrow. Below that, the URL "GET /api/user/" is displayed. The main content area shows the response details:

```

HTTP 200 OK
Allow: GET, POST, HEAD, OPTIONS
Content-Type: application/json
Vary: Accept
X-VTAIR-Version: 2.2.6

[
  {
    "id": 1,
    "uuid": "2180e12e-7b2e-48d7-8b42-73feaecb07b",
    "first_name": "admin",
    "last_name": "admin",
    "username": "admin",
    "lang": "en",
    "is_active": true,
    "auth_server": [
      "47b3f44f-b62b-40c1-b621-51256ec4b520"
    ],
    "groups": [],
    "user_permissions": [],
    "ssh_key": null,
    "system_access": false,
    "bookmark_1": null,
    "bookmark_2": null,
    "bookmark_3": null,
    "bookmark_4": null,
    "bookmark_5": null,
    "certificate": null,
    "tfa_webgui": false
  },
  {
    "id": 2,
    "uuid": "78f610c1-9a5f-4898-996a-d89bc86e9477",
    "first_name": "hasync",
    "last_name": "hasync",
    "username": "hasync",
    "lang": "en",
    "is_active": true,
  }
]

```

POST requests

To write data to your device you can use a POST request. Type

```
curl -k -u USERS:PASSWORD -d 'DATA' https://IPADDRESS/api/user/
```

the *DATA* string needs to include all the fields you want to fill separated by &. For example (shortened for readability):

```
'uuid=null&first_name=John&lastname=Doe&username=johnDoe&lang=en'
```

Token

Each User has an API Token that can be used instead of the user and password. For this the format of the Authorization Header is "Token <ACCESS_TOKEN>".

```
curl -k -H "Authorization: Token <ACCESS_TOKEN>" https://IPADDRESS/api/user/
```

COMMANDS

25.1 Speedtest

Run a speedtest from the command line

```
usage: speedtest.py [-h] [--no-download] [--no-upload] [--single] [--bytes] [--share] [--simple] [--csv] [--csv-delimiter CSV_DELIMITER] [--csv-header] [--json] [--list]
                    [--server SERVER] [--exclude EXCLUDE] [--mini MINI] [--source SOURCE] [--timeout TIMEOUT] [--secure] [--no-pre-allocate] [--version]

Command line interface for testing internet bandwidth using speedtest.net. -----
↳ -----
https://github.com/sivel/speedtest-cli

optional arguments:
-h, --help            show this help message and exit
--no-download        Do not perform download test
--no-upload          Do not perform upload test
--single            Only use a single connection instead of multiple. This
↳ simulates a typical file transfer.
--bytes            Display values in bytes instead of bits. Does not affect the
↳ image generated by --share, nor output from --json or --csv
--share            Generate and provide a URL to the speedtest.net share
↳ results image, not displayed with --csv
--simple            Suppress verbose output, only show basic information
--csv              Suppress verbose output, only show basic information in CSV
↳ format. Speeds listed in bit/s and not affected by --bytes
--csv-delimiter CSV_DELIMITER
                    Single character delimiter to use in CSV output. Default ",
↳ "
--csv-header        Print CSV headers
--json            Suppress verbose output, only show basic information in JSON
↳ format. Speeds listed in bit/s and not affected by --bytes
--list            Display a list of speedtest.net servers sorted by distance
--server SERVER    Specify a server ID to test against. Can be supplied
↳ multiple times
--exclude EXCLUDE  Exclude a server from selection. Can be supplied multiple
↳ times
--mini MINI        URL of the Speedtest Mini server
--source SOURCE    Source IP address to bind to
--timeout TIMEOUT  HTTP timeout in seconds. Default 10
--secure          Use HTTPS instead of HTTP when communicating with speedtest.
↳ net operated servers
--no-pre-allocate  Do not pre allocate upload data. Pre allocation is enabled
↳ by default to improve upload performance. To support systems with insufficient
↳ memory, use this
                    option to avoid a MemoryError
```

(continues on next page)

(continued from previous page)

<code>--version</code>	Show the version number and exit
------------------------	---

25.2 Command Line Tools

25.2.1 logcleanup

Clean up logfiles that are too big.

Usage: <code>logcleanup.py</code>

Run periodically by the system.

25.2.2 vtair-upgrade

Command line update tool.

Usage: <code>vtair-upgrade</code>

25.2.3 vtair-upgrade-single

Command line update tool for a single package.

Usage: <code>vtair-upgrade-single [PACKAGENAME]</code>
--

25.2.4 vtair-upgrade via USB Image

Command line update with a USB image of the installer as update source

Usage: <code>vtair-console update --local</code>
--

25.2.5 check-routes

Command line tool to check all routes and gateways

Usage: <code>check-routes</code>

25.3 XDP Command Line Tools

XDP command line tools can be used to manage and show options of the xdp offloader feature.

25.3.1 xdp_vair_user

Tool to attach the XDP programm and set the blacklist.

Usage: xdp_vtair_user [options]

DOCUMENTATION:
 XDP flowoffload
 - Allows selecting BPF section --progsec name to XDP-attach to --dev

Required options:
 -d, --dev <ifname> Operate on device <ifname>

Other options:
 -h, --help Show help
 -F, --force Force install, replacing existing program on interface
 -U, --unload Unload XDP program instead of loading
 -M, --reload-maps Recreate pinned maps
 -B, --blacklist Reload Blacklist
 -b, --blacklistread Read **and** output Blacklist
 -O, --option Option Setting mode required **for** enable **or** disable
 -E, --enable Enable XDP Forward mode on loaded XDP program
 -D, --disable Disable XDP Forward mode on loaded XDP program
 --filename <file> Load program **from** <file>
 --progsec <section> Load program **in** <section> of the ELF file

25.3.2 xdp_stats

Tool to read out stats of XDP.

Usage: xdp_stats [options]

DOCUMENTATION:
 XDP stats program
 - Finding xdp_stats_map via --dev name info

Required options:
 -d, --dev <ifname> Operate on device <ifname>

Other options:
 -h, --help Show help
 -b, --blacklist Blacklist
 -C, --clear Clear **all** values **in** xdp_stats_map **or** blacklist

ROADMAP

- **MPTCP:**

Multipath TCP offers multiple connections between two hosts and also adjusts the send rate and balances the degree of congestion within each sub-flow to improve throughput/resource utilisation. We want to explore the ability to connect two TBF with MPTCP for SDWAN.

- **Dynamic Charting Framework:**

A dynamic charting framework would allow us to chart arbitrary data from the OS that can be read like states, CPU utilization and so on.

- **Web Filter connection to Intrusion Protection:**

We want to forward decrypted Web Filter traffic to the Intrusion Protection engine. This would allow us to also check encrypted web traffic that is decrypted by the Web Filter against the IPS Ruleset.

CHANGELOG

27.1 Version 25.07

1. Cellular add auth paramter for connection
2. IDS Report fix time of day it is send
3. Bugfixes

27.2 Version 25.04

1. HAProxy added maximum backend connections
2. LDAP Sync check for unique LDAP ID
3. SHDSL Save and Restore Config
4. Intrusion Protection Report XLXS fix
5. SNMP v3 user write access fix
6. TOTP User Device Cache fix
7. SDWAN Interface feature removed

The SDWAN feature is now removed. Please use alternatives like ZeroTierOne for this functionality.

27.3 Version 25.01

1. OT Enforcer:
Integration of the Tofino OT Enforcer for Modbus, IEC104, DNP3, ENIP, Goose, OPC, AMP Protocols
2. New Logo:
Added the new VT AIR Belden Logo and Color
3. Other Changes:
 - Cellular Unblock SIM PIN with PUK
 - HAProxy improvements for custom error page validation
 - DHCP Host Reservation improvements for the data validation

27.4 Version 24.10

1. DHCP Relay:

The DHCP Relay can now be used alongside the DHCP Server on the Firewall. Only one of each can run on a single interface.

2. DNS Firewall:

The DNS Firewall was reworked and offers different categories now.

3. HAProxy Frontend:

You can now connect Frontends, the main Frontend will carry all major settings. This makes it easier to distinguish frontend configurations, that can be grouped.

4. Webfilter Active Directory:

Support for binding the Webfilter to Active Directory for authentication and group checks.

5. Firewall Rule Last Used:

Firewall rules will show a last used counter and information about the states and traffic. It allows to see which rules are used how much.

6. Other Changes:

- LDAPs fixes
- HAProxy improvements for custom error pages
- Notification if the hard disk space runs low
- Kea DHCP Server support for relay agents

27.5 Version 24.07

1. DDoS Whitelist:

DDoS has an accept parameter now to whitelist ips from blocking

2. Config Check:

Services like the Webfilter will run a config check now before applying new settings

3. Webfilter:

The number of used CPUs can be configured. The blocklists have been reworked and have their own tab now. They can be enabled per category. Custom Configs for Pre ACL and Post ACL

4. LLDP:

LLDP neighbors can now be seen in the GUI if the LLDP service is active

5. Other Changes:

- Bond Diagnostics
- HAProxy improvements for custom error pages
- DNS Diagnostics has a field to resolve IPs
- Captive Portal Diagnostics Show User if any
- Unbound DNS Safesearch
- DHCP HA Mode can be configured
- SNMP for Cellular modems

- Letsencrypt custom ACME server support
- STP configure Port priority
- Intrusion Protection for Layer 2 Bridges
- Add CSP header for security

27.6 Version 24.04

1. Interface Groups:

Allow interfaces to be grouped. At the moment the group can only be used in NAT rules.

2. Active/Active Firewall Cluster:

In the VRRP IP options a new field sets the default destination for an VRRP IP. This allows for an Active/Active Firewall Cluster where each firewall can have active VRRP IPs. The clients in the network need to have different Gateways to either use Firewall 1 or Firewall 2. In case of a failover one Firewall will hold all IPs.

3. Gateway Check in the routing daemon:

The Gateway Check is now moved to the dedicated vtair-routing daemon for faster and more reliable Gateway failovers.

4. HAProxy Custom Error Page:

Error pages are now configurable and can be used in combination with ACLs and Actions to customize when a page is show.

5. WebVPN 2FA Support:

A new option allows to use the Version 2FA in the User settings for the WebVPN.

6. Other Changes:

- Kernel Update to 6.6 LTS
- SNMP add write for VT AIR OIDs
- Fix IPsec interface check when multiple phase1 share one interface
- WLAN Client option for SSID and Password
- Fix logserver changes are not applied
- HASync also sync the Captive Portal Database
- HAProxy make Actions sortable
- HAProxy option to have one backend per host name
- HAProxy fix ACL IPs with a large amount of entries
- IPsec logfile from diagnostics page
- OpenVPN logfile from diagnostics page
- OpenVPN Copy ask for new Name
- Field for Kernel boot options
- HAProxy move to nbthreads instead of processes
- WebVPN RDP new option for default keyboard layout
- HAProxy add client certificate option Optional or Required
- HAProxy health check for LDAP

- Dynamic Routing Diagnostics show internal routing database
- IPSec Phase 1 new IPComp option
- Aliase Entries introduce paging for large amount of entries

27.7 Version 24.01

1. LTE450:

Support for the new LTE450 network

2. Password Change:

At first login a password must be set for the admin user before the GUI is available. This is a major change to the previous default password and is required to comply with new security regulations.

3. SNMP:

New custom SNMP endpoints to read the data of Wireguard, IPSec, OpenVPN Server and OpenVPN Client

4. New Database Backend Connector:

The database connector in VT AIR was rewritten to provide better stability and circumvent situations when the database is busy.

5. Firewall Sets:

The firewall backend uses more Sets now which speed up the firewall rule load time especially for large setups and geoips.

6. States Sync:

Option to write synced states directly into the state table instead of using the external cache. This allows for faster failover but higher costs during sync.

7. Other Changes:

- Fix a race condition where the cache could be filled with old data
- User Download own Wireguard Profile
- Dashboard Firewall, IDS, WAF Alert when Logger is disabled
- Network Object import lists with Mac Addresses
- Work queue has more details now in diagnostics
- WebVPN add User, Password and Domain field
- Fix for Captive Portal HASync of Files
- Firewall uses the new ipsec Identifier
- A Security Patch Repository is added when the update licence expires
- Fix DHCP Pool lease lifetime option
- Fix bond in bridge change not triggering a change
- Fix Captive Portal interface change not triggering a change
- Firewall setting for default policy
- Captive Portal Diagnostics show traffic data
- Intrusion Detection Report Excel Table Report
- Certificates list view show extra information like DNS

- Fix Interface Stats Diagnostics data not showing correct date
- DNS fix no restart after interface change
- WAF various fixes for excluding rules, parsing ajax requests and setting default data

27.8 Version 23.10

1. WAF Engine:

The Web Application Firewall engine is changed to Coraza. Modsecurity is end of life soon and we transition over to the new engine. It also allows more efficient integration into HAProxy with the spoa interface. Along with this change, a custom error html page can be set on each HAProxy backend.

2. Routing Backend

The static routing backend is outsourced to a new daemon vtair-routing. All static and mpls routes are now handled by this new routing daemon which is far more efficient than our previous implementation.

3. Rename LTE

All GUI entries that had LTE in it are now renamed to Cellular. Since we support 5G now we decided to go with a more generic name.

4. Zero Tier One

Support for multiple Zero Tier One connections

5. Password Change

If a user wants to change their own password, the old password will be required as well now.

6. Password Strength Indicator

For all passwords, we added a strength indicator to see how good the password is

7. Login Attempts

Are now logged and shown in the Diagnostics under GUI Logins. All attempts are logged, regardless of success.

8. Running Services

Will show their corresponding ports in the diagnostics service page.

9. Connected Devices

All open connections to the VT AIR itself can be seen in the Diagnostics under Firewall - Host Connections

10. User OpenVPN Profile Download

Users can now download their own OpenVPN Profile in the Profile section when logged into the WebGUI

11. IPSec Phase 1 Fallback

Another Phase 1 can be picked as a backup tunnel to start in case of the original Phase 1 being down. A Ping check needs to be configured along with the Fallback tunnel to check if the remote endpoint is available.

12. IPSec Interface for multiple Phase 1

If the networks in the Phase 2 do not overlap, an IPSec Interface can now be used by multiple Phase 1. This makes the management of firewall rules and routes easier as the interface will carry all the different traffic.

13. Other Changes:

- Webserver IP can now be picked by interface IPs and Virtual IPs
- Cache gateway status up/down in the backend for faster processing
- Letsencrypt can now be used with HAProxy in Webserver mode
- The backup restore progress has more details in the GUI now and shows information until the end
- Diagnostics Firewallrule Output is now streamed from the Webserver. On large setups the page blocked the entire webserver.
- WPA Supplicant uses the default wpa_supplicant-wired service name now instead of a custom one
- More choices for the ICMPv6 types in firewall rules
- Diagnostics DHCP the apply change banner is now sticky at the top of the screen when scrolling for better visibility
- Improvements and speedups when using DHCP Interfaces during startup
- Improvements in detecting when interfaces go up and down
- Fix for VRRP status was sometimes not shown correctly
- OpenVPN show interface name in the settings of the tunnel
- Firewallrule deletion show warning that open states are unaffected
- IPSec Diagnostics has a new overview list page of all connections
- HAProxy TCP mode allow certificates and client certificate authentication
- HAProxy added a new a global custom config section
- Fix the use of CRLs with HAProxy
- Fix the AND / OR logic in HAProxy
- Fix radvd needs IPv6 DNS server and does not start with IPv4 (RFC8106)
- Fix webproxy spelling error for splice
- Interface IPv6 track config can now utilize the ID to fix a subnet to an interface
- Fix DNAT IPv6 was missing the [] to seperate the port
- Fix Webproxy transparent proxy did not prperly work with IPv6 since the localhost address can not be used for sending (RFC4291)
- ACME DNS Handle has a description field now
- Fix Network Objects dynamic entries need to be validated one by one
- Fix loganalyzer can not save certain json data
- DHCP Server allow pools with a single IP
- DHCP Server expose the reclaim parameter
- Unifi App Image will have a volume created automatically on creation

27.9 Version 23.07

1. XDP DDoS Protection:

DDoS Firewall Rules are now loaded into XDP which allows for much faster drop rates and protection. A generic XDP program is now loaded on non native XDP Interfaces if XDP is enabled for the DDoS protection. Intrusion Protection can now also mark flows/states for dropping in XDP when a drop rule hits, allowing for a much faster drop rate of bad traffic.

2. DDoS more options:

DDoS options are now more fine grained. It is possible to either count dropped traffic (default) or all traffic against the DDoS rate limit. Additional options are always available for SYN and ICMP packets to cover specialized DDoS attack cases.

3. LTE Support second SIM Card:

LTE modems with a second SIM card can be configured in the GUI now with automatic SIM card switching. This allows to utilize both SIM card slots and if a Gateway of one connection goes down, the Gateway check can trigger a SIM card change. Only one SIM card can be activate at a given time. There is also a GUI option in the diagnostics section of LTE to manually change the SIM card slot.

4. Firewall Option to Disable XDP for a flow:

If XDP is enabled you can now exclude flows through a firewall rule options. It is useful for QoS or Diagnostics.

5. IPSec Hardware Offload Setting:

In case of a Mellanox NIC that supports IPSec offload you can enable the setting in the GUI

6. Faster Gateway configuration at boot:

The default Gateway will be added faster now on boot if possible. This will work for static Gateways and DHCP Gateways.

7. Option to show Hostname in header:

Show the hostname of the VT AIR in the header and in the login screen. This way you can more easily identify which VT AIR you are on

8. VRF Support:

Virtual routing and forwarding allows for better separation of network interfaces and routes. One can now group interfaces by VRF and VRF also allows the creation of a Layer 3 VPN (L3VPN) in combination with our dynamic routing options. VRF can be added in the Interface configuration and added to each assigned Interface in the advanced options.

9. SNMP Contrack States:

Export the number of used contrack states to SNMP

10. HAProxy more Options:

The configuration of SSL and Cipher Parameter is now possible in the GUI.

11. Firewall Detect Possible Duplicate Rules:

Each Interface Firewall and Global Firewall Rule has a new option in the GUI to show possible duplicate rules. VT AIR checks the 6 tuple (Source IP, Destination IP, Source Port, Destination Port, Protocol, Interface) to check if there is another rule that might cover the same rule. We do not check any extra options though so a manual check has to be performed. The design requires the firewall service to run first and fill up the data for the check. The same goes for changes of firewall rules which need to be applied first before the new data set is available.

12. Firewall Optimizations:

We use Sets now for Network Objects and especially Geo IPs, this is a config generation change only. The change allows us to only load used Objects which will speed up firewall rule loading by a lot especially for setups utilizing the Geo IP data. There are no changes to the GUI and it is backend change only.

13. Other GUI Changes:

- Rename XDP Offloader to XDP
- Update to the Copyright list of used packages

14. Other Changes:

- API Schema file is now only rewritten on a version change to make the GUI start faster
- Cleanup of old logrotate files in the config directory
- Fix for addons not available across worker processes
- Fix for Letsencrypt DNS Handles not being HASynced to the secondary firewall
- Fix for Interface and VirtualIP can have the same IP Address on the same interface
- Fix for LTE Interface has no Link Local IPv6 address in some cases
- Fix for Wired WPA Supplicant not having a fake SSID
- Fix for Bridge interface members and DHCP Server not being in the correct state when the GUI starts. They are now reloaded upon the GUI start so we can control interface changes correctly
- HAProxy delete certificates that are not in use by any Frontend anymore
- HAProxy duplicate backend do not also duplicate the ACL and Verdict rules in the Frontend
- Bootup load firewall rules faster
- WLAN and WWAN interfaces create a stable naming of wwanX and wlanX
- SNMP fix bridge OID values
- Support for 5G modems
- Fix Gateway Monitoring not always recording data for diagnostics
- Logcleanup can now shrink /var/log to the configured RAM Disk size if RAM disk is enabled
- Fix QoS Tab is created for non eligible interfaces

27.10 Version 23.04

1. eXpress Data Path flow offloader (XDP)
2. SNMP allow for multiple Trap Server
3. SNMP custom traps
4. Services can have non existing Virtual IPs on standby
5. LTE Dual Stack fixes

27.11 Version 23.01

1. DNS Firewall extend lists
2. Webfilter extend lists
3. DHCP Static Entry as Firewall Object
4. IPSec allow start and trap at the same time
5. Captive Portal Voucher
6. Captive Portal Redirect to another VT AIR
7. Docker Backup Script
8. Webfilter more options in the GUI for Man in the Middle and redirect, as well as logging
9. Webfilter add LDAP Support
10. Change Diagnostic Data to influxdb

