



# Reference Manual

## Contents

1. Introduction .....	5
The zones.....	6
The Panda Gatedefender Appliance Management Interface.....	7
Accessing the Panda Gatedefender Appliance.....	11
2. The System Menu .....	13
Dashboard.....	14
Network configuration.....	16
Event notifications .....	22
Updates.....	24
Support .....	24
Panda Perimetral Management Console .....	25
Passwords.....	26
Web Console.....	26
SSH access.....	26
GUI Settings.....	27
Backup .....	28
Shutdown .....	30
License Agreement.....	30
3. The Status Menu.....	31
System Status.....	32
Network status.....	33
System graphs .....	33
Traffic graphs.....	34
Proxy graphs.....	34
Connections.....	35
VPN connections.....	36
SMTP mail statistics.....	36
Mail queue.....	36
4. The Network Menu .....	37
Edit hosts.....	38
Routing .....	39
Interfaces.....	41
5. The Services Menu.....	43
DHCP server.....	44
Dynamic DNS .....	46
Antivirus Engine .....	47

Time server .....	49
Mail Quarantine.....	49
Spam Training.....	50
Intrusion Prevention.....	51
High availability.....	53
Traffic Monitoring.....	55
SNMP Server.....	55
Quality of Service .....	55
6. The Firewall Menu.....	59
Common configuration items.....	60
Port forwarding / NAT.....	61
Port forwarding / Destination NAT.....	61
Outgoing traffic .....	63
Inter-Zone traffic .....	65
VPN traffic .....	65
System access.....	66
Firewall Diagrams.....	66
7. The Proxy Menu.....	67
HTTP .....	69
POP3 .....	76
FTP.....	77
SMTP .....	78
DNS.....	87
8. The VPN Menu.....	89
OpenVPN server .....	90
Server configuration.....	90
Authentication.....	94
OpenVPN client (Gw2Gw) .....	97
IPsec.....	100
Certificates .....	104
9. The Hotspot Menu .....	108
Hotspot Settings .....	109
Administration Interface.....	113
Accounts.....	113
Tickets .....	119
Reports.....	122
Settings .....	125

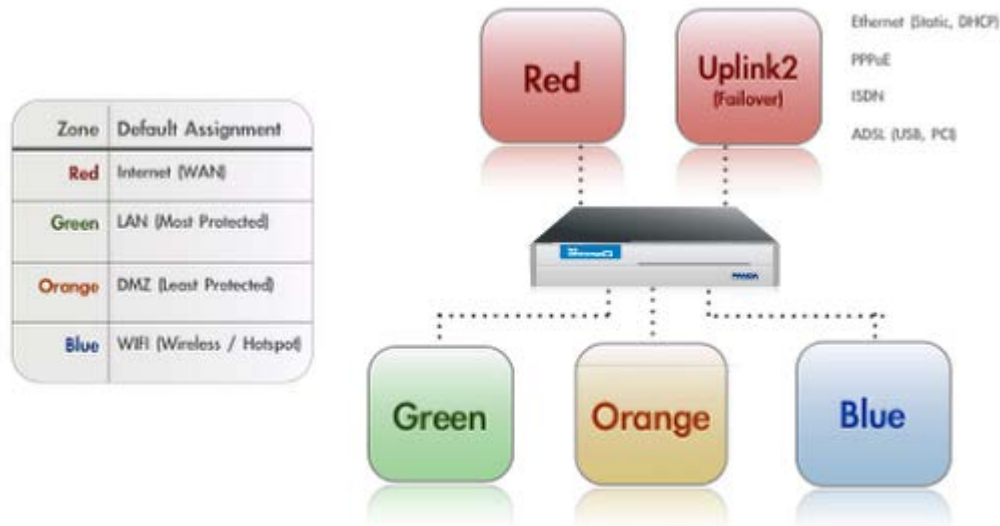
Hotspot User.....	135
Client Access to the Hotspot.....	136
10. The Logs and Reports Menu.....	139
Dashboard.....	140
Traffic Monitoring.....	143
Live.....	145
Common actions.....	146
Summary.....	147
System.....	147
Service.....	148
Firewall.....	148
Proxy.....	148
Settings.....	149
Trusted Timestamping.....	149
11. Glossary.....	151
APPENDIX A. Quicksheet - Where Can I...?.....	153
Hotspot.....	153
Network.....	153
Miscellaneous.....	153
APPENDIX B. GNU Free Documentation License.....	154

# 1. Introduction

---

## The zones

One of the most important concepts on which the Panda Gatedefender Appliance is grounded, the *Zone*, finds its root in IPCOP's idea to protect the networks it can reach by grouping them into different segments -the *zone*, indeed- and allowing the traffic to be exchanged only in certain directions among these segments. The four main zones are identified by a color and may group together a number of servers or workstation that have a same purpose.



- RED, this is the so-called *Untrusted segment*, i.e., the WAN: It encompasses all the networks outside the Panda Gatedefender Appliance or, broadly speaking, the Internet, and is the source of incoming connections. This is the only zone that can **not** be managed: but only access to and from it can be granted or limited.
- GREEN, the internal network, i.e., the LAN. This zone is the most protected one and is dedicated to the workstations and should never be directly accessed from the RED zone. It is also the only zone that by default can access the management interface.
- ORANGE, The DMZ. This zone should host the servers that need to access the Internet to provide services (e.g., SMTP/POP, SVN and HTTP and so on). It is a good practice that the ORANGE zone be the only zone directly accessible from the RED zone. Indeed, if an attacker manages to break into one of the servers, she will be trapped within the DMZ and will not be able reach the GREEN zone, making impossible for her to gain sensitive information from local machines in the GREEN zone.
- BLUE, the WiFi zone, i.e., the zone that should be used by wireless clients to access the Internet. Wireless networks are often not secure, so the idea is to trap by default all the wireless connected clients into their own zone without access to any other zone except RED.

For the Panda Gatedefender Appliance to correctly operate, it is not necessary to configure the ORANGE and BLUE zones. Indeed, it suffices to define the GREEN zone, since also the RED zone can be in some cases left unconfigured.

The Panda Gatedefender Appliance has pre-defined firewall rules that forbid the network traffic to flow between some of the zones. