

# Oneshield Firewall Reference Manual r. 2.2.1.8

Copyright (c) 2008 Delemont Technology Srl, Italy.  
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

## Index

[Index](#)  
[Preface](#)  
[Accessing the Oneshield Firewall GUI](#)  
[Features and enhancements in version 2.2](#)  
[Legal notice](#)  
[Acknowledgments](#)  
[Oneshield web site](#)  
[Chapter 1: The System Menu](#)  
[Home](#)  
[Network configuration](#)  
[Support](#)  
[Oneshield Network](#)  
[Passwords](#)  
[SSH access](#)  
[GUI settings](#)  
[Backup](#)  
[Shutdown](#)  
[Credits](#)  
[Chapter 2: The Status Menu](#)  
[System status](#)  
[Network status](#)  
[System graphs](#)  
[Traffic graphs](#)  
[Proxy graphs](#)  
[Connections](#)  
[OpenVPN connections](#)  
[SMTP mail statistics](#)  
[Mail queue](#)  
[Chapter 3: The Network Menu](#)  
[Edit hosts](#)  
[Routing](#)  
[Interfaces](#)  
[Chapter 4: The Services Menu](#)  
[DHCP server](#)  
[Dynamic DNS](#)  
[ClamAV antivirus](#)  
[Time server](#)  
[Traffic shaping](#)  
[Spam Training](#)  
[Intrusion detection](#)  
[High availability](#)  
[Traffic Monitoring](#)  
[Chapter 5: The Firewall Menu](#)  
[Port forwarding / NAT](#)  
[Outgoing traffic](#)  
[Inter-Zone traffic](#)  
[VPN traffic](#)  
[System access](#)  
[Chapter 6: The Proxy Menu](#)  
[HTTP](#)  
[POP3](#)  
[SIP](#)  
[FTP](#)  
[SMTP](#)  
[DNS](#)  
[Chapter 7: The VPN Menu](#)  
[OpenVPN server](#)  
[OpenVPN client \(Gw2Gw\)](#)  
[IPsec](#)  
[Chapter 8: The Hotspot Menu](#)  
[Hotspot](#)  
[Dialin](#)  
[Password](#)  
[Allowed sites](#)  
[Chapter 9: The Logs Menu](#)  
[Live](#)  
[Summary](#)  
[System](#)  
[Service](#)  
[Firewall](#)  
[Proxy](#)  
[Settings](#)  
[Appendix: GNU Free Documentation License](#)

## Preface

**Oneshield Firewall** is an Open Source Unified Threat Management (UTM) appliance software. This document is a concise reference to the **Oneshield Firewall** web interface.

### Accessing the Oneshield Firewall GUI

To access the **Oneshield Firewall** GUI is as simple as starting your browser and entering the IP address of the internal (**GREEN**) interface or the hostname of your **Oneshield Firewall**.

Your browser will be redirected to a secure HTTPS connection (port 10443). Since **Oneshield Firewall** uses a self-signed HTTPS certificate, your browser might ask you to accept the certificate during the first connection. The system will then ask for username and password. Specify "admin" as the username and provide the password you set during the installation or, if you bought an appliance, the one you got from your reseller.

You should now be looking at the start page of your **Oneshield Firewall** GUI. You can immediately start exploring the different options and the information available to you through this interface. The rest of this guide follows the layout of the main navigation bar – each chapter corresponds to one of the main navigation items.

### Features and enhancements in version 2.2

#### Web Interface

Completely redesigned web interface; Many usability enhancements

#### Enhanced management of WAN/RED connections

Support for multiple uplinks; multiple IPs/networks on each WAN/RED interface; uplink monitoring with automatic failover (ISP failover); easy editing/management of uplinks; support for new uplink types: UMTS, PPTP

## Networking

VLAN support (IEEE 802.1Q trunking); policy routing: routing based on user, interface, mac, protocol or port

## Port Forwarding / NAT

Multiple uplink support, allowing different rules per uplink; port forwarding of traffic coming from VPN endpoints; source NAT management; option for rule based logging

## System Access

External access has now been enhanced and renamed to system access; fine grained management of permissions regarding access to the system from LAN, WAN, DMZ and VPN endpoints; default policy for firewall/system access is now set to DENY; firewall services automatically define ports required for their proper function, but access can be restricted; support for ICMP protocol

## Outgoing Firewall

Support for ICMP protocol; handling of multiple sources/ports/protocols per rule

## Zone Firewall

The DMZ pinholes section has been enhanced and renamed to zone firewall; fine grained filtering of local network traffic; rules based on zones, physical interfaces, MAC addresses; support for ICMP protocol; handling of multiple sources/ports/protocols per rule

## Intrusion Detection

New version of Snort IDS with reduced RAM usage and enhanced performance; support for inline intrusion detection

## High Availability

Multi-node appliance cluster; hot standby (active/passive); automatic node data synchronization; process monitoring/watchdog

## HTTP Proxy

Time based access control with multiple time intervals; group based web access policies; zone based operation mode: transparent, with or without authentication

## Content Filter

Better handling of content filter categories; enhanced performance

## SMTP Proxy

Enhanced performance; optional setting for smarthost port; additionally secures SMTP traffic coming from VPNs (roadwarrior and gateway to gateway)

## DNS Proxy

Route specific domains to a custom DNS

## Hotspot

Better account listing, with pagination, sorting and search; per user and global bandwidth limiting; MAC-address based user accounts; user accounts import/export per CSV; single-click ticket generation (quick ticket); automatic client network configuration (support for DHCP and static IP); enhanced user/client portal; generic JSON-API for external accounting and third party integration (like hotel management software); support for multiple network interfaces

## OpenVPN

X.509 and 2 factor based authentication; pushing of DNS settings to clients; pushing of global or per client routes; support for NATed VPN endpoints; support for VPN over HTTP proxy; automatic connection failover; every VPN endpoint is resolvable through DNS (vpn.<username>.domain)

## Oneshield VPN Client

Downloadable from [Oneshield Network](#); works with Microsoft Windows (Vista, XP, 2000), MacOS X, Linux; multiple connections at once; encrypted configuration profiles; PSK, X509 based and 2 factor authentication; runs as service and allows unprivileged users to start a connection; can start the connection automatically on boot / on user logon; supports OpenVPN server fallback, when primary server fails

## IPsec

Rewrite of the base; added debugging possibilities; IPsec on orange; default MTU can be overridden; simplified GUI by removing side (left/right) configuration and swapped completely to local/remote labeling; added ID fields; added dead peer detection options

## Live Log Viewer

Realtime log viewer with filtering and highlighting; displays all the logfiles you are interested in at the same time

## Logs

Every service supports remote logging; daily log rotation

## Backup

Zero-configuration backups to USB stick: plug in an USB stick and it "just works"; restore from any USB stick

## Support

One click to grant access to [Oneshield](#) support team; integrated ticketing support

## Legal notice

The Oneshield Firewall Reference Manual 2.2 ("this document") is copyright (c) 2008 Delemont Technology Srl, Italy ("[Oneshield](#)"). Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation, with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Some parts of this document are based on the IPCop Administrative Guide by Chris Clancey, Harry Goldschmitt, John Kastner, Eric Oberlander, Peter Walker. Some parts of this document are based on the IPCop Advanced Proxy Administrative Guide by Marco Sondermann.

The information contained within this document may change from one version to the next. All programs and details contained within this document have been created to the best of our knowledge and tested carefully. However, errors cannot be completely ruled out. Therefore [Oneshield](#) does not express or imply any guarantees for errors within this document or consequent damage arising from the availability, performance or use of this or related material.

The use of names in general use, names of firms, trade names, etc. in this document, even without special notation, does not imply that such names can be considered as free in terms of trademark legislation and that they can be used by anyone. All trade names are used without a guarantee of free usage and might be registered trademarks. As a general rule, [Oneshield](#) adheres to the notation of the manufacturer. Other products mentioned here could be trademarks of the respective manufacturer.

## Acknowledgments

Without the great work of the Smoothwall and then the IPCop team, neither [Oneshield Firewall](#) nor this document would exist. Therefore we would like to thank them all for their hard work.

Thanks to Sourceforge for the hosting. Without Sourceforge we would not have the possibility to gain such a huge worldwide visibility. You are really helping us very much!

## Oneshield web site

For more information please visit [Oneshield's](#) web site at <http://www.Oneshieldsecurity.com>.

## Chapter 1: The System Menu

Select **System** from the menu bar at the top of the screen.

The following links will appear in a submenu on the left side of the screen. They allow for basic administration and monitoring of your [Oneshield Firewall](#).

- Home – system and internet connection status overview
- Network configuration – network and interface configuration
- Support – support request form
- Oneshield Network – [Oneshield Network](#) registration information
- Passwords – set system passwords
- SSH access – enable/configure Secure Shell (SSH) access to your [Oneshield Firewall](#)
- GUI settings – such as interface language
- Backup – backup/restore [Oneshield Firewall](#) settings as well as reset to factory default
- Shutdown – shutdown/reboot your [Oneshield Firewall](#)
- Credits – thanks to all contributors

Each link will be explained individually in the following sections.

## Home

Select **System** from the menu bar at the top of the screen, then select **Home** from the submenu on the left side of the screen.

This page displays an overview of the uplink connection(s) and general system health.

A table is displayed, detailing the connection status of each uplink. Usually you will see just a single uplink called **main**, since it is the primary uplink. Of particular interest is the status field of the individual uplink:

- Stopped - The uplink is not connected.
- Connecting - The uplink is currently connecting.
- Connected - The uplink is connected and fully operational.
- Disconnecting - The uplink is currently disconnecting. **Oneshield Firewall** keeps pinging the gateway and announces when it becomes available.
- Failure - There was a failure while connecting the uplink.
- Failure, reconnecting - There was a failure while connecting to the uplink. **Oneshield Firewall** is trying again.
- Dead link - The uplink is connected, but the hosts that were defined in **Network, Interfaces** to check the connection could not be reached. Essentially this means that the uplink is not operational.

Each uplink can be operated in either managed mode (default) or manual mode. In managed mode **Oneshield Firewall** monitors and restarts the uplink automatically when needed. If managed mode is disabled, the uplink can be activated or deactivated manually. There will be no automatic reconnection attempt if the connection is lost.

Finally, after the uplink table, you can find a system health line, which looks similar to the following example:

```
efw-1203950372.localdomain - 13:45:49 up 1 min, 0 users, load average: 4.84, 1.89, 0.68
This is basically the output of the Linux uptime command. It shows the current time, the days/hours/minutes that Oneshield Firewall has been running without a reboot, the number of console logins and the load averages for the past 1, 5, and 15 minutes.
```

## Network configuration

Select **System** from the menu bar at the top of the screen, then select **Network configuration** from the submenu on the left side of the screen.

Network and interface configuration is fast and easy with the wizard provided in this section. The wizard is divided into steps: you can navigate back and forth using the <<< and >>> buttons. You can freely navigate all steps and decide to cancel your actions at any moment. Only in the last step you will be asked to confirm the new settings. If you confirm, the new settings will be applied. This might take some time during which the web interface might not respond.

Following is a detailed list of each wizard step.

### Choose type of RED interface

When **Oneshield Firewall** was installed, the trusted network interface (called the **GREEN** interface) has already been chosen and set up.

This screen allows to choose the untrusted network interface (called the **RED** interface): the one that connects your **Oneshield Firewall** to the "outside" (typically the uplink to your internet provider). **Oneshield Firewall** does support the following types of **RED** interfaces:

- ETHERNET STATIC - You want to operate an Ethernet adapter and you need to setup network information (IP address and netmask) manually. This is typically the case when you connect your **RED** interface to a simple router using an Ethernet crossover cable.
- ETHERNET DHCP - You want to operate an Ethernet adapter that gets network information through DHCP. This is typically the case when you connect your **RED** interface to a cable modem/router or ADSL/ISDN router using an Ethernet crossover cable.
- PPPoE - You want to operate an Ethernet adapter that is connected via an Ethernet crossover cable to an ADSL modem. Note that this option is only needed if your modem uses bridging mode and requires your firewall to use PPPoE to connect to your provider. Pay attention not to confuse this option with the ETHERNET STATIC or ETHERNET DHCP options used to connect to ADSL routers that handle the PPPoE themselves.
- ADSL (USB, PCI) - You want to operate an ADSL modem (USB or PCI devices).
- ISDN - You want to operate an ISDN adapter.
- ANALOG/UMTS Modem - You want to operate an analog (dial-up) or UMTS (cell-phone) modem.
- GATEWAY - Your **Oneshield Firewall** has no **RED** interface. This is unusual since a firewall normally needs to have two interfaces at least - for some scenarios this does make sense though. One example would be if you want to use only a specific service of the firewall. Another, more sophisticated example is an **Oneshield Firewall** whose **BLUE** zone is connected through a VPN to the **GREEN** interface of a second **Oneshield Firewall**. The second firewall's **GREEN** IP address can then be used as a backup uplink on the first firewall. If you choose this option, you will need to configure a default gateway later on.

### Choose network zones

**Oneshield Firewall** borrows IPCop's idea of different zones. At this point you've already encountered the two most important zones:

- GREEN** - is the trusted network segment.
- RED** - is the untrusted network segment.

This step allows you to add one or two additional zones, provided you have enough interfaces. Available zones are:

- ORANGE** - is the demilitarized zone (DMZ). If you host servers, it is wise to connect them to a different network than your **GREEN** network. If an attacker manages to break into one of your servers, he or she is trapped within the DMZ and cannot gain sensible information from local machines in your **GREEN** zone.
- BLUE** - is the wireless zone (WLAN). You can attach a hotspot or WiFi access point to an interface assigned to this zone. Wireless networks are often not secure - so the purpose is to trap all wirelessly connected machines into their own zone without access to any other zone except **RED** (by default).

Note that one network interface is reserved for the **GREEN** zone. Another one may already be assigned to the **RED** zone if you have selected a **RED** interface type that requires a network card. This might limit your choices here to the point that you cannot choose an **ORANGE** or **BLUE** zone due to lack of additional network interfaces.

### Network Preferences

This step allows you to configure the **GREEN** zone and any additional zone you might have set up in the previous step (**ORANGE** or **BLUE**).

Each zone is configured in its own section with the following options:

- IP address - Specify one IP address (such as 192.168.0.1). Pay attention not to use addresses that are already in use in your network. You need to be particularly careful when configuring the interfaces in the **GREEN** zone to avoid locking yourself out of the web interface! If you change IP addresses of an **Oneshield Firewall** in a production environment, you might need to adjust settings elsewhere, for example the HTTP proxy configuration in web browsers.
- Network mask - Specify the CIDR / network mask from a selection of possible masks (such as /24 - 255.255.255.0). It is important to use the same mask for all devices on the same subnet.
- Additional addresses - You can add additional IP addresses from different subnets to the interface here.

- Interfaces - Map the interfaces to zones. Each interface can be mapped to only one zone and each zone must have at least one interface. However, you might assign more than one interface to a zone. In this case these interfaces are bridged together and act as if they were part of a switch.  
All shown interfaces are labeled with their PCI identification number, the device description as returned by `lspci` and their MAC addresses. A symbol shows the current link status: a tickmark shows that the link is active, an X means there is no link and a question mark will tell you that the driver does not provide this information.

Note that **Oneshield Firewall** internally handles all zones as bridges, regardless of the number of assigned interfaces. Therefore the Linux name of the interfaces is `brX`, not `ethX`.

Additionally, the system's host and domain name can be set at the bottom of the screen.

You need to use IP addresses in different network segments for each interface, for example:

IP = 192.168.0.1, network mask = /24 - 255.255.255.0 for **GREEN**  
 IP = 192.168.10.1, network mask = /24 - 255.255.255.0 for **ORANGE**  
 IP = 10.0.0.1, network mask = /24 - 255.255.255.0 for **BLUE**

It is suggested to follow the standards described in RFC1918 and use only IP addresses contained in the networks reserved for private use by the Internet Assigning Numbers Authority (IANA):

10.0.0.0 - 10.255.255.255 (10.0.0.0/8), 16,777,216 addresses  
 172.16.0.0 - 172.31.255.255 (172.16.0.0/12), 1,048,576 addresses  
 192.168.0.0 - 192.168.255.255 (192.168.0.0/16), 65,536 addresses

The first and the last IP address of a network segment are the network address and the broadcast address respectively and must not be assigned to any device.

### Internet access preferences

This step allows you to configure the **RED** interface, that connects to the internet or any other untrusted network outside **Oneshield Firewall**.

You will find different configuration options on this page, depending on the type of the **RED** interface you have chosen earlier. Some interface types require more configuration steps than others. Below is a description of the configuration for each type.

- ETHERNET STATIC - You need to enter the IP address and network mask of the **RED** interface, as well as the IP address of your default gateway - that is, the IP address of the gateway that connects your **Oneshield Firewall** to the internet or another untrusted network. Optionally, you can also specify the MTU (maximum transmission unit) and the Ethernet hardware address (MAC address) of the interface - usually this is not needed.
- ETHERNET DHCP - You just need to specify whether you want DHCP to set the IP address of the DNS (domain name server) automatically or you want to set it manually.
- PPPoE - You need to enter the username and password assigned to you by your provider, the authentication method (if you do not know whether PAP or CHAP applies, keep the default PAP or CHAP) and whether you want the IP address of the DNS (domain name server) to be assigned automatically or you want to set it manually. Optionally, you can also specify the MTU (maximum transmission unit) and your provider's service and concentrator name - usually this is not needed.
- ADSL (USB, PCI) - There are 3 sub-screens for this choice.  
First you need to select the appropriate driver for your modem.  
Then you need to select the ADSL type: PPPoA, PPPoE, RFC 1483 static IP or RFC 1483 DHCP.  
Next, you need to provide some of the following settings (depending on the ADSL type fields are available or not): the VPI/VCI numbers as well as the encapsulation type; the username and password assigned to you by your provider and the authentication method (if you don't know whether PAP or CHAP applies, use the default PAP or CHAP); the IP address and network mask of the **RED** interface, as well as the IP address of your default gateway (RFC 1483 static IP only); whether you want the IP address of the DNS (domain name server) to be assigned automatically or you want to set it manually. Optionally, you can also specify the MTU (maximum transmission unit) - usually this is not needed.
- ISDN - You need to select your modem driver, phone numbers (your provider's number and the number used to dial out), as well as the username and password that have been assigned to you by your provider and the authentication method (if you don't know whether PAP or CHAP applies, use the default PAP or CHAP). Also specify whether you want the IP address of the DNS (domain name server) to be assigned automatically or you want to set it manually. Optionally, you can also specify the MTU (maximum transmission unit) - usually this is not needed.
- ANALOG/UMTS Modem - There are 2 sub-screens for this choice.  
First you need to specify the serial port your modem is connected to and whether it is a simple analog modem or a UMTS/HSDPA modem. Note that `/dev/ttyS0` is normally used as serial console and is therefore not available for modems.  
Next you need to specify the modem's bit-rate, the dial-up phone number or access point name, the username and password that have been assigned to you by your provider and the authentication method (if you don't know whether PAP or CHAP applies, use the default PAP or CHAP). Also specify whether you want the IP address of the DNS (domain name server) to be assigned automatically or you want to set it manually. For UMTS modems it is also necessary to specify the access point name. Optionally, you can also specify the MTU (maximum transmission unit) - usually this is not needed.  
Please read the note below for problems with modems.
- GATEWAY - You just need to specify the IP address of your default gateway - that is, the IP address of the gateway that connects your **Oneshield Firewall** to the internet or another untrusted network.

Some modern UMTS modems are USB mass storage devices as well. These modems usually register two devices (e.g. `/dev/ttyUSB0`, `/dev/ttyUSB1`). In this case the second device is the modem. This type of modem can cause problems when restarting the firewall because the firewall tries to boot from the USB mass storage device.

SIM cards that require a personal identification number (PIN) are not supported by **Oneshield Firewall**.

### Configure DNS resolver

This step allows you to define up to two addresses for DNS (domain name server), unless they are assigned automatically. Should only one nameserver be used it is necessary to enter the same IP address twice. The IP addresses that are entered must be accessible from this interface.

### Apply configuration

This last step asks you to confirm the new settings.

Click the OK, apply configuration button to go ahead. Once you did this, the network wizard will write all configuration files to the disk, reconfigure all necessary devices and restart all depending services. This may take up to 20 seconds, during which you may not be able to connect to the administration interface and for a short time no connections through the firewall are possible.

The administration interface will then reload automatically. If you have changed the IP address of the **GREEN** zone's interface, you will be redirected to the new IP address. In this case and/or if you have changed the hostname a new SSL certificate will be generated.

## Support

Select **System** from the menu bar at the top of the screen, then select **Support** from the submenu on the left side of the screen.

A support request can be created directly from this screen. Fill in all necessary information and submit your request. A member of the Oneshield support team will contact you as soon as possible. Please provide a detailed problem description in order to help the support team to resolve the issue as quickly as possible.

Optionally, you can grant access to your firewall via SSH (secure shell). This is a secure, encrypted connection that allows support staff to log in to your **Oneshield Firewall** to verify settings, etc. This option is disabled by default. When enabled, the support team's public SSH key is copied to your system and access is granted via that key. Your root password is never disclosed in any way.

## Oneshield Network

Select **System** from the menu bar at the top of the screen, then select **Oneshield Network** from the submenu on the left side of the screen.

Your **Oneshield Firewall** can connect to **Oneshield Network** (EN). **Oneshield Network** allows for easy and centralized monitoring, managing and upgrading of all your **Oneshield Firewall** systems with just a few clicks.

This screen contains three tabs.

The **Subscriptions** tab shows a summary of your **Oneshield Network** support status. The last section lists your activation keys. You need at least one valid activation key (not expired) to receive updates from and participate in **Oneshield Network**. There is a key for each support channel (typically just one). If the firewall has not yet been registered the registration form is shown.

The **Remote Access** tab allows to specify whether your **Oneshield Firewall** can be reached through **Oneshield Network** at all, and if so, through which protocol: HTTPS means the web interface can be reached through **Oneshield Network** and SSH means it is possible to login via secure shell through **Oneshield Network**.

The **Updates** tab displays and controls the update status of your system. There are three sections.

Firstly, pressing the **Check for new updates!** button will access your support channels looking for new updates. If any updates are found they will be listed (updates are distributed as RPM packages). Pressing the **Start update process NOW!** button will install all updated packages.

Secondly – to save you some time – the system retrieves the update list automatically. You may choose the interval to be hourly, daily, weekly (the default) or monthly – do not forget to click on **Save** to save the settings.

Thirdly, by pressing **Update signatures now** you can update the ClamAV antivirus signatures. This works only if ClamAV is in use, for example in combination with the email or HTTP proxy.

## Passwords

Select **System** from the menu bar at the top of the screen, then select **Passwords** from the submenu on the left side of the screen.

You can change one password at a time here. Specify each new password twice and press **Save**. The following users are available:

**Admin** – the user that can connect to the web interface for administration.

**Root** – the user that can login to the shell for administration. Logins can be made locally to the console, through the serial console or remotely via SSH (secure shell) if it has been activated.

**Dial** – the **Oneshield Firewall** client user.

## SSH access

Select **System** from the menu bar at the top of the screen, then select **SSH access** from the submenu on the left side of the screen.

This screens allows you to enable remote SSH (secure shell) access to your **Oneshield Firewall**. This is disabled by default which is the recommended setting. SSH access is always on when one of the following is true:

- Oneshield support team access is allowed in **System**, **Support**.
  - SSH access is enabled in **System**, **Oneshield Network**, **Remote Access**.
  - High availability is enabled in **Services**, **High Availability**.
- Some SSH options can be set:

- SSH protocol version 1 – This is only needed for old SSH clients that do not support newer versions of the SSH protocol. This is strongly discouraged since there are known vulnerabilities in SSH protocol version 1. You should rather upgrade your SSH clients to version 2, if possible.
- TCP forwarding – Check this if you need to tunnel other protocols through SSH. See the note below for a use case example.
- password authentication – Permit logins through password authentication.
- public key authentication – Permit logins through public keys. The public keys must be added to `/root/.ssh/authorized_keys`.

Finally there is a section detailing the public SSH keys of this **Oneshield Firewall** that have been generated during the first boot process.

Assume you have a service such as telnet (or any other service that can be tunneled through SSH) on a computer inside your **GREEN** zone, say port 23 on host 10.0.0.20.

This is how you can setup a SSH tunnel through your **Oneshield Firewall** to access the service securely from outside your LAN.

1. Enable SSH and make sure it can be accessed (see **Firewall**, **System access**).
2. From an external system connect to your **Oneshield Firewall** using

```
ssh -N -f -L 12345:10.0.0.20:23 root@Oneshield_firewall
```

where `-N` tells SSH not to execute commands, but just to forward traffic, `-f` runs SSH in the background and `-L 12345:10.0.0.20:23` maps the external system's port 12345 to port 23 on 10.0.0.20 as it can be seen from your **Oneshield Firewall**.

3. The SSH tunnel from port 12345 of the external system to port 23 on host 10.0.0.20 is now established. In this example you can now telnet to port 12345 on localhost to reach 10.0.0.20.

## GUI settings

Select **System** from the menu bar at the top of the screen, then select **GUI settings** from the submenu on the left side of the screen.

In the community release it is also possible to click on the **Help** translating this project link which will open the **Oneshield Firewall** translation page. Any help is appreciated.

Two options regarding the web interface can be set in this screen: whether to display the hostname in the browser window title and the language of the web interface (English, German and Italian are currently supported).

## Backup

Select **System** from the menu bar at the top of the screen, then select **Backup** from the submenu on the left side of the screen.

In this section you can create backups of your **Oneshield Firewall** configuration and restore the system to one of these backups when needed. Backups can be saved locally on the **Oneshield Firewall** host, to a USB stick or downloaded to your computer. It is also possible to reset the configuration to factory defaults and to create fully automated backups.

### Backup sets

By clicking on the **Create new Backup** button a dialog opens up where you can configure the new system snapshot:

- configuration - includes all configurations and settings you have made, that is the content of the directory `/var/efw`.
- database dumps - includes a database dump, which for example includes hotspot accounting information.
- log files - includes the current log files
- log archives - includes older log files, backups with this option checked will get very big after some time
- remark - an additional comment can be added here

Click on the **Create new Backup** button again to go ahead and create the backup.

Following is the list of available backups (initially empty): you can choose to download them, delete them or restore them by clicking on the appropriate icon in this list. Each backup is annotated with zero or more of the following flags:

- S - Settings. The backup contains your configurations and settings.
- D - Database. The backup contains a database dump.
- E - Encrypted. The backup file is encrypted.
- L - Log files. The backup contains log files.
- A - Archive. The backup contains older log files.
- ! - Error! The backup file is corrupt.
- C - Created automatically. The backup has been created automatically by a scheduled backup job.
- U - This backup has been saved to a USB stick.

#### Encrypt backup

You can provide a GPG public key that will be used to encrypt all backups. Select your public key by clicking on the **Browse** button and then choosing the key file from your local file system. Make sure **Encrypt backup archives** is checked. Confirm and upload the key file by clicking **Save**.

#### Import Backup files

You can upload a previously downloaded backup. Select your backup by clicking on the **Browse** button and then choosing the backup file from your local file system. Fill in the **Remark** field in order to name the backup and upload it by clicking **Save**. It is not possible to import encrypted backups. You must decrypt such backups before uploading them.

The backup appears in the backup list above. You can now choose to restore it by clicking on the restore icon.

#### Reset to factory defaults

Clicking the **Factory defaults** button allows you to reset the configuration of your Oneshield Firewall to factory defaults and reboot the system immediately after. A backup of the old settings is saved automatically.

#### Scheduled backups

Select the **Scheduled backups** tab if you wish to enable and configure automated backups.

First, enable and configure automatic backups. You can choose what should be part of the backup: the configuration, database dumps, log files and old log files as seen in the **Backup Sets** section. You can also choose how many backups you want to keep (2-10) and the interval between backups (hourly, daily, weekly or monthly). When you're done click the **Save** button.

Next, you can tell the system whether or not you want backups emailed to you. If you wish to receive backups by email you can enable this feature and select the email address of the recipient. You can then **Save** the settings. There is also a **Send a backup now** button that will save the settings and try to send an email with the backup immediately, so you can test the system. Optionally you can also provide a sender email address (this must be done if your domain or hostname are not resolvable by your DNS) and the address of a smarthost to be used (in case you want all outgoing email go through your companies SMTP server, rather than be sent directly by your **Oneshield Firewall**). If the SMTP proxy is disabled it is absolutely necessary to add a smarthost to be able to send emails.

## Shutdown

Select **System** from the menu bar at the top of the screen, then select **Shutdown** from the submenu on the left side of the screen.

In this screen you can shutdown or reboot your **Oneshield Firewall** by clicking the **Shutdown** or the **Reboot** button respectively.

## Credits

Select **System** from the menu bar at the top of the screen, then select **Credits** from the submenu on the left side of the screen.

This screen displays the list of people that brought **Oneshield Firewall** to you.

## Chapter 2: The Status Menu

Select **Status** from the menu bar at the top of the screen.

The following links will appear in a submenu on the left side of the screen. They give detailed status information about various aspects of your **Oneshield Firewall**:

- **System status** - services, resources, uptime, kernel
  - **Network status** - configuration of network interfaces, routing table and ARP cache
  - **System graphs** - graphs of resource usage
  - **Traffic Graphs** - graphs of bandwidth usage
  - **Proxy graphs** - graph of HTTP proxy access statistics during the last 24 hours
  - **Connections** - list of all open TCP/IP connections
  - **OpenVPN connections** - list of all OpenVPN connections
  - **SMTP mail statistics** - graph of SMTP proxy filter statistics during the last day/week/month/year
  - **Mail queue** - SMTP server's mail queue
- Each link will be explained individually in the following sections.

### System status

Select **Status** from the menu bar at the top of the screen, then select **System status** from the submenu on the left side of the screen.

This screen is divided into the following sections (accessible via tabs or scrolling):

- Services** - lists the status of all the services installed on **Oneshield Firewall** - a service might appear as **STOPPED** simply because the corresponding feature is not enabled.
- Memory** - this is the output of the Linux `free` command. The first bar shows the total used memory: it is normal for this value to be close to 100% for a long running system, since the Linux kernel uses all available RAM as disk cache. The second bar shows the memory actually used by processes: ideally this should be below 80% to keep some memory available for disk caching - if this value approaches 100%, the system will slow down because active processes are swapped to disk: you should consider upgrading RAM then. The third bar indicates the swap usage. For a long running system it is normal to see moderate swap usage (the value should be below 20%), especially if not all the services are used all the time.
- Disk usage** - this is the output of the Linux `df` command. It shows the used disk space for each disk partition (`/`, `/boot` and `/var` for a default install). `/` and `/boot` should be rather constant, `/var` grows while using the system.

- Uptime and users - this is the output of the Linux `w` command. It reports the current time, information about how long your system has been running without a reboot, the number of shell users that are currently logged into the system (normally there should not be any) and the system load average for the past 1, 5 and 15 minutes. Additionally, if any shell user is logged into the system, some information about the user is displayed (such as the remote host from which he or she is logged in).
- Loaded modules - this is the output of the Linux `lsmod` command. It shows the loaded kernel modules (the information is of interest to advanced users only).
- Kernel version - this is the output of the Linux `uname -r` command. It shows the current kernel version.

### Network status

Select **Status** from the menu bar at the top of the screen, then select **Network status** from the submenu on the left side of the screen.

This page shows the output of the Linux command `ip addr show` (Ethernet interfaces, bridges and virtual devices), the status of the network adapters (if available), the routing table and the ARP cache (MAC / IP addresses in the local LANs).

### System graphs

Select **Status** from the menu bar at the top of the screen, then select **System graphs** from the submenu on the left side of the screen.

This page contains system resource graphs for the last 24 hours: CPU, memory, swap and disk usage. Clicking on one of the graphs will open a new page with the respective usage graphs for the last day, week, month and year.

### Traffic graphs

Select **Status** from the menu bar at the top of the screen, then select **Traffic graphs** from the submenu on the left side of the screen.

This page contains traffic graphs for the last 24 hours. Clicking on one of the graphs will open a new page with traffic graphs for the last day, week, month and year of the chosen interface.

### Proxy graphs

Select **Status** from the menu bar at the top of the screen, then select **Proxy graphs** from the submenu on the left side of the screen.

This page contains graphs with access statistics for the HTTP proxy during the last 24 hours.

### Connections

Select **Status** from the menu bar at the top of the screen, then select **Connections** from the submenu on the left side of the screen.

This page shows the list of current connections from, to or going through **Oneshield Firewall**. The source and destination of every connection are highlighted in the color of the zones they belong to. Additionally to the four zones (**GREEN, RED, ORANGE, BLUE**) that are defined by **Oneshield Firewall**, two other colors are shown. **BLACK** is used for local connections on the firewall whereas **PURPLE** connections belong to virtual private networks (VPNs).

### OpenVPN connections

Select **Status** from the menu bar at the top of the screen, then select **OpenVPN connections** from the submenu on the left side of the screen.

This page shows a list of OpenVPN connections. It is possible to kill or ban connected users by clicking on the **kill** or **ban** button respectively.

### SMTP mail statistics

Select **Status** from the menu bar at the top of the screen, then select **SMTP mail statistics** from the submenu on the left side of the screen.

This page shows statistics of the SMTP traffic (sending email) through **Oneshield Firewall** for the last day, week, month and year. This information is only available when the SMTP proxy is used.

### Mail queue

Select **Status** from the menu bar at the top of the screen, then select **Mail queue** from the submenu on the left side of the screen.

This page shows the current email queue (only available when the SMTP proxy is used). It is also possible to flush the queue by clicking on the **Flush mail queue** button.

## Chapter 3: The Network Menu

Select **Network** from the menu bar at the top of the screen.

The following links will appear in a submenu on the left side of the screen. They allow setting up network-related configuration options:

- **Edit hosts** - define hosts for local domain name resolution
  - **Routing** - define static routes and set up policy routing
  - **Interfaces** - edit your uplinks or create VLANs
- Each link will be explained individually in the following sections.

### Edit hosts

Select **Network** from the menu bar at the top of the screen, then select **Edit hosts** from the submenu on the left side of the screen.

**Oneshield Firewall** contains a caching DNS server (dnsmasq) that checks the system's host file for name look-ups. In this section you can define a custom host entry that will then be resolved for all clients.

Click the **Add a host** link to add a host entry. This is done by specifying IP address, hostname and domain name and then confirming the host entry by clicking on the **Add Host** button.

An existing entry can be deleted by clicking on the trash bin in its row. To edit an entry it is necessary to click on the pencil symbol. The line is then highlighted and a pre-filled form opens up. After all the changes have been applied the entry is saved by clicking on the **Update Host** button.

### Routing

Select **Network** from the menu bar at the top of the screen, then select **Routing** from the submenu on the left side of the screen. It is possible to choose between two types of routing: static routing and policy routing.

#### Static routing

Allows to associate specific network addresses with given gateways or uplinks. Click the **Add a new rule** link to specify a static routing rule using the following fields:

- Source Network** - source network in CIDR notation (example: 192.168.10.0/24)
- Destination Network** - destination network in CIDR notation (example: 192.168.20.0/24)
- Route Via** - enter the static IP address of a gateway or choose between the available uplinks
- Enabled** - check to enable rule (default)
- Remark** - a remark to remember the purpose of this rule later

Click the **Save** button to confirm your rule. You can then disable/enable, edit or delete each rule from the list of rules by clicking on the appropriate icon on the right side of the table (see the icon legend at the bottom).

#### Policy routing

Allows to associate specific network addresses and service ports / protocols with given uplinks. Click the **Create a policy routing rule** link to specify a policy routing rule. The following fields are available:

- Source - The source can be a list of zones or interfaces, a list of IPs or networks in CIDR notation (example: 192.168.10.0/24), a list of OpenVPN users or a list of MAC addresses. By selecting <ANY> the rule will match every source.
  - Destination - The destination can be a list of IPs, networks in CIDR notation or a list of OpenVPN users. By selecting <ANY> the rule will match every source.
  - Service/Port - Optionally you can specify the protocol and, in case of TCP, UDP or TCP + UDP, a port for the rule. Some predefined combinations, e.g. HTTP (protocol TCP, port 80), can be selected from the Service dropdown list.
  - Route Via - Choose the uplink that should be used for this rule. If you want to use the backup uplink whenever the chosen uplink becomes unavailable, the checkbox has to be checked.
  - Type Of Service - The type of service (TOS) can be chosen here.  
 The binary number behind each type of service describes how this type works. The first three bits describe the precedence of the packet: 000 stands for default precedence and 111 describes the highest precedence. The fourth bit describes the delay where 0 means normal delay and 1 means low delay. The fifth bit describes the throughput. 1 increases the throughput while 0 stands for normal throughput. The sixth bit controls the reliability. Again 1 increases reliability and 0 is the setting for normal reliability. The eight IP precedence values are called class selectors (CS0-7). Additionally twelve values have been created for assured forwarding (AFxy, x being a class from 1 to 4 and y being drop precedence from 1 to 3) that provide low packet loss with minimum guarantees about latency. Expedited forwarding (EF PHB) has been defined to ask for low-delay, low-jitter and low-loss service.
  - Remark - Set a remark to remember the purpose of the rule.
  - Position - Define where to insert the rule (relative position in the list of rules).
  - Enabled - Check this checkbox to enable the rule (default).
  - Log all accepted packets - Check this to log all packets that are affected by this rule.
- Click the **Create rule** button to confirm your rule. You can then disable, edit or delete any rule from the list by clicking on the respective icon on the right side of the table. You can also change the order of the rules (by clicking on the down and up arrow icons). After making changes to a rule, do not forget to click the **Apply** button on the top of the list!

## Interfaces

Select **Network** from the menu bar at the top of the screen, then select **Interfaces** from the submenu on the left side of the screen, finally choose one of the two following tabs:

### Uplink editor

Additional uplinks can be defined by clicking on the **Uplink editor** tab: choose the type of uplink, then fill in the type-specific form. The fields are almost the same as in the network configuration wizard (see the "Network configuration" section in "The System Menu" chapter). The following options differ from the network configuration wizard:

- Type - This selection includes one additional protocol: PPTP. PPTP can be configured to work in static or in DHCP mode. This is done by selecting the respective value from the "PPTP method" dropdown. The IP address and netmask must be defined in the appropriate textfields and is only required if the static method has been chosen. Additional IP/netmask or IP/CIDR combinations can be added in the field below if the respective checkbox is enabled. Phone number, username and password are not required but may be needed for some configurations to work. This depends on the provider's settings. The authentication method can be PAP or CHAP. If you are not sure which one to use, just keep the default value "PAP or CHAP" that will work in either case.
- Start uplink on boot - This checkbox specifies whether an uplink should be enabled at boot time or not. This is useful for backup uplinks which are managed but do not need to be started during the boot procedure.
- if this uplink fails - If enabled, this field gives you the possibility to choose an alternative uplink from the dropdown list. This uplink will be activated if the current uplink should fail.
- Reconnection timeout - With this timeout you can specify the time (in seconds) after which an uplink tries to reconnect if it fails. This value depends on your provider's settings. If you are unsure just leave this field empty.

### VLANs

Virtual LANs (VLANs) can be defined by clicking on the **VLANs** tab. The idea behind offering VLAN support in **Oneshield Firewall** is helping to allow arbitrary associations of VLAN ids to firewall zones. To add an association click the **Add new VLAN link**, then specify the following parameters:

- Interface - the physical interface the VLAN is connected to
- Zone - the Zone the VLAN is associated with
- VLAN ID - VLAN ID (0-4095)

Whenever a virtual LAN is created a new interface is created. This interface is named ethX.y where X is the number of the interface and y is the VLAN ID. This interface is then assigned to the chosen zone. "NONE" can be chosen, if the interface is used as High Availability management port.

## Chapter 4: The Services Menu

Select **Services** from the menu bar at the top of the screen.

**Oneshield Firewall** can provide a number of useful services that can be configured in this section. In particular, these include services used by the various proxies, such as the ClamAV antivirus.

Intrusion detection, high availability and traffic monitoring can be enabled here as well. Following is a list of links that appear in the submenu on the left side of the screen:

- DHCP server - DHCP (Dynamic Host Configuration Protocol) server for automatic IP assignment
  - Dynamic DNS - Client for dynamic DNS providers such as DynDNS (for home / small office use)
  - ClamAV antivirus - configure the ClamAV antivirus used by the mail and web proxies
  - Time server - enable/configure NTP time server, set time zone or update time manually
  - Traffic shaping - prioritize your IP traffic
  - Spam Training - configure training for the spam filter used by the mail proxies
  - Intrusion detection - configure the intrusion detection system (IDS) Snort
  - High availability - configure your **Oneshield Firewall** in a high availability setup
  - Traffic Monitoring - enable or disable traffic monitoring with ntop
- Each link will be explained in the following sections.

### DHCP server

Select **Services** from the menu bar at the top of the screen, then select **DHCP server** from the submenu on the left side of the screen.

The DHCP (Dynamic Host Configuration Protocol) service allows you to control the IP address configuration of all your network devices from **Oneshield Firewall** in a centralized way.

When a client (host or other device such as networked printer, etc.) joins your network it will automatically get a valid IP address from a range of addresses and other settings from the DHCP service. The client must be configured to use DHCP – this is something called "automatic network configuration" and is often the default setting. You may choose to provide this service to clients on your **GREEN** zone only, or include devices on the **ORANGE** (DMZ) or **BLUE** (WLAN) zone. Just tick the check boxes that are labeled **Enabled** accordingly.

Click on the **Settings** link to define the DHCP parameters as described below:

- Start address / End address** - Specify the range of addresses to be handed out. These addresses have to be within the subnet that has been assigned to the corresponding zone. If you want to configure some hosts to use manually assigned IP addresses or fixed IP addresses (see below), be sure to define a range that does not include these addresses or addresses from the OpenVPN address pool (see **OpenVPN**, **OpenVPN server**) to avoid conflicts. If you intend to use fixed leases only (see below), leave these fields empty.
  - Default / Max lease time** - This defines the default / maximum time in minutes before the IP assignment expires and the client is supposed to request a new lease from the DHCP server.
  - Domain name suffix** - This is the default domain name suffix that is passed to the clients. When the client looks up a hostname, it will first try to resolve the requested name. If that is not possible, the client will append this domain name suffix preceded by a dot and try again.  
Example: if the fully qualified domain name of your local file server is earth.example.com and this suffix is "example.com", the clients will be able to resolve the server by the name "earth".
  - Primary / Secondary DNS** - This specifies the domain name servers (DNS) to be used by your clients. Since **Oneshield Firewall** contains a caching DNS server, the default value is the firewall's own IP address in the respective zone.
  - Primary / Secondary NTP server** - Here you can specify the Network Time Protocol (NTP) servers to be used by your clients (to keep the clocks synchronized on all clients).
  - Primary / Secondary WINS server** - This setting specifies the Windows Internet Name Service (WINS) servers to be used by your clients (for Microsoft Windows networks that use WINS).
- Advanced users might wish to add custom configuration lines to be added to `dhcpd.conf` in the text area below the settings forms. Pay attention that **Oneshield Firewall**'s interface does not perform any syntax check on these lines: Any mistake here, might inhibit the DHCP server from starting!

**Example:**

The following extra lines may be used to handle VoIP telephones that need to retrieve their configuration files from an HTTP server at boot time:

```
option tftp-server-name "http://$GREEN_ADDRESS";
option bootfile-name "download/snom/{mac}.html";
```

Note the use of `$GREEN_ADDRESS` which is a macro that is replaced with the firewall's own **GREEN** interface address.

### Fixed leases

Sometimes it is necessary for certain devices to always use the same IP address while still using DHCP. Clicking on the **Add a fixed lease** link allows to assign static IP addresses to devices. The devices are identified with their MAC addresses. Note that this is still very different from setting up the addresses manually on each of these devices, since each device will still contact the DHCP server to get its address.

A typical use case for this is the case of thin clients on your network that boot the operating system image from a network server using PXE (Preboot Execution Environment).

The following parameters can be set to define fixed leases:

- MAC address** - the client's MAC address
- IP address** - the IP address that will always be assigned to this client
- Description** - optional description
- Next address** - the address of the TFTP server (only for thin clients / network boot)
- Filename** - the boot image file name (only for thin clients / network boot)
- Root path** - the path of the boot image file (only for thin clients / network boot)
- Enabled** - if this checkbox is not ticked the fixed lease will be stored but not written down to `dhcpd.conf`

Every fixed lease can be enabled, disabled, edited or removed by clicking on the respective icon (icons are described in the legend at the bottom of the fixed leases table).

### List of current dynamic leases

The DHCP sections ends with a list of currently assigned dynamic IP addresses.

## Dynamic DNS

Select **Services** from the menu bar at the top of the screen, then select **Dynamic DNS** from the submenu on the left side of the screen.

Dynamic DNS providers like DynDNS offer a service that allows assigning a globally available domain name to IP addresses. This works even with addresses that are changing dynamically such as those offered by residential ADSL connections. For this to work, each time the IP address changes, the update must be actively propagated to the dynamic DNS provider.

**Oneshield Firewall** contains a dynamic DNS client for 14 different providers – if enabled, it will automatically connect to the dynamic DNS provider and tell it the new IP address after every address change.

For each account (you might use more than one) click on the **Add a host** link, then specify the following parameters:

- Service** - choose the dynamic DNS provider
- Behind a proxy** - (only applies if you use the no-ip.com service) check this box if your **Oneshield Firewall** is connecting to the internet through a proxy
- Enable wildcards** - some dynamic DNS providers allow having all sub domains of your domain point to your IP address, i.e. www.example.dyndns.org and example.dyndns.org will both resolve to the same IP address: by checking this box you enable this feature (if supported by your dynamic DNS provider)
- Hostname and Domain** - the hostname and domain as registered with your dynamic DNS provider, for instance "example" and "dyndns.org"
- Username and Password** - as given to you by your dynamic DNS provider
- behind Router (NAT)** - check this if your **Oneshield Firewall** is not directly connected to the internet, i.e. behind another router / gateway: in this case the service at <http://checkip.dyndns.org> is used to find out what your external IP address is
- Enabled** - check to enable (default)

Please note that you still have to export a service to the **RED** zone if you want to be able to use you domain name to connect to your home/office system from the internet. The dynamic DNS provider just does the domain name resolution part for you. Exporting a service might typically involve setting up port forwarding (see **Firewall**, **Port forwarding / NAT**).

## ClamAV antivirus

Select **Services** from the menu bar at the top of the screen, then select **ClamAV antivirus** from the submenu on the left side of the screen.

The mail proxy (POP and SMTP) and web proxy (HTTP) components of **Oneshield Firewall** use the well known ClamAV antivirus service. This sections lets you configure how ClamAV should handle archive bombs (see the next paragraph for an explanation) and how often information about new viruses is downloaded ("signature update schedule"). You can also see when the last scheduled update has been performed as well as manually start an update.

#### Anti archive bomb configuration

Archive bombs are archives that use a number of tricks to load antivirus software to the point that they hog most of the firewall's resources (denial of service attack). Tricks include sending small archives made of large files with repeated content that compress well (for example, a file of 1 GB containing only zeros compresses down to just 1 MB using zip), or multiple nested archives (e.g. zip files inside zip files) or archives that contain a large number of empty files, etc...).

To avoid these types of attack, ClamAV is preconfigured not to scan archives that have certain attributes, as configured here:

- Max. archive size - Archives larger than this size in MB are not scanned.
- Max. nested archives - Archives containing archives are not scanned if the nesting exceeds this number of levels.
- Max. files in archive - Archives are not scanned if they contain more than this number of files.
- Max compression ratio - Archives whose uncompressed size exceeds the compressed archive size by more than X times, where X is the specified number, are not scanned, the default value is 1000 - note that normal files typically uncompress to no more than 10 times the size of the compressed archive.
- Handle bad archives - What should happen to archives that are not scanned because of the above settings: it is possible to choose between "Do not scan but pass" and "Block as virus".
- Block encrypted archives - Since it's technically impossible to scan encrypted (password protected) archives, they might constitute a security risk and you might want to block them by checking this box.

#### ClamAV signature update schedule configuration

Another important aspect of running ClamAV are the antivirus signatures updates: information about new viruses must be downloaded periodically from a ClamAV server. The configuration pane (top right) lets you choose how often these updates are performed - the default is once every hour. Tip: move the mouse over the question marks to see when exactly the updates are performed in each case - the default is one minute past the full hour.

#### ClamAV virus signatures

This section shows when the last update has been performed and what the latest version of ClamAV's antivirus signatures is.

Click on **Update signatures now** to perform an update right now (regardless of scheduled updates) - note that this might take some time. There is also a link to ClamAV's online virus database in case you are looking for information about a specific virus.

### Time server

Select **Services** from the menu bar at the top of the screen, then select **Time server** from the submenu on the left side of the screen.

**Oneshield Firewall** keeps the system time synchronized to time server hosts on the internet by using the network time protocol (NTP).

A number of time server hosts on the internet are preconfigured and used by the system. Click on **Override default NTP servers** to specify your own time server hosts. This might be necessary if you are running a setup that does not allow **Oneshield Firewall** to reach the internet. These hosts have to be added one per line.

Your current time zone setting can also be changed in this section.

The last form in this section gives you the possibility to manually change the system time. This makes sense if the system clock is way off and you would like to speed up synchronization (since automatic synchronization using time servers is not done instantly).

### Traffic shaping

Select **Services** from the menu bar at the top of the screen, then select **Traffic shaping** from the submenu on the left side of the screen.

The purpose of traffic shaping is to prioritize the IP traffic that is going through your firewall depending on the service. A typical application is to prioritize interactive services such as Secure Shell (SSH) or voice over IP (VoIP) over bulk traffic like downloads.

#### Traffic shaping per uplink

Click on the icons on the right side of the table to enable or disable traffic shaping for every single uplink. For traffic shaping to work properly it is also very important to specify the actual values for the down and up bandwidth for each uplink: click on the pencil icon (edit), then fill in the down and up bandwidth expressed in kbit per second.

#### Traffic shaping services

Add your traffic shaping rules: click on **Create a service** to add a new rule, specifying:

- Enabled - check to enable (default)
- Protocol - whether the service to be prioritized is a TCP or UDP service (example: SSH is a TCP service)
- Priority - give a priority: "high", "medium" or "low"
- Port - the destination port of the service to be prioritized (example: SSH uses port 22)

Click on **Create service** to save the settings and apply the new rule.

### Spam Training

Select **Services** from the menu bar at the top of the screen, then select **Spam Training** from the submenu on the left side of the screen.

SpamAssassin can be configured to learn automatically which emails are spam mails and which are not (so called ham mails). To be able to learn, it needs to connect to an IMAP host and check pre-defined folders for spam and ham messages.

The default configuration is not used for training. All it does is provide default configuration values that are inherited by the real training sources which can be added below. By clicking on the **Edit default configuration** link a new pane appears where the default values can be set:

- Default IMAP host - the IMAP host that contains the training folders
- Default username - the login name for the IMAP host
- Default password - the password of the user
- Default ham folder - the name of the folder that contains only ham messages
- Default spam folder - the name of the folder that contains only spam messages
- Schedule an automatic spam filter training - the interval between checks. This can either be disabled or be an hourly, daily, weekly, or monthly interval. For exact information about the scheduled time you can move your mouse cursor over the question mark next to the chosen interval.

Spam training sources can be added in the section below. By clicking on the **Add IMAP spam training source** link a new pane appears. The options for the additional training hosts are similar to the default configuration options. The only thing that is missing is the scheduling. This will always be inherited from the default configuration.

Three additional options are available.

- Enabled - if this box is ticked the training source will be used whenever spamassassin is trained
- Remark - in this field it is possible to save comment to remember the purpose of this source at a later time

Delete processed mails - if this box is ticked mails will be deleted after they have been processed

The other options can be defined just like in the default configuration. If they are defined they override the default values. To save a source it is necessary to click on the **Update Training Source** button after all desired values have been set.

A source can be tested, enabled, disabled, edited or removed by clicking on the appropriate icon in its row. The icons are explained in the legend at the bottom of the page.

It is also possible to check all connections by clicking on the **Test all connections** button. Note that this can take some time if many training sources have been defined or the connection to the IMAP servers is slow.  
To start the training immediately the **Start training now** has to be clicked. It is important to note that training can take a long time depending on the number of sources, the connection speed and most importantly on the number of emails that will be downloaded.

You can also train the antispam engine manually if the SMTP Proxy is enabled for incoming as well as for outgoing mails.  
This is done by sending spam mails to spam@spam.spam. Non-spam mails can be sent to ham@ham.ham.  
For this to work it is necessary that spam.spam and ham.ham can be resolved. Typically this is achieved by adding these two hostnames to the host configuration in **Network**, **Edit hosts**, **Add a host** on your [Oneshield Firewall](#).

## Intrusion detection

Select **Services** from the menu bar at the top of the screen, then select **Intrusion detection** from the submenu on the left side of the screen.

[Oneshield Firewall](#) includes the well known intrusion detection (IDS) and prevention (IPS) system Snort. It is directly built into the IP-firewall (Snort inline). At this time no rules can be added through the web interface, hence Snort is usable only for advanced users that can load their own rules through the command line. Functionality to manage rules from the web interface will be added in a future update.

## High availability

[Oneshield Firewall](#) can be easily run in high availability (HA) mode. At least 2 [Oneshield Firewall](#) machines are required for HA mode: one assumes the role of the active (master) firewall while the others are standby (slave) firewalls.

If the master firewall fails, an election between the slaves will take place and one of them will be promoted to the new master, providing for transparent failover.

### Master setup

To set up such a HA configuration, first set up the firewall that is going to be the master:

1. Execute the setup wizard, filling in all needed informations.
2. Log into the administration web interface, select **Services** from the menu bar at the top of the screen, then select **High availability** from the submenu on the left side of the screen.
3. Set **Enable High Availability** to **Yes** and set **High Availability side** to **Master**.
4. At this point an extra panel appears where the master-specific settings can be configured:  
The **Management network** is the special subnet to which all [Oneshield Firewalls](#) that are part of a HA setup must be connected (either via the **GREEN** interface or via a dedicated physical network). The default is 192.168.177.0/24. Unless this subnet is already used for other purposes there is no need to change this.  
The **Master IP Address** is the first IP address of the management network.  
The **Management port** is the network port that connects this firewall (the master) to the slave or slaves. This can either be the **GREEN** zone (i.e. the management network is physically the same as the **GREEN** network) or it can be a dedicated network port (eth0, eth1, ...), provided the firewall has an interface not yet used and you are planning to have a dedicated physical network for the management network.  
Next, there are some fields that you can fill in if you wish to be notified by email if a failover event takes place.  
Finally, click on **Save**, then **Apply** to activate the settings.

### Slave setup

Setup the the firewall that is going to be the slave:

1. Execute the setup wizard, including the network wizard, filling in all needed information. It is not necessary to configure services etc, since this information will be synchronized from the master. However, it is necessary to register the slave with Oneshield Network.
2. Log into the administration web interface, select **Services** from the menu bar at the top of the screen, then select **High availability** from the submenu on the left side of the screen.
3. Set **Enable High Availability** to **Yes** and set **High Availability side** to **Slave**.
4. At this point an extra panel appears where the slave-specific settings can be configured:  
Choose the **management network** option according to the settings on the master: either **GREEN** zone or a dedicated network port.  
Fill in the **Master IP address (CIDR)** field: 192.168.177.1/24 unless you choose a non-standard management network address for the master.  
Fill in the **Master root password** (the slave needs this to synchronize its configuration from the master).  
Finally, click on **Save**, then **Apply** to activate the settings.  
At this point the slave cannot be reached anymore via its old IP address (factory default or previous **GREEN** address) since it is in standby mode. It is connected to the master only through the management network.  
If you log in to the master again, on the HA page you can see a list of connected slaves. If you click on the **Go to Management GUI** link you can open the slave's administration web interface via the management network (routed via the master firewall).

## Traffic Monitoring

Select **Services** from the menu bar at the top of the screen, then select **Traffic Monitoring** from the submenu on the left side of the screen.

Traffic monitoring is done by ntop and can be enabled or disabled by clicking on the main switch on this page. Once traffic monitoring is enabled a link to the monitoring administration interface appears in the lower section of the page. This administration interface is provided by ntop and includes detailed traffic statistics. ntop displays summaries as well as detailed information. The traffic can be analyzed by host, protocol, local network interface and many other types of information.

For detailed information about the ntop administration interface please have a look at [About](#), [Online Documentation](#) on the ntop administration interface itself or visit the [ntop documentation page](#).

## Chapter 5: The Firewall Menu

Select **Firewall** from the menu bar at the top of the screen.

This section allows setting up the rules that specify if and how IP traffic flows through your [Oneshield Firewall](#).  
Following is a list of links that appear in the submenu on the left side of the screen:

- **Port forwarding / NAT** - configure port forwarding and NAT (network address translation)
- **Outgoing traffic** - allow or disallow outgoing (towards **RED**) traffic - settings are per zone, host, port, etc.
- **Inter-Zone traffic** - allow or disallow traffic between zones
- **VPN traffic** - specify whether hosts connecting through a VPN should be firewalled
- **System access** - grant access to the [Oneshield Firewall](#) host itself  
Each of these subsections will be explained individually in the following chapters.

### Port forwarding / NAT

#### Port forwarding

Select **Firewall** from the menu bar at the top of the screen, then select **Port forwarding / NAT** from the submenu on the left side of the screen.

Port forwarding grants limited network access from the external **RED** zone (typically the internet) to hosts on an internal zone, such as the DMZ (**ORANGE**) or even the trusted LAN (**GREEN**). However, forwarding to the **GREEN** zone is not recommended from a security point of view.

You can define which port on which external interface (incoming port) will be forwarded to a given host/port on the inside (destination). Typical use cases might be to forward port 80 on an external interface to a webserver in the DMZ or to forward port 1022 on an external interface to a SSH server on port 22 of a host in the DMZ. You need to supply the following parameters:

Protocol - protocol: TCP, UDP, GRE (generic routing encapsulation - used by tunnels) or all  
Incoming IP - the (external) interface  
Port on incoming - which port (1 - 65535) to listen to on the external interface

- Destination IP - the IP of the destination host to which incoming traffic is forwarded to
- Destination Port - the port (1–65535) on the destination host to which incoming traffic is forwarded to
- Remark - a remark for you to remember the purpose of the forward rule later
- Enabled - check to enable rule (default)
- SNAT incoming connections - specify whether incoming traffic should appear to be originating from the firewall IP instead of the actual IP
- Enable log - log all packets that match this rule

Click the **Add** button to confirm your rule. You can then disable/enable, edit or delete each rule from the list by clicking on the appropriate icon on the right side of the table (see the icon legend at the bottom).

After making changes or additions to your rule set, do not forget to click the **Apply** button on the top of the screen!

Once a rule is defined, you can limit access to the forwarding destination from the external **RED** zone. To do so, you need to click on the plus-icon ("Add external access") next to the rule: this allows limiting access to a given source (host or network address). You can do this repeatedly to add more sources. A use case for this would be to grant SSH access to the external port 1022 only to one trusted external IP from the internet.

#### Source NAT

In this section you can define to which outgoing connections source network address translation (Source NAT) should be applied. Source NAT can be useful if a server behind your **Oneshield Firewall** has its own external IP and outgoing packets should therefore not use the **RED** IP address of the firewall. Adding Source NAT rules is similar to adding port forwarding rules. The following options are available:

- Source - In this field you can specify whether outgoing connections that are initiated from a network or IP address, or connections initiated by a VPN user should be Source NATed. If you choose the first **Type** you must then enter IP or network addresses into the textarea below (one address per line). If you choose the second **Type** you can select the users you want from the multiselection field below.
- Destination - In this field you can specify whether connections to a **Zone/VPN/Uplink**, to a **Network/IP** or to a **User** should be NATed. If you choose the first **Type** you must then select a zone, a VPN or an uplink from the multiselection field below. If you choose the second **Type** you must enter IP or network addresses into the textarea below (one address per line). If you choose the third **Type** you can select the users you want from the multiselection field below.
- Service/Port - Here you can specify the service that should be NATed. In the **Service** selectbox you can select pre-defined values for different protocols. If you want to specify a service yourself you must select the protocol in the **Protocol** selectbox and, should you want to add a port as well, enter the destination ports into the **Destination port** textarea (one port per line).
- NAT - Here you can choose whether you want to apply Source NAT or not. If you choose to use source network address translation you can select the IP address that should be used. The **Auto** entries will automatically choose the IP address depending on the outgoing interface.  
In certain cases you may want to explicitly declare that no Source NAT should be performed, e.g. if a server in your DMZ is configured with an external IP and you do not want its outgoing connections to have your **RED** IP as source.
- Enabled - Tick this checkbox if the rule should be applied.
- Remark - You can enter a short note here so you can later remember the purpose of this rule.
- Position - Here you can specify after which rule you want to insert this rule.

To save the rule just click on the **Save** button.

Configuring an SMTP server running on IP 123.123.123.123 (assuming that 123.123.123.123 is an additional IP address of your uplink) in the DMZ with source NAT:

1. Configure your **ORANGE** zone as you like.
2. Setup the SMTP server to listen on port 25 on an IP in the **ORANGE** zone.
3. Add a static ethernet uplink with IP 123.123.123.123 to your **Oneshield Firewall** in the **Network, Interfaces** section.
4. Add a source NAT rule and specify the **ORANGE** IP of the SMTP server as source address. Be sure to use **NAT** and set the NATed source IP address to 123.123.123.123.

#### Outgoing traffic

Select **Firewall** from the menu bar at the top of the screen, then select **Outgoing traffic** from the submenu on the left side of the screen.

**Oneshield Firewall** comes with a preconfigured set of rules, that allow outgoing traffic (i.e. "internet access") from the **GREEN** zone with regard to the most common services (HTTP, HTTPS, FTP, SMTP, POP, IMAP, POP3s, IMAPs, DNS, ping). All other services are blocked by default.

Likewise, access to HTTP, HTTPS, DNS and ping is allowed from the **BLUE** zone (WLAN) while only DNS and ping are allowed from the **ORANGE** zone (DMZ).

Everything else is forbidden by default.

In this section you can disable/enable, edit or delete rules by clicking on the appropriate icon on the right side of the table (see the icon legend at the bottom). You can also add your own rules by clicking on the **Add a new firewall rule** link at the top. Please consider that the order of rules is important: the first matching rule decides whether a packet is allowed or denied, no matter how many matching rules might follow. You can change the order of rules using the arrow down/up icons next to each rule.

A rule is defined by the following parameters:

- Source - select a zone or interface, specify one or more network/host addresses or MAC addresses
- Destination - select the entire **RED** zone, one or more uplinks or one or more network/host addresses
- Service Port - the destination service: select a service name from the list or specify a protocol and one or more port numbers (1–65535)
- Action - what should be done with the packet: accept it, deny it (drop it without feedback to the sender) or reject it (let the sender know the firewall dropped the packet)
- Remark - a remark for you to remember the purpose of the firewall rule later
- Position - at what position in the list should the rule be inserted
- Enabled - check to enable this rule (default)
- Log all accepted packets - Log all accepted packets (does not include denied/rejected packets): this is off by default as it will create large volumes of log data

After making changes to a rule, do not forget to click the **Apply** button on the top of the list!

At the bottom of the page you can also find the rules that are set automatically by **Oneshield Firewall** depending on your configuration. It is possible to disable or enable the whole outgoing firewall by using the **Enable Outgoing firewall** toggle. When disabled, all outgoing traffic is allowed (not recommended).

#### Inter-Zone traffic

Select **Firewall** from the menu bar at the top of the screen, then select **Inter-Zone traffic** from the submenu on the left side of the screen.

This section allows you to set up rules that determine how traffic can flow between the different network zones, excluding the **RED** zone.

**Oneshield Firewall** comes with a simple set of preconfigured rules: traffic is allowed from the **GREEN** zone to any other zone (**ORANGE** and **BLUE**) and traffic is allowed within each zone.

Everything else is forbidden by default.

Analogous to the outgoing traffic firewall you can disable/enable, edit or delete rules by clicking on the appropriate icon on the right side of the table. You can also add your own rules by clicking on the [Add a new inter-zone firewall rule](#) link at the top. Please see the preceding section ([Outgoing traffic](#)) for details about handling firewall rules.

The inter-zone firewall can be disabled/enabled as a whole using the [Enable Inter-Zone firewall](#) toggle. When disabled, all traffic is allowed between all zones other than the **RED** zone (not recommended).

### VPN traffic

Select [Firewall](#) from the menu bar at the top of the screen, then select [VPN traffic](#) from the submenu on the left side of the screen.

The VPN traffic firewall allows to add firewall rules applied to hosts that are connected via VPN.

The VPN traffic firewall is normally not active, which means traffic can flow freely between the VPN hosts and hosts in the **GREEN** zone and VPN hosts can access all other zones. Please note that VPN hosts are not subject to the outgoing traffic firewall or the Inter-Zone traffic firewall. If you need to limit access from or to VPN hosts you need to use the VPN traffic firewall.

The handling of the rules is identical to the outgoing traffic firewall.

Please refer to the [Outgoing traffic](#) section in this chapter for details about handling firewall rules.

### System access

Select [Firewall](#) from the menu bar at the top of the screen, then select [System access](#) from the submenu on the left side of the screen.

In this section you can set up rules that grant or deny access to the [Oneshield Firewall](#) itself.

There is a list of preconfigured rules that cannot be changed. This is to guarantee the proper working of the firewall, since these rules are automatically created as they are required by the services the firewall provides. Click on the >> button labeled "Show rules of system services" to show these rules.

Click on the [Add a new system access rule](#) link to add your own custom rules here. The following parameters describe the rule:

- Source address - specify one or more network/host addresses or MAC addresses
- Source interface - specify a zone or interface
- Service/Port - the destination service: select a service name from the list or specify a protocol and one or more port numbers (1-65535)
  - Action - what should be done with the packet: accept it, deny it (drop it without feedback to the sender) or reject it (let the sender know the firewall dropped the packet)
  - Remark - a remark for you to remember the purpose of the system access rule later
  - Position - at what position in the list should the rule be inserted
  - Enabled - check to enable rule (default)
- Log all accepted packets - Log all accepted packets (besides denied/rejected packets): this is off by default as it will create large volumes of log data

Click the [Add](#) button to confirm your rule. You can then disable/enable, edit or delete each rule from the list of rules by clicking on the appropriate icon on the right side of the table (see the icon legend at the bottom).

After making changes or additions to your rule set, do not forget to click the [Apply](#) button on the top of the list!

## Chapter 6: The Proxy Menu

Select [Proxy](#) from the menu bar at the top of the screen.

A proxy is a service on your [Oneshield Firewall](#) that can act as a gatekeeper between clients (e.g. a web browser) and network services (e.g. a web server on the internet). Clients connect to the proxy which in turn can retrieve, cache, filter and potentially block the information from the original server. A proxy is called transparent if all traffic goes through it, of the client's configuration. Non-transparent proxies hence rely on the collaboration of the client (e.g. the proxy settings of your web browser).

Following is a list of proxies that are available on [Oneshield Firewall](#). Each proxy can be configured via the links that are in the submenu on the left side of the screen:

- [HTTP](#) - configure the web proxy including authentication, content filter and antivirus
  - [POP3](#) - configure the proxy for retrieving mail via the POP protocol, including spam filter and antivirus
  - [SIP](#) - configure the proxy for the session initiation protocol (SIP) used by voice over IP systems
  - [FTP](#) - enable or disable the FTP proxy (check files that are downloaded via FTP for viruses)
  - [SMTP](#) - configure the proxy for sending or retrieving mail via the SMTP protocol, including spam filter and antivirus
  - [DNS](#) - configure the caching domain name server (DNS) including anti-spyware
- Each section will be explained individually below.

### HTTP

Select [Proxy](#) from the menu bar at the top of the screen, then select [HTTP](#) from the submenu on the left side of the screen.

#### Configuration

Click on the [Enable HTTP Proxy](#) toggle to enable the HTTP proxy ([Oneshield Firewall](#) uses the Squid caching proxy). Once the proxy is up and running, a number of controls appear.

First of all, you can define the way users in each zone (**GREEN** and, if enabled also **ORANGE**, **BLUE**) can access the proxy. Per zone choices are:

- disabled - the proxy server is not available in the given zone
- no authentication - the proxy server is available to anyone (no need to log in), but you need to configure your browser manually
- authentication required - users need to configure their browser manually and need to log in in order to use the proxy server
- transparent - the proxy server is available to anyone and no browser configuration is needed (HTTP traffic is intercepted by the proxy server)

Some browsers, including Internet Explorer and Firefox, are able to automatically detect proxy servers by using the Web Proxy Autodiscovery Protocol (WPAD). Most browsers also support proxy auto-configuration (PAC) through a special URL. When using an [Oneshield Firewall](#) the URL looks like this: `http://<IP OF YOUR FIREWALL>/proxy.pac`.

Next, comes a section with global configuration options:

- Proxy port - the TCP port used by the proxy server (defaults to 8080)
- Visible hostname - the proxy server will assume this as its hostname (will also show at the bottom of error messages)
- Cache administrator email - the proxy server will show this email address in error messages
- Language of error messages - the language in which error messages are displayed
- Max upload size - limit for HTTP file uploads (such as used by HTML forms with file uploads) in KB (0 means unlimited)

Then you will find a number of additional options, each in its own panel that can be expanded by clicking on the + icon:

Allowed Ports and SSL Ports

- Ports - list the TCP destination ports to which the proxy server will accept connections when using HTTP (one per line, comments start with #)
  - SSL Ports - as above, but when using HTTPS instead of HTTP
  - Log settings
    - Log enabled - log all URLs being accessed through the proxy (master switch)
    - Log query terms - also log parameters in the URL (such as ?id=123)
    - Log user-agents - also log user agents, i.e. which web browsers access the web
    - Log contentfiltering - also log when content is filtered
  - Firewall logs outgoing connections - have the firewall log web accesses (transparent proxies only)
    - Allowed Subnets per Zone
      - GREEN / ORANGE / BLUE - for each zone that the proxy serves you can define which subnets are allowed to access the proxy (defaults to all subnets associated with the respective zone) - give one subnet per line (example: 172.16.1.0/255.255.255.0 or 172.16.1.0/24). Note: there should be at least one entry for each active zone. If you do not want to allow connections from a whole zone, then rather disable the proxy on that zone using the select boxes below the Enable HTTP Proxy toggle.
    - Bypass / Banned Sources and Destinations
      - Bypass transparent proxy - specify sources (upper left panel) or destinations (upper right panel), that are not subject to transparent proxying; give one subnet, IP address or MAC address per line
      - Bypass proxy filter - specify source IP addresses (mid left panel) or source MAC addresses (mid right panel) that, while still passing through the proxy, are not subject to filtering
      - Banned clients - specify source IP addresses (lower left panel) or source MAC addresses (lower right panel) that are banned (unconditionally blocked by the proxy)
    - Cache management
      - Harddisk / Memory cache size - give the amount of memory the proxy should allocate for caching web sites, respectively on disk or in RAM (in Megabytes)
      - Max / Min object size - give upper and lower size limits of objects that should be cached (in Kilobytes)
      - Enable offline mode - if this option is on, the proxy will never try to update cached objects from the upstream webserver - clients can then browse cached, static websites even after the uplink went down
      - Do not cache these domains - in this textarea you can specify which domains should not be cached (one domain per line)
    - Upstream proxy
      - Upstream proxy - use this option to make your Oneshield Firewall's proxy connect to another (upstream) proxy; specify the upstream proxy as "host:port"
  - upstream username / password - specify credentials, if authentication is required for the upstream proxy
  - Username / client IP forwarding - forward the username / client IP address to the upstream proxy
- Click the Save button to confirm and save the configuration changes. Do not forget to click the Apply button to restart the proxy for the changes to become active.

The Clear cache button allows to delete all web pages and files cached by the HTTP proxy.

#### Authentication

Oneshield Firewall's proxy supports four different authentication types: Local, LDAP, Windows, Radius. Each of these types needs different configuration parameters and is described below. However, the global configuration parameters are:

- Number of authentication processes - the number of authentication processes that can run simultaneously
- Authentication cache TTL (in minutes) - the time in minutes how long authentication data should be cached
- Limit of IP addresses per user - the maximum number of IP addresses from which a user can connect to the proxy simultaneously
- User / IP cache TTL (in minutes) - the time in minutes how long an IP address will be associated with the logged in user
- Authentication realm prompt - this text will be shown in the authentication dialog
- Require authentication for unrestricted source addresses - if you disable this unrestricted source addresses will not have to provide their credentials
- Domains without authentication - in this textarea you can enter domain names that can be accessed without being authenticated (one per line)
- Sources (SUBNET / IP / MAC) without authentication - in this textarea you can enter source subnets, IP addresses or MAC addresses that do not require authentication (one per line)

The following parameters are available for local authentication.

- User management - Click on this button if you want to manage local users.
- Min password length - Here you can set the minimum password length for local users.

The following parameters are available for LDAP authentication.

- Base DN - the base distinguished name, this is the start point of your search
- LDAP type - here you can choose whether you are using an Active Directory server, a Novell eDirectory server, a LDAP version 2 server or a LDAP version 3 server
- LDAP server - the IP address or fully qualified domain name of your LDAP server
- Port - the port on which the server is listening
- Bind DN username - the fully distinguished name of a bind DN user, the user must have permission to read user attributes
- Bind DN password - the password of the user
- user objectClass - the bind DN user must be part of this objectClass
- group objectClass - the bind DN user must be part of this objectClass

The following parameters are available for Windows authentication.

- Domain - the domain you want to join
- PDC hostname - the hostname of the primary domain controller
- BDC hostname - the hostname of the backup domain controller
- Username - the username you want to use to join the domain
- Password - the user's password
- Join Domain - click here to join the domain
- Enable user-based access restrictions - if you tick this checkbox you can add authorized and unauthorized users to the textfields that will appear below
- Use positive/negative access control - you can choose whether you want to use positive or negative access control, in the textfields you can enter one user per line that should have access or should not have access, depending on the access control policy you chose

The following parameters are available for Radius authentication.

- RADIUS server - the address of the RADIUS server
- Port - the port on which the RADIUS server is listening

- Identifier - an additional identifier
- Shared secret - the password to be used
- Enable user-based access restrictions - if you tick this checkbox you can add authorized and unauthorized users to the textfields that will appear below
- Use positive/negative access control - you can choose whether you want to use positive or negative access control, in the textfields you can enter one user per line that should have access or should not have access, depending on the access control policy you chose

#### Use native Windows authentication with Active Directory

In order to be able to use Windows' native authentication with active directory you have to make sure that a few conditions are met:

- The firewall must join the domain.
- The system clocks on the firewall and on the active directory server have to be in sync.
- In the Proxy, DNS, Custom nameserver a custom nameserver has to be entered.
- The firewall must be able to resolve the name of the Active Directory server (e.g. through an entry in Network, Edit hosts).
- The realm must be a fully qualified domain name.
- The PDC hostname has to be set to the netbios name of the Active Directory server.

#### Default policy

The default policy applies to all users of the proxy, whether they are authenticated or not. Policy settings include a simple user agent and MIME type filter as well as advanced time-based virus scanning and content filtering rules.

- Restrict allowed clients for web access - This checkbox activates the user agent filter, it restricts web access to the selected user agents.
- Max download size - This sets the limit for HTTP file downloads in KB (0 means unlimited).
- Block MIME types - Enabling this option will activate a filter which checks incoming headers for their MIME type. If the MIME type of the incoming file is set to be blocked, access will be denied. This way you can block files not corresponding to the company policy (for example multimedia files).
- Allowed clients for web access - Here you can choose allowed clients and browsers from a list after clicking on the + icon.
- Blocked MIME types - You can specify blocked MIME types by clicking on the + icon and then adding one type per line. The syntax conforms to the standard defined by the IANA. Examples: application/javascript, audio/mpeg, image/gif, text/html, video/mpeg

Click the Save button to save the default policy settings.

You can view your own rules in the Rule list. Any rule can specify if web access is blocked or allowed, in this last case you can activate and select a filter type. To add a new rule just click on Create a rule and the following settings can be performed:

- Web access - Specify whether the rule allows web access or blocks it; also state whether it has effect all day long or at a specific time: choose the days of the week on which you want this rule to be applied and, in case the rule is not valid all day long, you can also set the time range.
  - Source - Here you can choose to connections from which sources this rule will be applied. This can be either <ANY> a Zone or a list of Network/IP addresses (one address per line).
  - Destination - Here you can choose connections to which destinations will be affected by this rule. This can be either <ANY>, a Zone, a list of Network/IP addresses (one address per line) or a list of domains (one domain per line).
  - Filter type - Choose antivirus scan only to create a rule which only scans for viruses, choose content filter only to create a rule which analyzes the content of web pages and filters it according to the settings in the Content filter section. If you choose unrestricted no checks will be performed.
  - Position - Specify where to place the new rule. Larger numbers have higher priority.
- If you tick the check box Activate antivirus scan on the Proxy, HTTP, Content filter page then all rules (new ones and old ones) marked as content filter only are changed to content filter + antivirus. This means that antivirus filter and content filter work concurrently.

You can then change priority, edit or delete each rule from the list of rules by clicking on the appropriate icon on the right side of the table (see the icon legend at the bottom)

#### Content filter

Firstly, in order to use the content filter, you have to use Content filter as filter type in a rule (either in Default policy or Policy profiles). Oneshield Firewall's Content Filter (DansGuardian) takes advantage of three filtering techniques.

The first is called PICS (Platform for Internet Content Selection), it is a specification created by W3C that uses metadata to label webpages to help parental control. The second is based on an advanced phrase weighting system, it analyzes the text of web pages and calculates a score for each page. The last method takes advantage of a huge list of categorized URLs and domains, all URLs requested are compared with the blacklist before being served to clients.

The screen is divided into a general configuration section and a section where the specific filtering policy can be chosen.

- Activate antivirus scan - Enable both the content filter (Dansguardian) and the antivirus proxy (HAVP).
- Enable logging - Log blocked requests.
- Platform for Internet Content Selection - Enable parental control based on PICS metadata.
- Max. score for phrases - Specify the maximum score level of a trustworthy page (50-300). You can tune this level: if children browse the web through Oneshield Firewall you should set a value of about 50, for teenagers it should be 100 and for young adults 160.
- Content Filter - This section allows filter configuration based on phrase analysis. You can block or allow categories of sites by clicking on the icon beside it. Subcategories are shown when clicking on the + icon.
- URL Blacklist - This section allows configuration of filtering based on URL comparison. You can block or allow categories of sites by clicking on the icon beside the category name. Subcategories are shown by clicking on + icon.
- Custom black and white lists - Content filtering may cause false positives and false negatives - here you can list domains that should always be blocked or allowed regardless of the results of the content filter's analysis.

Phrase analysis requires much more computing power than other technologies (PICS and URL blacklist). If you wish to disable this filtering technique you can mark all categories as allowed in the Content Filter section.

When whitelisting a domain always make sure to whitelist all necessary domains for that site to work as well.

An example:

- google.com is blocked, which means all subdomains of google.com are blocked as well
- maps.google.com is whitelisted so you can access it
- maps.google.com does not work like it should because it tries to get data from other google servers
- you will have to whitelist these domains (e.g. mt0.google.com) as well

Click on Save to save the settings of content filter.

## Antivirus

In this section you can configure the virus scanner engine (ClamAV) used by the HTTP proxy.

- Max. content scan size - Specify the maximum size for files that should be scanned for viruses.
- Do not scan the following URLs - A list of URLs that will not be scanned for viruses (one per line).
- Last update - Shows the day and time of the last virus signatures update and the total amount of viruses recognized by ClamAV (in parenthesis).

Click on **Save** to save the settings of the virus scanner engine.

## Group policies

On this page you can create groups that can be associated to different policy profiles. These groups can be associated to users when using Local authentication in the [Proxy, HTTP, Authentication](#) section.

You can add a group by clicking on the [Create a group](#) link and entering a group name. After clicking on the [Create group](#) button the group is saved. The profile of the groups can be changed by selecting the appropriate policy profile and then clicking on the [Save](#) button below the group list. Groups can be deactivated, activated and removed by clicking on the respective icons (as described in the legend below the list).

## Policy profiles

It is possible to create additional profiles that can be used in the [Proxy, HTTP, Group policies](#) section. Policy profiles are created just like the default policy in the [Proxy, HTTP, Default policy](#) section.

## POP3

Select [Proxy](#) from the menu bar at the top of the screen, then select [POP3](#) from the submenu on the left side of the screen. In this section you can configure the POP3 (incoming mail) proxy.

### Global settings

On this page you can configure the global configuration settings of the POP3 proxy. You can enable or disable the POP3 proxy for every zone. It is also possible to enable the [Virus scanner](#) and the [Spam filter](#) for incoming emails. If you want to log every outgoing POP3 connection you can enable the [Firewall logs outgoing connections](#) checkbox.

### Spam filter

On this page you can configure how the POP3 proxy should react once it finds a spam email.

- Spam subject tag - Here you can specify a prefix for the spam email's subject.
- Required hits - This option defines how many hits are required for a message to consider it spam. The default value is 5.
- Enable message digest spam detection(pyzor) - If you want to detect spam using message digests you can enable this option. Note that this might slow down your POP3 proxy.
- White list - Here you can whitelist sender email-addresses (one address per line). It is also possible to whitelist whole domains by using wildcards, e.g. \*@example.com.
- Black list - Here you can blacklist sender email-addresses (one address per line). It is also possible to blacklist whole domains by using wildcards, e.g. \*@example.com.

## SIP

Select [Proxy](#) from the menu bar at the top of the screen, then select [SIP](#) from the submenu on the left side of the screen.

The SIP Proxy is a proxy/masquerading daemon for the SIP and RTP protocols. SIP (Session Initiation Protocol, RFC3261) and RTP (Real-time Transport Protocol) are used by Voice over IP (VoIP) devices to establish telephone calls and carry voice streams.

The proxy handles registrations of SIP clients on the LAN and performs rewriting of the SIP message bodies to make SIP connections possible through [Oneshield Firewall](#) and therefore allow SIP clients (like x-lite, kphone, linphone or VoIP hardware) to work behind NAT. Without this proxy, connections between clients are not possible at all if both are behind NAT, since one client cannot reach the other directly and therefore no RTP connection can be established between them.

Once enabled, the following options can be configured (confirm the settings by clicking [Save](#)).

- Status - transparent means all outgoing traffic to the SIP port will be automatically redirected to the SIP proxy; enabled means the proxy will listen to the SIP port and clients need to be made aware of the proxy
- SIP Port - default: 5060
- RTP Port Low / High - The UDP Port range that the SIP proxy will use for incoming and outgoing RTP traffic. By default the range from 7070 to (and including) 7090 is used. This allows up to 10 simultaneous calls (2 ports per call). If you need more simultaneous calls, increase the range.
- Outbound proxy host / port - The SIP Proxy itself can send all traffic to another outbound proxy.
- Autosave registrations - This allows the SIP proxy to remember registrations after a restart.
- Log calls - Check this if you want to log established calls in the SIP proxy log.
- [Firewall logs outgoing connections](#) - This will show outgoing connections in the firewall log.

## FTP

Select [Proxy](#) from the menu bar at the top of the screen, then select [FTP](#) from the submenu on the left side of the screen.

The FTP (File Transfer Protocol) proxy is available only as transparent proxy, this allows scanning for viruses on FTP downloads. Note that only connections to the standard FTP port (21) are redirected to the proxy. This means that if you configure your clients to use the HTTP proxy also for the FTP protocol, this FTP proxy will be bypassed!

You can enable the transparent FTP proxy on the [GREEN](#) zone and on the other enabled zones ([ORANGE](#), [BLUE](#)). The following options can be configured (confirm the settings by clicking [Save](#)).

- [Firewall logs outgoing connections](#) - Show outgoing connections in the firewall log.
- Bypass the transparent Proxy - Specify sources (left panel) or destinations (right panel), that are not subject to transparent FTP proxying. Always specify one subnet, IP address or MAC address per line.  
[Oneshield Firewall](#) supports transparent FTP proxying with frox if and only if it is directly connected to the internet. If you have another NATing firewall or router between [Oneshield Firewall](#) and the internet, frox does not work because it uses an active FTP upstream.

## SMTP

Select [Proxy](#) from the menu bar at the top of the screen, then select [SMTP](#) from the submenu on the left side of the screen.

The SMTP (simple mail transfer protocol) proxy can relay and filter email traffic as it is being sent towards email servers.

The scope of the SMTP proxy is to control and optimize SMTP traffic in general and to protect your network from threats when using the SMTP protocol. The SMTP (Simple Mail Transport Protocol) protocol is used whenever an email is sent by your mail client to a remote mail server (outgoing mail). It will also be used if you have your own mail server running on your LAN ([GREEN](#) interface) or your DMZ ([ORANGE](#) interface) and are allowing mails to be sent from the outside of your network (incoming requests) through your mail server. The SMTP proxy configuration is split into several subsections.

### Warning

In order to download mail from a remote mailserver with your local mail clients, the POP3 or IMAP protocol will be used. If you

want to protect that traffic too, you have to enable the POP3 proxy in Proxy, POP3. Scanning of IMAP traffic is currently not supported. With the mail proxy functionality, both sorts of traffic (incoming and outgoing mail) can be scanned for viruses, spam and other threats. Mail will be blocked if necessary and notices will be sent to both the receiving user and the administrator. With the possibility to scan incoming mail, the mail proxy can handle incoming connections and pass the mail to one or more internal mail servers in order to remove the necessity to have SMTP connections from the outside within your local networks.

## Main

This is the main configuration section for the SMTP proxy. It contains the following options:

- Enabled - This enables the SMTP proxy in order to accept requests on port 25.
- Transparent on GREEN, BLUE, ORANGE - If the transparent mode is enabled, all requests to destination port 25 will be intercepted and forwarded to the SMTP proxy without the need to change the configuration on your clients.
- Antivirus is enabled - Check this box if you would like to enable antivirus. The antivirus can be configured in the Proxy, SMTP, Antivirus link.
- Spamcheck is enabled - Check this box if you would like to filter spam emails. The spam filter can be configured in the Proxy, SMTP, Spam section.
- File extensions are blocked - Check this box if you would like to block mails that contain attached files with certain extensions. The file extensions can be configured in the Proxy, SMTP, File extensions section.
- Incoming mail enabled - If you have an internal mailserver and would like the SMTP proxy to forward incoming mails to your internal server you must enable this option.
- Firewall logs outgoing connections - Tick this on if you want the firewall to log all established outgoing connections. Note that in some countries this may be illegal.

You need to configure the email domains for which the server should be responsible. You can add the list of domains in the Proxy, SMTP, Domains section.

To save and apply the settings you must click on the Save changes and restart button.

## Antivirus

The Antivirus is one of the main features of the SMTP proxy module. Three different actions can be performed when a mail that contains a virus is sent. It is also possible to configure an email address for notifications.

- Mode - You can choose between three different modes how infected mails should be handled.  
DISCARD: if you choose this mode the mail will be deleted  
BOUNCE: if you choose this mode the email will not be delivered but bounced back to the sender in form of a non-delivery notification  
PASS: if you choose this mode the mail will be delivered normally
- Email used for virus notifications - Here you can provide an email-address that will receive a notification for each infected email that is processed.
- Virus quarantine - Here you can specify what kind of quarantine you are using. Valid values are:
  - leaving this field empty will disable the quarantine.
  - virus-quarantine this stores infected mails on the firewall (in /var/amavis/virusmails), this is the default setting.
  - valid.email@address any valid email address will result in the infected emails being forwarded to that email address.

To save and apply the settings just click on the Save changes and restart button.

## Spam

The antispam module knows several different ways to protect you from spam mails. In general spamassassin and amavisd-new are used to filter out spam. SpamAssassin provides several means of detecting spam. It has a score tally system where large numbers of inter-related rules fire off and total up a score to determine whether a message is spam or not.

The page is divided into two sections: SMTP Proxy and greylisting.

While most simple spam mails such as well known spam messages and mail sent by known spam hosts are blocked, spammers always adapt their messages in order to circumvent spam filters. Therefore it is absolutely necessary to always train the spam filter in order to reach a personalized and stronger filter (bayes).

The SMTP Proxy section contains the main configuration for the spam filter.

- Spam destination - You can choose between three different modes how spam emails should be handled.  
DISCARD: if you choose this mode the email will be deleted  
BOUNCE: if you choose this mode the email will not be delivered but bounced back to the sender in form of a non-delivery notification  
PASS: if you choose this mode the email will be delivered normally
- Email used for notification on spam alert - Here you can provide an email-address that will receive a notification for each spam email that is processed.
- Spam quarantine - Here you can specify what kind of quarantine you are using. Valid values are:
  - leaving this field empty will disable the spam quarantine.
  - spam-quarantine this stores spam mails on the firewall (in /var/amavis/virusmails), this is the default setting.
  - valid.email@address any valid email address will result in the spam emails being forwarded to that email address.
- Spam tag level - If SpamAssassin's spam score is greater than this number X-Spam-Status and X-Spam-Level headers are added to the email.
- Spam mark level - If SpamAssassin's spam score is greater than this number mails are tagged with the Spam subject and an X-Spam-Flag header.
- Spam quarantine level - Mails that exceed this spam score will be moved to the quarantine.
- Send notification only below level - Send notification emails only if the spam score is below this number.
- Spam subject - Here you can specify a prefix for the subject of marked spam emails.

The second section contains configuration options for Oneshield Firewall's greylisting. It contains the following options:

- greylisting enabled - Check this box if you want to enable greylisting.
- delay(sec) - The greylisting delay in seconds can be a value between 30 and 3600.
- Whitelist recipient - You can whitelist email-addresses or whole domains in this textarea, e.g. test@Oneshield.com or the domain Oneshield.com (one entry per line).
- Whitelist client - You can whitelist a mailserver's address here. This means that all emails coming from this server's address will not be checked for spam (one entry per line).

Save the settings and restart the SMTP Proxy by clicking on the Save changes and restart button.

## File Extensions

This allows you to block files with certain file extensions which may be attached to mails. Mails which contain such attachments will be recognized and the selected action will be performed for the respective mail. The following options can be configured:

- Blocked file extensions - You can select one or more file extensions to be blocked. In order to select multiple files press the control key and click on the desired entries with your mouse.

- Banned files destination - You can choose between three different modes how emails that contain such attachments should be handled.  
DISCARD: if you choose this mode the email will be deleted  
BOUNCE: if you choose this mode the email will not be delivered but bounced back to the sender in form of a non-delivery notification  
PASS: if you choose this mode the email will be delivered normally
  - Banned files quarantine - Here you can specify what kind of quarantine you are using. Valid values are:
    - leaving this field empty will disable the quarantine for mails with blocked attachments.
    - `spam-quarantine` this stores mails with blocked attachments on the firewall (in `/var/amavis/virusmails`), this is the default setting.
    - `valid.email@address` any valid email address will result in the emails with blocked attachments being forwarded to that email address.
  - Email used for notification on banned files - Whenever an email with an attachment that is blocked due to its file extension is found, a notification email is sent to this address.
  - Block double extensions - If you enable this option, files with double extensions will be blocked since these files are usually created to harm computers (blocked double extensions are composed of any extension followed by `.exe`, `.com`, `.vbs`, `.pif`, `.scr`, `.bat`, `.cmd` or `.dll`).
- Save the settings and restart the SMTP Proxy by clicking on the **Save changes and restart** button.

#### Blacklists/Whitelists

An often used method to block spam e-mails are so called real-time blacklists (RBL). These lists are created, managed and updated by different organisations. If a domain or a sender IP address is listed in one of the blacklists, emails from it will be refused without further notice. This saves more bandwidth than the RBL of the antispam module, since here mails will not be accepted and then handled, but dismissed as soon as a listed IP address is found. This dialogue also gives you the possibility to explicitly block (blacklist) or allow (whitelist) certain senders, recipients, IP addresses or networks.

#### Warning

Sometimes it may happen that IP addresses have been wrongly listed by the RBL operator. If this should happen, it may negatively impact your communication, to the effect that mail will be refused without the possibility to recover it. You also have no direct influence on the RBLs.

In the RBL section you can enable the following lists:

- `bl.spamcop.net` - This RBL is based on submissions from its users ([www.spamcop.net](http://www.spamcop.net)).
- `zen.spamhaus.org` - This list replaces `sbl-xbl.spamhaus.org` and contains the Spamhaus block list as well as Spamhaus' exploits block list and its policy block list.
- `cbl.abuseat.org` - The CBL takes its source data from very large spamtraps. It only lists IPs exhibiting characteristics which are specific to open proxies of various sorts (HTTP, socks, AnalogX, wingate etc.) which have been abused to send spam, worms/viruses that do their own direct mail transmission, or some types of trojan-horse or "stealth" spamware, without doing open proxy tests of any kind.
- `dul.dnsbl.sorbs.net` - This contains a list of Dynamic IP Address ranges ([www.au.sorbs.net](http://www.au.sorbs.net)).
- `list.dsbl.org` - DSBL is the Distributed Sender Blackhole List. It publishes the IP addresses of hosts which have sent special test emails to `listme@listme.dsbl.org` or another listing address. The main delivery method of spammers is the abuse of non-secure servers. For that reason many people want to know which servers are non-secure so they can refuse email from these servers. DSBL provides exactly that information ([www.dsbl.org](http://www.dsbl.org)).
- `dsn.rfc-ignorant.org` - This is a list which contains domains or IP networks whose administrators choose not to obey to the RFCs, the standards of the net ([www.rfc-ignorant.org](http://www.rfc-ignorant.org)).
- `ix.dnsbl.manitu.net` - A publicly available DNS blacklist which is permanently regenerated from the IP blacklist and the spam hash table of the spam filter NIX Spam.

Save the settings and restart the SMTP Proxy by clicking the **Save changes and restart** button.

#### Note

Advanced users can modify the list by editing the file `/var/efw/smtpd/default/RBL`.

You can also create custom black- and whitelists by adding entries to the fields in the `blacklist/whitelist` section. The following textareas can be filled out in this section:

- `sender whitelist` - Mails from these addresses or domains will always be accepted.
- `sender blacklist` - Mails from these addresses or domains will never be accepted.
- `recipient whitelist` - Mails to these addresses or domains will always be accepted.
- `recipient blacklist` - Mails to these addresses or domains will never be accepted.
- `client whitelist` - Mails that have been sent from these IP addresses or hosts will always be accepted.
- `client blacklist` - Mails that have been sent from these IP addresses or hosts will never be accepted.

To save the changes and restart the SMTP proxy click on the **Save changes and restart** button.

Examples for recipient/sender black- and whitelists:

- a whole domain - `example.com`
- only subdomains - `.example.com`
- a single address - `admin@example.com`

#### Domains

If you have enabled incoming mail and would like to forward that mail to a mail server behind your **Oneshield Firewall** - usually set up in the **GREEN** or **ORANGE** zone - you need to declare the domains which will be accepted by the SMTP proxy and to which of your mail servers the incoming mail should be forwarded to. It is possible to specify multiple mail servers behind Oneshield Firewall for different domains. It is also easily possible to use Oneshield Firewall as a backup MX.

- Domain - The domain this mailservers is responsible for.
- Internal mailservers - The address of the mailservers.

To add a domain click the **Add** button. To apply the changes the SMTP proxy has to be restarted by clicking on the **Save changes and restart** button. Existing entries can be edited and deleted by clicking on the respective icon (as described in the legend at the bottom of the page).

#### Mail Routing

This option allows you to send a blind carbon copy (BCC) to a specified email address. This option will be applied to all emails that are sent to the specified recipient address or are sent from the specified sender address.

- Direction - Specify whether you want to apply this copying process for a certain Sender or Recipient.
- Mail address - Here you specify the mail address of the recipient or sender (depending on what you have chosen above).
- BCC address - The mail address where you want to send the copy of the emails.

The mail route is saved by clicking on the **Add mail route** button. Existing entries can be changed or deleted by clicking on the respective icons which are explained in the legend at the bottom of the page.

#### Warning

Neither the sender nor the recipient will be notified of the copy. In most countries of this planet it is highly illegal to read other people's private messages. Do not abuse this feature.

#### Advanced

On this page you can configure the advanced settings of the SMTP proxy. In the Smarthost section the following options can be configured:

- Smarthost enabled for delivery - Check this box if you want to use a smarthost to deliver emails.
- Address of smarthost - Here you can enter the address of the smarthost.
- Authentication required - Check this box if the smarthost requires authentication.
  - Username - This username is used for authentication.
  - Password - This password is used for authentication
- Authentication method - Here you can choose the authentication methods that are supported by your smarthost. PLAIN, LOGIN, CRAM-MD5 and DIGEST-MD5 are supported.

The settings are saved and applied by clicking on the **Save changes and restart** button.

If you have a dynamic IP address because you are using an ISDN or an ADSL dialup internet connection you might get problems sending mails to other mail servers. More and more mail servers check whether your IP address is listed as a dynamic IP address and therefore might refuse your emails. Hence it could be necessary to use a smarthost for sending emails. A smarthost is a mail server which your SMTP proxy will use as outgoing SMTP server. The smarthost needs to accept your emails and relays them for you. Normally you may use your provider's SMTP server as smarthost, since it will accept to relay your emails while other mail servers may not.

In the IMAP Server for SMTP Authentication section you can configure which IMAP server should be used for authentication when sending emails. Most of all this is important for SMTP connections that are opened from the **RED** zone. The following settings can be configured:

- Authentication enabled - Check this box if you want to enable IMAP authentication.
- IMAP server - Here you can enter the address of the IMAP server.
- Number authentication daemons - This settings defines how many concurrent logins should be possible through your **Oneshield Firewall**.

The settings are saved and applied by clicking on the **Save changes and restart** button.

In the Advanced settings additional parameters can be defined. The options are:

- smtpd HELO required - If this is enabled the connecting client must send a HELO (or EHLO) command at the beginning of an SMTP session.
- reject invalid hostname - Reject the connecting client when the client HELO or EHLO parameter supplies an invalid hostname.
- reject non-FQDN sender - Reject the connecting client if the hostname supplied with the HELO or EHLO command is not a fully-qualified domain name as required by the RFC.
- reject non-FQDN recipient - Reject the request when the RCPT TO address is not in fully-qualified domain name form, as required by the RFC.
- reject unknown sender domain - Reject the connection if the domain of the sender email address has no DNS A or MX record.
- reject unknown recipient domain - Reject the connection if the domain of the recipient email address has no DNS A or MX record.
- SMTP HELO name - The hostname to send with the SMTP EHLO or HELO command. The default value is the IP of RED. Specify a hostname or IP address.
- Always BCC address - Optionally you can enter an email address here that will receive a blind carbon copy of each message that goes through the SMTP proxy.
- smtpd hard error limit - The maximum number of errors a remote SMTP client is allowed to produce without delivering mail. The SMTP Proxy server disconnects once this limit is exceeded (default 20).
- Language email templates - The language in which error messages should be sent.
- maximal email size - The maximum size a single message is allowed to have.

The settings are saved and applied by clicking on the **Save changes and restart** button.

#### DNS

Select **Proxy** from the menu bar at the top of the screen, then select **DNS** from the submenu on the left side of the screen.

In this section you can change the settings for the DNS proxy. It is divided into three subpages.

##### DNS proxy

On this page you can enable the transparent DNS proxy for the **GREEN**, **ORANGE** and **BLUE** zones (if they are active).

You can also define for which source addresses the proxy will be bypassed in the lower left textarea. These sources can be IP addresses, addresses of subnets and MAC addresses (one per line).

In the lower right textarea you can enter destinations for which the proxy is bypassed. In this textarea IP addresses and addresses of subnets can be entered. To save the settings you must click on the **Save** button.

##### Custom nameserver

On this page you can add custom nameservers for specific domains. You can add a new custom nameserver by clicking on the **Add new custom name server** for a domain link. To change an existing entry you have to click on the pencil icon in its row. Clicking on a trash can icon will delete the custom nameserver in that row.

The following details can be saved for custom nameservers:

- Domain - The domain for which you want to use the custom nameserver.
- DNS Server - The IP address of the nameserver.
- Remark - An additional comment you might want to save.

##### Anti-spyware

On this page you can configure how your **Oneshield Firewall** should react if a domain name has to be resolved that is known to be used by spyware. The options that can be set are:

- Enabled - If enabled these requests will be redirected to localhost.
- Redirect requests to spyware listening post - If this is enabled the requests will be redirected to the spyware listening post instead of localhost.
- Whitelist domains - Domain names that are entered here are not treated as spyware targets regardless of the list's content.
- Blacklist domains - Domain names that are entered here are always treated as spyware targets regardless of the list's content
- Spyware domain list update schedule - Here you can specify how often the spyware domain list should be updated. Possible values are Hourly, Daily, Weekly and Monthly. By moving the mouse cursor over the respective question mark you can see when exactly the updates will be performed.

The settings are saved and applied by clicking on the **Save** button.

## Chapter 7: The VPN Menu

Select VPN from the menu bar at the top of the screen.

Virtual private networks (VPNs) allow networks to connect directly to each other over potentially unsafe networks such as the internet. All network traffic through the VPN connection is transmitted securely, inside an encrypted tunnel, hidden from prying eyes. Such a configuration is called a Gateway-to-Gateway VPN. Similarly, a single computer somewhere on the internet can use a VPN tunnel to connect to a trusted LAN. The remote computer, sometimes called a Road Warrior, appears to be directly connected to the trusted LAN while the VPN tunnel is active.

Oneshield Firewall can create VPNs based on the IPsec protocol supported by most operating systems and network equipment, as well as VPNs based on the OpenVPN service.

Unfortunately, the tools needed to set up IPsec vary greatly among different systems, may be complicated to use or may have interoperability issues. Therefore, Oneshield recommends OpenVPN in situations where there is no need to support an existing IPsec infrastructure. Oneshield Firewall includes a user friendly OpenVPN client for Microsoft Windows, Linux and MacOS X.

Following is a list of links that appear in the submenu on the left side of the screen and that allow setting up VPNs of any of the types mentioned:

- OpenVPN server – set up the OpenVPN server so that clients (be it Road Warriors or other Oneshield Firewalls in a Gateway-to-Gateway setup) can connect to your GREEN zone through a VPN tunnel
  - OpenVPN client (Gw2Gw) – set up the client-side of a Gateway-to-Gateway setup between two or more Oneshield Firewalls
  - IPsec – set up IPsec-based VPN tunnels
- Each link will be explained individually in the following sections.

### OpenVPN server

Select VPN from the menu bar at the top of the screen, then select OpenVPN server from the submenu on the left side of the screen.

#### Server configuration

In this panel you can enable the OpenVPN server and define the range of addresses within the GREEN zone that are going to be assigned to connecting clients.

Click on Save to save the settings and start the OpenVPN service. The first time the service is started a new (self-signed) certificate for this OpenVPN server is generated. Click on the Download CA certificate link to download it. You will need it later when setting up the clients.

The following panel shows a list of currently connected clients, once OpenVPN is up and running.

It is possible to kill and ban connections. The difference between killing and banning is that banned users are not able to reconnect after their connection has been killed.

#### Accounts

This panel contains the list of OpenVPN accounts.

Click on Add account to add an account. The following parameters can be specified for each account:

	Account information
Username	– user login name
Password / Verify password	– specify password (twice)
	Client routing
Direct all client traffic through the VPN server	– if you check this, all the traffic from the connecting client (regardless of the destination) is routed through the uplink of the Oneshield Firewall that hosts the OpenVPN server. The default is to route traffic with a destination that is not part of any of the internal Oneshield zones (such as internet hosts) through the client's uplink
Don't push any routes to client	– (advanced users only) normally, when a client connects, tunneled routes to networks that are accessible via VPN are added to the client's routing table – check this box if you do not want this to happen and are prepared to manipulate your clients' routing tables manually
Networks behind client	– only needed if you want to use this account as client in a Gateway-to-Gateway setup: enter the networks behind this client you would like to push to the other clients
Push only these networks	– add your own network routes to be pushed to the client here (overrides all automatically pushed routes)
	Custom push configuration
Static ip addresses	– normally, dynamic IP addresses are assigned to clients, you can override this here and assign a static address
Push these nameservers	– assign nameservers on a per-client basis here
Push domain	– assign search domains on a per-client basis here

In all of these fields, addresses and networks must be given in CIDR notation (e.g. 192.168.0.0/24).

Click the Save button to save the account settings. You can at any moment disable/enable, edit or delete accounts by clicking on the appropriate icon on the right side of the table (see the icon legend at the bottom).

If you are planning to have two or more branch offices connected through a Gateway-to-Gateway VPN it is good advice to choose different subnets for the LANs in the different branches. For example, one branch might have a GREEN zone with the 192.168.1.0/24 subnet while the other branch uses 192.168.2.0/24. This way, correct routes will be assigned in a fully automatic way and you do not have to deal with pushing custom routes.

#### Advanced

Use this panel to change advanced settings. Among other things, certificate-based authentication (as opposed to password-based) can be set up in this section.

The first section has some generic settings regarding the server:

Port / Protocol	– port 1194 / protocol UDP are the default OpenVPN settings. It is a good idea to keep these values as they are – if you need to make OpenVPN accessible via other ports (possibly more than one), you can use port forwarding (see Firewall, Port Forwarding). A use case for setting TCP as the protocol is when you want to access the OpenVPN server through a third-party HTTP proxy.
Block DHCP responses coming from tunnel	– check this if you're getting DHCP responses from the LAN at the other side of the VPN tunnel that conflict with your local DHCP server
Don't block traffic between clients	– the default is to isolate clients from each other, check this if you want to allow traffic between different VPN clients

In the second section you can change the global push options.

Push these networks	– if enabled, the routes to the specified networks are pushed to the connected clients
Push these nameservers	– if enabled, the specified nameservers are pushed to the connected clients
Push domain	– if enabled, the specified search domains are pushed to the connected clients

All addresses and network addresses must be given in CIDR notation (such as 192.168.0.0/24).

The third section lets you specify the authentication method:

Oneshield Firewall's default method is PSK (username/password). If you want to use this method, you do not have to change the settings here.

The Download CA certificate link lets you download the certificate for this OpenVPN server as it is needed by the clients (this is the public certificate, which is used to verify the authenticity of the server). Furthermore, the Export CA as PKCS#12 file link lets you download the certificate in PKCS#12 format (keep it private!), which can be imported into any OpenVPN server that you wish to use as a fall back server.

Finally, should this system be a fall back system, you can upload the PKCS#12 file that you exported from your primary server (leave "Challenge password" empty if the file came from an [Oneshield Firewall](#)).

If you would rather use a X.509–certificate–based method here (either certificate only or certificate plus password), things get a bit more complicated. It is assumed (and required) that you use an independent certificate authority (CA) for this purpose. It is neither possible nor desired to host such a certificate authority on [Oneshield Firewall](#).

You need to generate and sign certificates for the server and for every client using your certificate authority. The certificates type must be explicitly specified and be one of "server" and "client" ("netscape certificate type" field).

The server certificate file in PKCS#12 format must be uploaded in this section (specify the "Challenge password" if you supplied one to the certificate authority before or during the creation of the certificate).

The client certificates need to have the common name fields equal to their OpenVPN user names. Watch out: if you use certificate–only authentication a client that has a valid certificate can connect even if there is no corresponding OpenVPN user account!

You can also upload a revocation list, in case you lost a client certificate and hence have revoked it on your CA.

#### VPN client download

Click on the link to download the Oneshield VPN client for Microsoft Windows, MacOS X and Linux from [Oneshield Network](#).

### OpenVPN client (Gw2Gw)

Select VPN from the menu bar at the top of the screen, then select OpenVPN client (Gw2Gw) from the submenu on the left side of the screen.

In this section you can set up the client side of a Gateway–to–Gateway VPN connection. Click on Add tunnel configuration to enter information about the OpenVPN server you want to connect to (there can be more than one):

- Connection name - just a label for this connection
  - Connect to - the remote OpenVPN server's fully qualified domain name and port (such as `ew.example.com:port`) – the port is optional and defaults to 1194
  - Upload certificate - if the server is configured to use PSK authentication (password/username), you must upload the server's host certificate (the one you get from the Download CA certificate link at the server). Otherwise, if you use certificate–based authentication, you must upload the server's PKCS#12 file (you can get it from the Export CA as PKCS#12 file link on the server (advanced section of the OpenVPN submenu).
  - PKCS#12 challenge password - specify the "Challenge password" if you supplied one to the certificate authority before or during the creation of the certificate
  - Username / Password - if the server is configured to use PSK authentication (password/username) or certificate plus password authentication, give the username and password of the OpenVPN server account here
  - Remark - your comment
- Click on Advanced tunnel configuration to see more options:
- Fallback VPN servers - specify one or more (one per line) fallback OpenVPN servers in the form `ew.example.com:port` (the port is optional and defaults to 1194). If the connection to the main server fails, a fallback server will take over.
  - Connection type - "routed" (the client firewall acts as a gateway to the remote LAN) or "bridged" (as if the client firewall was part of the remote LAN). Default is "routed".
  - Block DHCP responses coming from tunnel - check this if you are getting DHCP responses from the LAN at the other side of the VPN tunnel that conflict with your local DHCP server
  - NAT - check this if you want to hide the clients connected through this [Oneshield Firewall](#) behind the firewall's VPN IP address. Doing so will prevent incoming connection requests to your clients.
  - Protocol - UDP (default) or TCP. Set to TCP if you want to use a HTTP proxy (next option).
  - HTTP proxy - if your [Oneshield Firewall](#) can access the internet only through an upstream HTTP proxy it is still possible to use it as an OpenVPN client in a Gateway–to–Gateway setup. However, you must use the TCP protocol for OpenVPN on both sides. Fill in the HTTP proxy account information in these text fields: proxy host (such as `proxy.example.com:port`, where port defaults to 8080), username and password. You can even use a forged user agent string if you want to camouflage your [Oneshield Firewall](#) as a regular web browser.

Click the Save button to save the tunnel settings. You can at any moment disable/enable, edit or delete tunnels from the list by clicking on the appropriate icon on the right side of the table (see the icon legend at the bottom).

### IPsec

Select VPN from the menu bar at the top of the screen, then select IPsec from the submenu on the left side of the screen.

IPsec (IP Security) is a generic standardized VPN solution. As opposed to OpenVPN encryption and authentication are already done on the OSI layer 3 as an extension to the IP protocol. Therefore IPsec must be implemented in the IP stack which is part of the kernel. Since IPsec is a standardized protocol it is compatible to most vendors that implement IPsec. Compared to OpenVPN IPsec's configuration and administration is usually quite difficult due to its complexity. Because of its design some situations are even impossible to handle, whereas they work well with OpenVPN, especially if you have to cope with NAT. However, Oneshield Firewall implements an easy to use administration interface that supports different authentication methods. We strongly encourage you to use IPsec only if you need to because of interoperability purposes. Use OpenVPN wherever you can, especially if you have to work with NAT.

In the Global settings section you can set the main parameters for your IPsec configuration. The values you can set are:

- Local VPN hostname/IP - Here you can enter the external IP (or a fully qualified domain name) of your IPsec host.
- Enabled - By ticking this checkbox you enable IPsec.
- VPN on ORANGE - If this is enabled it is possible for a user to connect to the VPN from the **ORANGE** zone.
- VPN on BLUE - If this is enabled it is possible for a user to connect to the VPN from the **BLUE** zone.
- Override default MTU - If you want to override the default maximum transmission unit you can specify the new value here. Usually this is not needed.
- Debug options - Ticking checkboxes in this section will increase the amount of data that is logged to `/var/log/messages`.

In the Connection status and control section you can see a list of accounts and their connection status. The list shows Name, Type, Common name, Remark and Status of each connection. By clicking on the icons in the Actions column you can perform various actions as described in the icon legend below the list. You can add a connection by clicking on the Add button. A page will open and you can choose whether you want to add a Host–to–Net Virtual Private Network or a Net–to–Net Virtual Private Network. Submit your choice by clicking on the Add button.

On the next page you can specify the details for this connection (you will also see this page when editing an existing connection). You can configure the network parameters in the first section of the page:

- Name - the name of this connection
- Enabled - if checked, this connection is enabled
- Interface - this is only available for host–to–net connections and specifies to which interface the host is connecting
- Local subnet - the local subnet in CIDR notation, e.g. `192.168.15.0/24`

- Local ID - an ID for the local host of the connection
  - Remote host/IP - the IP or fully qualified domain name of the remote host
  - Remote subnet - this is only available for net-to-net connections and specifies the remote subnet in CIDR notation, e.g. 192.168.16.0/24
  - Remote ID - an ID for the remote host of this connection
  - Dead peer detection action - what action should be performed if a peer disconnects
  - Remark - a remark you can set to remember the purpose of this connection later
  - Edit advanced settings - tick this checkbox if you want to edit more advanced settings
- In the Authentication section you can configure how authentication is handled.
- Use a pre-shared key - Enter a pass phrase to be used to authenticate the other side of the tunnel. Choose this if you wish a simple Net-to-Net VPN. You can also use PSKs while experimenting in setting up a VPN. Do not use PSKs to authenticate Host-to-Net connections.
  - Upload a certificate request - Some roadwarrior IPsec implementations do not have their own CA. If they wish to use IPsec's built in CA, they can generate what a so called certificate request. This partial X.509 certificate must be signed by a CA. During the certificate request upload, the request is signed and the new certificate will become available on the VPN's main web page.
  - Upload a certificate - In this case, the peer IPsec has a CA available for use. Both the peer's CA certificate and host certificate must be included in the uploaded file.
  - Upload PKCS12 file - PKCS12 file password - Choose this option to upload a PKCS12 file. If the file is secured by a password you must also enter the password in the text field below the file selection field.
  - Generate a certificate - You can also create a new X.509 certificate. In this case, complete the required fields. Optional fields are indicated by red dots. If this certificate is for a Net-to-Net connection, the User's Full Name or System Hostname field must contain fully qualified domain name of the peer. The PKCS12 File Password fields ensure that the host certificates generated cannot be intercepted and compromised while being transmitted to the IPsec peer.

If you have chosen to edit the advanced settings of this connection, a new page will open after you hit the Save button. In this page you can set Advanced connection settings. Unexperienced users should not change the settings here:

- IKE encryption - Here you can specify which encryption methods should be supported by IKE (Internet Key Exchange).
  - IKE integrity - Here you can specify which algorithms should be supported to check the integrity of packets.
  - IKE group type - Here you can specify the IKE group type.
  - IKE lifetime - Here you can specify how long IKE packets are valid.
  - ESP encryption - Here you can specify which encryption methods should be supported by ESP (Encapsulating Security Payload).
  - ESP integrity - Here you can specify which algorithms should be supported to check the integrity of packets.
  - ESP group type - Here you can specify the ESP group type.
  - ESP key lifetime - Here you can specify how long an ESP key should be valid.
  - IKE aggressive mode allowed - Check this box if you want to enable IKE aggressive mode. You are encouraged NOT to do so.
  - Perfect Forward Secrecy - If this box is checked perfect forward secrecy is enabled.
  - Negotiate payload compression - Check this box, if you want to use payload compression.
- Finally save the settings by clicking on the Save button.

Back on the main IPsec page you can generate new certificates and upload existing CA certificates in the Certificate authorities section.

To upload a new certificate you have to provide a name in the CA name field. Then click on browse and select the certificate file before clicking the Upload CA certificate button.

To generate new root and host certificates just click on the Generate root/host certificates button. You will see a new page where you can enter the required information.

If you already created certificates and want to create new certificates you must click on the Reset button. Please note that by doing this not only the certificates but also certificate based connections will be erased.

If you want to generate new root and host certificates some information has to be entered. The fields are described below:

- Organization name - The organization name you want to use in the certificate. For example, if your VPN is tying together schools in a school district, you may want to use something like "Some School District."
- Oneshield Firewall hostname - This is used to identify the certificate. Use a fully qualified domain name or the firewall's RED IP address.
- Your email address - Here you can enter your email address.
- Your department - Here you can enter a department name.
- City - Here you can enter the name of your town or your city.
- State or province - Here you can enter the name of the state or province you are living in.
- Country - Choose your country here.
- Subject alt name - Here you can specify an alternative hostname for identification.

The certificates are created after clicking on the Generate root/host certificates button.

If you already created certificate somewhere else earlier you can upload a PKCS12 file in the lower section of the page instead of generating new certificates.

Upload PKCS12 file - Open the file selection dialog and select your PKCS12 file here.

PKCS12 file password - If the file is password protected you must enter the password here.

You can upload the file by clicking on the Upload PKCS12 file button.

#### Creating a Net-To-Net VPN with IPsec using certificate authentication

We have two firewalls A and B, where firewall A is our certification authority.

Firewall A - RED IP: 123.123.123.123, GREEN IP: 192.168.15.1/24

Firewall B - RED IP: 124.124.124.124, GREEN IP: 192.168.16.1/24

The following steps have to be performed on firewall A:

- In the VPN, IPsec menu enable IPsec and specify 123.123.123.123 as Local VPN hostname/IP.
- After saving click on the Generate host/root CA certificate button (unless you already generated these certificates before) and compile the form.
- Download the host certificate and save it as fw\_a\_cert.pem.
- In the Connection status and control section click on the Add button.
- Select Net-to-Net.
- Enter 124.124.124.124 in the Remote host/IP field, 192.168.15.0/24 as Local subnet and 192.168.16.0/24 as Remote subnet.
- In the Authentication section select Generate a certificate and compile the form, make sure to set a password.
- After saving, download the PKCS12 file and save it as fw\_a.p12.

The following steps have to be performed on firewall B:

- In the VPN, IPsec menu enable IPsec and specify 124.124.124.124 as Local VPN hostname/IP.
- After saving click on the Generate host/root CA certificate button (if you already generated them earlier you must Reset the previous certificates).
- Do not compile anything in the first section! Instead upload the fw\_a.p12 file and enter the password you set on firewall A.

- Click on Add in the Connection status and control section.
- Select Net-To-Net.
- Enter 123.123.123.123 in the Remote host/IP field, 192.168.16.0/24 as Local subnet and 192.168.15.0/24 as Remote subnet.
- Select Upload a certificate and upload the fw\_a\_cert.pem you have created on firewall A.

## Chapter 8: The Hotspot Menu

Select Hotspot from the menu bar at the top of the screen.

Oneshield Hotspot is a powerful hotspot that can be used for wireless connections as well as for wired LAN connections. The hotspot's captive portal will capture all connections passing through the BLUE zone, no matter what device they come from. Therefore the hotspot does not work if the BLUE zone is disabled.

The hotspot can be enabled or disabled by clicking on the main switch on this page. If the hotspot is enabled a link to its administration interface is shown. Clicking on the link opens a new browser window with the hotspot administration interface. Although this interface shares its design with the firewall, it contains a whole new menu structure.

- Hotspot – account and ticket management, statistics and settings
- Dialin – current connection state of the uplinks
- Password – change the password of the hotspot user
- Allowed Sites – sites that can be accessed without login

### Hotspot

This section includes subpages to manage accounts, tickets and ticket rates. Statistics can be viewed as well as current and previous connections. Finally it is possible to change the hotspot's settings here.

#### Accounts

On this page it is possible to administer user accounts. By default a list of available accounts is shown. This list can be sorted by Username/MAC, Name, Creation date or by the date until which the user account is valid. It is also possible to reverse the sort order by checking Reverse Order and to Hide disabled accounts as well as to search for accounts. Pagination is also available if the number of results exceeds the number of results per page that has been defined in Hotspot, Settings.

Every user can be edited by clicking on the Edit link in his row (for details see Hotspot, Accounts, Add new account). Tickets can be added to accounts by clicking on the Add ticket link. It is also possible to view the balance and the connection log of an account by clicking on the Balance and Connections links respectively.

#### Add a new account

On this page you can create a new account or an existing account can be modified. The information is split into two parts: Login information and Account information. To create an account you can fill the following fields:

##### Login information

- Username – In this field you have to enter the username.
- Password – In this field you can enter the password for the new account. If you do not have the time to think of an adequate password just leave this field empty and the password will be autogenerated.
- Valid until – The date until the account will be valid. If you want to change it you can either enter the new date manually or click on the ... button and select the new date from the calendar popup.
- Active? – This checkbox specifies if the account is enabled or not. If this is ticked on the account is active. If you want to disable a user tick this checkbox off.
- Language – Here you can select the user's native language if available. Otherwise English should be a good choice.
- Bandwidth limiting – If you do not want to use default values here you can tick the checkbox and specify an upload and download limit for the account in kb/s.
- Static IP address – If you want this account to always use the same IP address you can tick this checkbox and enter the IP address you want.

##### Account information

- Title – The person's title (e.g. Mrs., Dr.)
- Firstname – The user's first name.
- Lastname – The user's last name.
- Country – The country the user comes from.
- City – The city or town the user comes from.
- ZIP – The ZIP of the user's hometown.
- Street – The street in which the user lives.
- City of birth – The city or town in which the user was born.
- Birthdate – The user's birthdate.
- Document ID – The ID of the document that has been used to identify the user.
- Document Type – The type of document that has been used to identify the user.
- Document issued by – The issuer of the document (e.g. City of New York)
- Description – Additional description for the account.

The account information is stored by clicking on the Save button below the form. When editing an existing user it is also possible to print the user information by clicking on the Print button.

On the right side of the screen you will notice the Tickets section. If you want to add a new ticket to the user just select the appropriate ticket-type and hit the Add button. Below you will notice a list of all tickets for this user with the following information:

- Ticket Type – The type of the ticket
- Creation date – The date on which the ticket has been created
- Action – If the ticket has not yet been used you will be able to Delete it here by clicking on the appropriate link.

#### Add MAC-based account

This page is used just like the Hotspot, Accounts, Add new account page. The only difference is that for this type of accounts username and password are not needed. Instead the MAC-Address of a computer's network interface is entered and will be used to identify the account.

#### Import Accounts

It is possible to import accounts from a CSV (comma separated values) file. By clicking on the Browse.. button a file selection dialog is opened. After you have selected the file you can specify whether The first line of the CSV file contains the column titles by ticking or not ticking the checkbox. You should also add a Delimiter in the appropriate field. Usually a delimiter is either a semicolon (;) or a comma (,). If you do not specify a delimiter the system will automatically try to figure out which character has been used as the delimiter. To finally import the CSV file you must click on the Import accounts. button.

#### Export Accounts as CSV

When you click on this link a download dialog will be opened. The download is a CSV file that contains all the account data and can later be re-imported from the Hotspot, Accounts, Import Accounts page.

## Quick Ticket

On this page you can create a new user account with a ticket of your choice already assigned. The username and password are automatically generated. All you have to do is click on the ticket rate you wish to use and the user will be created. The Username, Password and Rate are then displayed on the screen. It is also possible to print this information by clicking on the [Print information](#) button.

## Ticket rates

Oneshield Firewall gives you the possibility to specify more than one ticket rate. You can even specify if you want a rate to be post-paid or pre-paid. It is also possible to create different rates for both types. This is useful if you want to sell different pre-paid types e.g. 4 pre-paid 15 minutes tickets should be more expensive than 1 pre-paid 1 hour ticket.

When opening the page a list with all defined ticket rates is shown. In this list you can see the different ticket rates, the following are the columns:

- Name - The name you gave to the ticket rate.
- Code - This is the ASA code for your ticket rate. Although this can be used only for the ASA hotel management system the field is mandatory.
- Hourly Price - This is the hourly price you have specified.
- Actions - Here you can choose to Edit or Delete a ticket rate by clicking on the respective link.

When editing or adding a ticket rate the Rate Name, Rate Code (ASA), Unit minutes (duration of one unit of this rate in minutes) and the Hourly price of this unit have to be specified. To save the ticket rate click on the [Save](#) button. The price per unit is calculated from unit minutes and the hourly price.

## Statistics

On this page you can see statistics about the hotspot usage and accounting information.

### Filter Period

This is the standard view. It shows a list of accounts and the following data for each account:

- Username - The username or MAC address of the account.
- Amount used - The amount of money that has been used by this account.
- Payed - The money that this user has already paid.
- Duration - The duration that this user has been connected to the hotspot.
- Traffic - The traffic that has been created by this account.

At the bottom of the page a summary over all accounts is shown.

At the top of the page it is possible to enter a start and an end date. By entering these dates into the [From](#) and [Filter](#) button the page will be reloaded with statistics between these two dates only.

Clicking on a username opens a page with details about the unpaid connections of this user. If a user pays, it is enough to enter the amount of money he paid into the [Amount](#) field and click on the [Bill](#) button. It is also possible to print these statistics by clicking on the [>>> Print](#) button.

### Open Accounting Items

This page displays a list of statistics like [Hotspot](#), [Statistics](#), [Filter Periods](#) but with one additional column. The [Amount to pay](#) column shows the amount of money for each account that has not been paid yet.

## Active Connections

On this page you can see all currently active connections on the hotspot. The list contains the following columns:

- Username - The username of the connected account.
- Description - The description of the connected account.
- Authenticated - Shows whether the connection is authenticated or not.
- Duration - The amount of time since this connection has been established.
- IDLE Time - The amount of time that the account has been connected without packets from this account passing through the hotspot.
- IP Address - The IP address that is connected to the hotspot.
- MAC Address - The MAC address of the connected interface.
- Action - Every active connection can be closed by clicking on the [Close](#) link in this column.

## Connection Log

On this page it is possible to see and filter previous connections. Like in the [Hotspot](#), [Active Connections](#) page the list contains various columns. The columns are:

- Username - The username of the connection.
- IP Address - The IP address that was used for the connection.
- MAC Address - The MAC address of the connected interface.
- Connection Start - The start time of the connection.
- Connection Stop - The end time of the connection.
- Download - The amount of data that has been downloaded during this connection.
- Upload - The amount of data that has been uploaded during this connection.
- Duration - The duration of the connection.

The list can be sorted by any of these columns by selecting the respective entry from the [Sort by](#) select box. The sort order can be reversed by ticking the [Reverse Order](#) checkbox. It is also possible to filter connections by entering a [Start Date](#) or an [End Date](#) in the respective fields and then clicking on the [Filter](#) button.

If more results than specified in [Hotspot](#), [Settings](#) are found, pagination is enabled and you can browse through the pages by clicking on the [First](#), [Previous](#), [Next](#) and [Last](#) links above the list.

### Export as CSV

The connection logs can be downloaded by clicking on the [Export as CSV](#) link. The download is in CSV format and contains all relevant information.

## Settings

On this page it is possible to change the hotspot's settings. The page contains two subpages for [System](#) settings and settings regarding the different [Languages](#).

### System

This page consists of two subsections. The first subsection is called [Global Settings](#). This subsection lets you define default values for connections as well as for the administration interface.

- Homepage after successful login - This lets you specify which page to open after a user has logged in successfully.
  - Currency - Here you can specify the symbol of your currency.
- Logout user on Idle-Timeout - In this dropdown you can select after how many minutes a user will be logged out when inactive.
  - Default account lifetime - Here you can enter the number of days an account will be valid by default.
  - Items per page - This value defines how many items will be displayed on each page in the hotspot administration interface.

- Bandwidth limiting - This option lets you specify the default upload and download limits per user in kb/s. If these fields are left empty no limit is applied.

The second subsection is called **Oneshield Hotspot API**. If you want to integrate the hotspot of Oneshield Firewall into an already existing system of yours, you can set the parameters here.

- Mode - Here you can choose whether your system uses Oneshield's *Generic API/JSON* interface or the *ASA jHotel* interface. The *ASA jHotel* interface is only needed by hotels that use the *ASA jHotel* hotel management software whereas the *generic API* can be implemented in other software systems. The other options depend on the selection you made here.
  - API enabled - This option is only visible if you chose *Generic API/JSON* in the selectbox above. The API is enabled if this checkbox is ticked.
  - Accounting URL - This option is only visible if you chose *Generic API/JSON* in the selectbox above. The hotspot will send accounting information to this URL. If you do not want the hotspot to handle accounting you can leave this field empty.
  - Accounting URL requires HTTP Authentication - This option is only visible if you chose *Generic API/JSON* in the selectbox above. If the URL you provided above requires HTTP authentication you must tick this checkbox. Two new textfields will appear where you can enter the *Username* and *Password* respectively.
  - ASA jHotel Interface enabled - This option is only visible if you chose *ASA jHotel* in the selectbox above. By ticking this checkbox you can enable the *ASA jHotel* interface.
  - ASA jHotel URL - This option is only visible if you chose *ASA jHotel* in the selectbox above. Here you can enter the URL of your *ASA jHotel* interface.
  - Allow guest registration (SelfService) - This option is only visible if you chose *ASA jHotel* in the selectbox above. If the hotel guests should be able to register themselves this checkbox has to be ticked.
  - Guest registration default rate - This option is only visible if you chose *ASA jHotel* in the selectbox above. In this selectbox you can select the default rate that will be applied to new accounts.
- Finally the options can be saved by clicking on the **Save** button.

#### Languages

On this page all language-dependent options can be set.

In the first section (*Supported Languages*) of this page it is possible to choose the *Supported Languages* for your hotspot. The languages must be selected in the multi-select box and then saved by clicking on the **Store** button.

In the second section (*Templates*) it is possible to modify the two templates (*Welcome Page*, *Account Print*) for every language. The language can be chosen in the *Edit language* selectbox whereas the template type can be selected from the *Template* selectbox. The *Welcome Page* template is presented to the user before logging in while the *Account Print* template is printed and handed out to the users after their registration.

The content of the templates can be changed with the help of a fully featured WYSIWYG (what you see is what you get) editor. In the *Account Print* template it is also possible to use placeholders which will then be replaced with real data when a user is registered. The templates can be saved by clicking on the **Store** button below the editor.

The third section is called *Strings* and contains translations for strings that are used in the webinterface of the hotspot. The translations can be changed and new translations can be added. This is done by selecting the language from the *Edit language* selectbox and then filling out the textfields. The translations are saved by clicking on the **Store** button.

#### Account Print template placeholders:

```
$title - the title of the account holder
$firstname - the first name of the account holder
$lastname - the last name of the account holder
$username - the username of the account
$password - the password of the account
```

#### Dialin

On this page it is possible to see and manage the status of the uplinks like in the *System*, *Home* section.

#### Password

On this page you can change the password for the hotspot account. Just enter the password in the *Password* field and confirm it in the *Again* field. The password is stored after hitting the **Save** button.

#### Allowed sites

On this page you can define which sites should be accessible without being authenticated. You can also specify whether all IPs should be able to connect to the hotspot or just IPs that belong to the **BLUE** zone.

To allow connections from any IP it is necessary to tick the *Enable AnyIP* checkbox. Sites that can be accessed without authentication have to be entered in the textarea below. One site per line is allowed. A site can be a normal domain name or a string of the format `protocol:IP[mask]:port`, e.g. `www.Oneshield.com` or `tcp:192.168.20.0/24:443`.

The settings are stored after clicking on the **Save** button.

## Chapter 9: The Logs Menu

Select **Logs** from the menu bar at the top of the screen.

**Oneshield Firewall** keeps logs of all firewall activities. The logs can be viewed and exported from this section.

Following is a list of links that appear in the submenu on the left side of the screen:

- **Live** - get quick, live view of the latest log entries as they are being generated
  - **Summary** - get daily summaries of all logs (generated by logwatch)
  - **System** - system logs (`/var/log/messages`) filtered by source and date
  - **Service** - logs from the intrusion detection system (IDS), OpenVPN and antivirus (ClamAV)
  - **Firewall** - logs from the IP firewall rules
  - **Proxy** - logs from the HTTP proxy, the SMTP proxy and the SIP proxy
  - **Settings** - specify log options such as how long log files should be kept
- Each link will be explained individually in the following sections.

#### Live

Select **Logs** from the menu bar at the top of the screen, then select **Live** from the submenu on the left side of the screen.

The live log viewer shows you a list of all log files that are available for real time viewing. You can select the logs you want to see by ticking the checkboxes. After clicking on the **Show selected logs** button a new window with the selected logs will open.

If you want to open a single log file you can click on the **Show this log only** link in the respective row.

This new window contains the main live log viewer. The viewer is configured at the top of the page in the **Settings**. On the right side the list of the logs that are currently displayed is shown. On the left side some additional control elements are shown. These control elements are:

- Filter - Only log entries that contain the expression in this field are shown.
- Additional filter - Like the filter above. Only that this filter is applied after the first filter.
- Pause output - Clicking on this button will prevent new log entries from appearing on the live log. However, after clicking the button once more all new entries will appear at once.
- Highlight - All log entries that contain this expression will be highlighted in the chosen color.
- Highlight color - By clicking on the colored square you can choose the color that will be used for highlighting.

- Autoscroll - This option is only available if in the Logs, Settings section Sort in reverse chronological order is turned off.  
In this case new entries will always be shown at the bottom of the page. If the checkbox is ticked the scrollbar will always be at the bottom of the Live logs section. If this is disabled the Live logs section will show the same entry no matter how many new entries are appended at the bottom.

If you want to show other log files you can click on the [Show more](#) link right below the list of log files that are shown. The controls will be replaced by a table in which you can select the log files you want to see by checking or unchecking the respective checkboxes. If you want to change the color of a log file you can click on the color palette of that log type and then choose a new color. To show the controls again you can click on one of the [Close](#) links below the table and below the list of shown log files.

Finally you can also increase or decrease the window size by clicking on the [Increase height](#) or [Decrease height](#) buttons respectively.

## Summary

Select [Logs](#) from the menu bar at the top of the screen, then select [Summary](#) from the submenu on the left side of the screen.

On this page you can see your [Oneshield Firewall](#)'s log summary. The following control elements are available:

- Month - Here you can select the month of the date that should be displayed.
- Day - Here you can select the day of the date that should be displayed.
- << / >> - By using these controls you can go one day back or forth in the history.
- Update - By clicking this button the page content will be refreshed.
- Export - Clicking this button will open a plain text file with logwatches output.

Depending on the settings in the [Log summaries](#) section of the [Logs, Settings](#) page you will see more or less output on this page.

## System

Select [Logs](#) from the menu bar at the top of the screen, then select [System](#) from the submenu on the left side of the screen.

In this section you can browse through the various system log files. You can search for log entries in the [Settings](#) section by using the following controls:

- Section - Here you can choose the type of logs you want to display.
- Filter - Only lines that contain this expression are shown.
- Jump to Date - Directly show log entries from this date.
- Jump to Page - Directly show log entries from this page in your result set (how many entries per page are shown can be configured on the [Logs, Settings](#) page).
- Update - By clicking on this button will perform the search.
- Export - Clicking on this button will export the log entries to a text file.

It is possible to see older and newer entries of the search results by clicking on the [Older](#) and [Newer](#) buttons right above the search results.

## Service

Select [Logs](#) from the menu bar at the top of the screen, then select [Service](#) from the submenu on the left side of the screen.

The service logs that can be seen here are those of the [IDS](#) (Intrusion Detection System), [OpenVPN](#) and [ClamAV](#). All these log sites share the same functionality:

- Filter - Only lines that contain this expression are shown.
- Jump to Date - Directly show log entries from this date.
- Jump to Page - Directly show log entries from this page in your result set (how many entries per page are shown can be configured on the [Logs, Settings](#) page).
- Update - By clicking on this button will perform the search.
- Export - Clicking on this button will export the log entries to a text file.

It is possible to see older and newer entries of the search results by clicking on the [Older](#) and [Newer](#) buttons right above the search results.

## Firewall

Select [Logs](#) from the menu bar at the top of the screen, then select [Firewall](#) from the submenu on the left side of the screen.

The firewall log search can be controlled like the search for service logs in [Logs, Service](#). Please refer to that section for details.

## Proxy

Select [Logs](#) from the menu bar at the top of the screen, then select [Proxy](#) from the submenu on the left side of the screen.

### HTTP

- Filter - Only lines that contain this expression are shown.
- Source IP - Show only log entries from the selected source IP.
- Ignore filter - Lines that contain this expression are not shown.
- Enable ignore filter - Tick this checkbox if you want to use the ignore filter.
- Jump to Date - Directly show log entries from this date.
- Jump to Page - Directly show log entries from this page in your result set (how many entries per page are shown can be configured on the [Logs, Settings](#) page).
- Restore defaults - Clicking on this button will restore the default search parameters.
- Update - By clicking on this button will perform the search.
- Export - Clicking on this button will export the log entries to a text file.

It is possible to see older and newer entries of the search results by clicking on the [Older](#) and [Newer](#) buttons right above the search results.

### Content filter

The content filter proxy log search can be controlled like the search for http proxy logs in [Logs, Proxy, HTTP](#). Please refer to that section for details.

### HTTP report

On this page you can enable the proxy analysis report generator by ticking the [Enable](#) checkbox and clicking on [Save](#) afterwards. Once the report generator is activated you can click on the [Daily report](#), [Weekly report](#) and [Monthly report](#) links for detailed HTTP reports.

### SMTP

The SMTP proxy log search can be controlled like the search for service logs in [Logs, Service](#). Please refer to that section for details.

### SIP

The SIP proxy log search can be controlled like the search for service logs in [Logs, Service](#). Please refer to that section for details.

## Settings

Select [Logs](#) from the menu bar at the top of the screen, then select [Settings](#) from the submenu on the left side of the screen.

On this page you can configure global settings for the logging of your [Oneshield Firewall](#). The following options can be configured:

- Number of lines to display - This defines how many lines are displayed per log-page.

- Sort in reverse chronological order - If this is enabled the newest results will be displayed first.
  - Keep summaries for \_\_ days - This defines for how many days log summaries should be stored.
    - Detail level - This defines the detail level for the log summary.
    - Enabled (Remote Logging) - Check this box if you want to enable remote logging.
    - Syslog server - This specifies to which remote server the logs will be sent. The server must support the latest IETF syslog protocol standards.
  - Log packets with BAD constellation of TCP flags - If this is enabled the firewall will log packets with a bad constellation TCP flag (e.g. all flags are set).
  - Log NEW connections without SYN flag - If this is enabled new TCP connections without SYN flag will be logged.
  - Log accepted outgoing connections - If you want to log all accepted outgoing connections this checkbox must be ticked.
    - Log refused packets - If you enable this all refused packets will be logged by the firewall.
- To save the settings click on the Save button.

## Appendix: GNU Free Documentation License

GNU Free Documentation License  
Version 1.2, November 2002

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc.  
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA  
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### 0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

### 1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

### 2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

### 3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

### 4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retittle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

#### 5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

#### 6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

#### 7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

#### 8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this license and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

#### 9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

#### 10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.