27.12 Version 22.10

1. Firewall Rule TCPDump
2. Firewall Rule Trace
3. Interface HASync
4. Add Multiple Options for DNS, DHCP, VirtualIP
5. Config Default Templates
6. Syslog TLS Option
7. Routing Backend Refactoring for faster speed
8. Gateway changes custom scripts
9. Firewall better custom rule GUI
10. GUI Updates and Factory Defaults output improvements
11. Certificate P12 also import CA
12. Network Object Entries reordering
13. Allow to select default firewall rule tab
14. Firewall temp rules with expiration date
15. New radius backend library

27.13 Version 22.07

1. IPv6 Network Prefix Translation
2. Windows AD Client for Identity Awareness
3. PC Client for Identity Awareness
4. Service Speed Improvements
5. Rename Alias to Network Objects
6. Select fields are now searchable in the Webgui

7. Firewall fields for IPs and Ports are changed to real time search fields
8. Firewall Rule support raw syntax
9. DNS Diagnostics
10. Diagnostics IP Addresses country flags
11. IPSec Identifier simplification
12. OpenVPN Diagnostics show encryption for each connected client
13. DHCP Server TFTP iPXE Support
14. QinQ choose VLAN Type
15. Intrusion Detection Option to exclude internal traffic
16. DynDNS Cron option for time based checks
17. Letsencrypt renew support custom script
18. Interface create option for default firewall rules

27.14 Version 22.04

1. Kernel Update to 5.15
2. Move Firewall Rules between Global and Interface
3. AWS Alias list
4. Allow all Interfaces to be disabled
5. Firewall Rule show order
6. DNS Domain allow exact match and all subdomains
7. Webfilter Virus Scan whitelist domains
8. DHCP Static IP lease checks
9. Improve States Diagnostics
10. QoS use only base interfaces
11. HASync optimizations
12. Firewall Rule delete button in edit screen
13. XLXS Export for firewall settings
14. Read Only Group
15. Zerotier Addon

27.15 Version 22.01

1. Systat Sum interfaces
2. WAF Dashboard
3. BGP Passive Neighbor
4. HASync Onboarding
5. HA Sync Sign and Warning Secondary
6. GeoIP Continents

7. OpenVPN Custom Overrides
8. Firewall Rule Divider
9. CSR Sign with CA
10. OpenVPN Remove Peer to Peer
11. Disk Mail Root Notifications
12. VRRP needs a static or dhcp IP
13. Auto Update change
14. Logfile Cleaner
15. HAProxy ssl
16. DNS Domain Overrides allow multiple
17. VRRP Fail on disk error
18. DNS Domain Firewall Rules
19. AWS and Azure
20. Webserver disable TLS 1.0 and TLS 1.1 and DHE Algorithm
21. OpenSSH disable DHE Algorithm

27.16 Version 21.10

1. Update to Debian 11
2. Intrusion Detection Events Dashboard
3. Firewall Events Dashboard
4. Dynamic Routing Custom Config Options
5. Intrusion Detection Email Reports
6. Dynamic Routing BPD Support
7. Dynamic Routing IS-IS Support
8. CSR Import
9. Wireguard Fast Peer Creation
10. High Availability Unicast Option (VRRP and States Sync)
11. Restructuring of the Diagnostics Menu
12. IPSec EAP Radius Support
13. LTE Diagnostics enhancements
14. Support for page size on list views like Firewall
15. Route Diagnostics shows Protocol Name
16. VRRP Fix for IPv4 and IPv6 Support
17. Authenticator 802.1X enhancements and diagnostics
18. OpenVPN Shared Key Config fixes
19. IPSec fix for AES-GCM in Phase 1
20. OpenVPN Restart on Gateway change

27.17 Version 21.07

1. DDoS Firewall Early Drop
2. Suricata DDoS Firewall Blocking
3. Suricata Update Rules or Groups
4. Gateway Check History
5. Web Application Firewall
6. HAProxy Proxy Option
7. Wireguard VRRP Master Option
8. Firewall Rules Delete All
9. Intrusion Protection VT AIR Pro Rules Support
10. Gateway Force Down Option
11. Letsencrypt DNS Authentication

27.18 Version 2.2.9

1. State Counter
2. GRO Fix
3. Netflow Export
4. App Container Environment Variables
5. MPLS LDP
6. OpenVPN GUI Improvements
7. CPU Profiles
8. Fixes

27.19 Version 2.2.8

1. Captive Portal User Authentication
2. VirtualIP Alias can have a Netmask
3. Intrusion Detection option Drop First
4. DHCP Options NTP Fix
5. OpenVPN User Authentication Diagnostics Fix
6. Captive Portal is part of the base Installation
7. Intrusion Detection Diagnostics add a protocol dropdown
8. IP reverse DNS for Firewall and Intrusion Detection Diagnostics
9. App Definition Copy
10. Identity Management
11. User based Firewall Rules
12. VirtualIP Carp setting for start mode (Master/Backup)

13. IPSec fixes and options for close/open/dpd
14. SDWAN support (Preview)
15. Linux Kernel 5.10 (LTS)

27.20 Version 2.2.7

1. App Control (Application Firewall Rules)
2. Security Dashboard
3. VXLAN Support
4. WebVPN Groups Support
5. Webfilter SSL Man in the Middle Support
6. Webfilter Auto Detect PAC File
7. Sudo Support
8. IPSec Ping Check
9. OpenVPN Copy Option
10. Webfilter is part of the base Installation
11. Intrusion Detection show predefined rules
12. Wireguard Copy Option
13. Route remove if Gateway is down

27.21 Version 2.2.6

1. New WebVPN Addon
2. Intrusion Detection is part of the base system
3. Intrusion Detection Speedups
4. SNAT output interfaces
5. Firewall rules trace
6. Google IPs as Alias
7. Notification Messages for Interface, Gateway, Virtual IP change
8. Web Filter (Squid) Fixes
9. Wireguard Config Import
10. Wireguard MTU option
11. Wireguard Routing Table option
12. Web Filter change blacklist
13. Audit Log Export
14. MPLS Support
15. Multipath Routes Support
16. Docker Fixes and Show Ports in the GUI
17. Users and Groups are moved to their own Menu item

18. GUI Login requires System Admin (Admin) or System User (User) group membership

27.22 Version 2.2.5

1. LTE fix SIM PIN leading zero is removed
2. Captiveportal fixes for OSX/iPhone
3. Apply Change now checks for in progress on the Webgui
4. Firewall Rule Routing Table Back Direction
5. Dashboard Traffic Widget can be added multiple times
6. IPSec Allow All/Any as Interface
7. Captive Portal Timeout for clients
8. Alias/CP Hostnames are now resolved more accurately
9. HAProxy Backend Sticky Table
10. Wireguard DNS Server
11. Wireguard Multiple IP Addresses
12. Wireguard Peer Export
13. Wireguard QRCode for config exports
14. PPPoE Interface Master Only
15. SHDSL Mode und PAM
16. Default Certificate can be removed
17. Dashboard Columns can be set
18. Firewall Diagnostics show current ruleset
19. CPU Mitigation can be enabled/disabled
20. SNMP Temperature export

27.23 Version 2.2.4

1. Squid ClamAV Virus Scanner
2. Squid Shallala Blacklist
3. IPSec Diagnostics shows Encryption Parameter
4. LTE Roaming Option
5. Diagnostics have auto reload enabled
6. IPSec Support additional Algorithms (AES-CCM, ChaCha20)
7. GRE-TAP Support (Layer 2)
8. PCrypt for parallel encryption speedup
9. LDAP Automatic User Sync
10. Auto Update Report Emails
11. DynDNS Strato Support
12. 802.1X Authenticator Addon

- 13. Firewall Custom Rules in GUI
- 14. WireGuard VPN Support

27.24 Version 2.2.3

- 1. Escape Virtual IP Password
- 2. LTE Templates for Providers
- 3. Update Pages shows individual updates
- 4. Traffic Widget option for PPS
- 5. Backup Name includes hostname and time
- 6. State Deletion of Offloaded Connections
- 7. Rate Limit SSH to VT AIR
- 8. IPSec Secondary Authentication
- 9. IPSec Client Connection Support
- 10. IPSec Support for EAP-TLS, EAP-MD5, EAP-MSChapv2
- 11. Squid Proxy Addon
- 12. Auditlogs for SHDSL, VDSL, LTE, Apps
- 13. LTE Autoconnect and Refresh Fixes
- 14. Captive Portal Updates
- 15. IPSec Fix Problems with Certificate Authentication
- 16. DHCP Client Leasetime Field Added
- 17. Certificate only requires CNAME
- 18. GRE Keepalive Support
- 19. SNMP Fixed Interface MIBs for VT AIR Models internal interfaces
- 20. Fixes

27.25 Version 2.2.2

- 1. Fixes
- 2. Firewall Time Support
- 3. VDSL Diagnostics
- 4. ARP Table Settings
- 5. QoS Bridge
- 6. LTE Diagnostics
- 7. Certificate Creation on User Page
- 8. Two Factor Authentication GUI + OpenVPN
- 9. Captive Portal

27.26 Version 2.2.1

1. Fixes
2. VDSL Settings and Diagnostics
3. Update Email Schedule for Updates
4. Portal Backup of config
5. NAT and Firewall Search
6. Copyright in GUI for all packages
7. GRE over IPSec fixes
8. GRE responder for keepalive IPv4
9. QoS Flow offload fixes

27.27 Version 2.2.0

1. Fixes
2. LDAP Sync User Groups
3. NAT Reflection Netmask
4. OpenVPN Gateways can be selected
5. QoS Flowtable fix
6. Session Timeout can be configured
7. Login IPs can be whitelisted
8. Diagnostics for NTP
9. DynDNS Home Support

27.28 Version 2.1.3

1. Fixes
2. Geo IPs
3. Office365 Firewall Rules
4. DNS Blacklists

27.29 Version 2.1.2

1. Fixes
2. Bond ARP Check
3. SNAT Routing Table

27.30 Version 2.1.1

1. Portal Connection Management
2. Bond in Bridge
3. Bond xmit policy
4. Gateway Groups Diagnostics
5. DNAT Routing Table

27.31 Version 2.1.0

1. Bridge Layer2 Firewall Rules
2. Flowtable Implementation
3. Remote Access Daemon
4. Bugfixes

27.32 Version 2.0.0

1. Config Mode
2. Suricata for IDS/IPS
3. UPNP IPv6 Support
4. Software Raid Support and Diagnostics
5. Syslogs for more Services
6. Auto RAID 1 Installation
7. App Armor

27.33 Version 1.6.0

1. Email Alerts for Updates
2. Strongswan Swancntrol
3. Allow for IPSec Interfaces
4. Backup/Restore fix
5. P12 Certificate Import
6. WPA Supplicant for wired Interfaces
7. IPSec multiple source IPs
8. UPNPNat working
9. Letsencrypt Support
10. Firewall Helper

27.34 Version 1.5.0

1. Addon Apcups
2. Addon Ntopng
3. DHCP Mac Deny
4. TCPCDump file download
5. RRD Graphs
6. SMART Status Hard Drives
7. Systemctl for Firewall
8. OpenVPN Server Authentication Server

27.35 Version 1.4.0

1. User Authentication Radius
2. User Authentication LDAP
3. Addon Avahi
4. Addon IGMPProxy
5. High Availability Config Sync
6. High Availability VRRP
7. High Availibility Firewall States Sync
8. Service changes for HA
9. LAGG set active port
10. SHDSL Option to disable modem
11. Wake on LAN

27.36 Version 1.3.0

1. Fix Users ssh key
2. Limiter Support
3. Fix Reset to factory defaults
4. Ability to change settings after restore before reload
5. Addon Structure
6. HAProxy Addon
7. Hostname Support for Firewall and IPSec
8. HWInterface Support
9. Webgui File Manager
10. VRRP Select Track Interfaces
11. SFP and Bridge Diagnostics
12. OpenVPN Importer

27.37 Version 1.2.0

1. QoS
2. Flowtables for fast forwarding
3. Track Interface
4. DHCPv6 Prefix Delegation
5. Bugfixes
6. DNS over TLS
7. Dynamic DNS
8. Fix firewall rule logging

27.38 Version 1.1.0

1. Fix IP detection problem in Axes behind reverse proxy
2. Add Routing Tables and the ability to assign them via Firewall Rules
3. Add Gateway Fallback and Loadbalancing
4. Handle all Gateways in code now
5. QinQ Interface Support
6. Allow VTI in Bonds
7. Fix backup to exclude certain data
8. MLPPP Support
9. Gateway Monitoring fixes
10. OpenVPN fixes
11. OpenVPN enable certificate + user authentication
12. GUI fixes

27.39 Version 1.0.1

1. fix consumer mixin bug

27.40 Version 1.0.0

1. Inital Release

INDICES AND TABLES

- [genindex](#)
- [modindex](#)
- [Search](#)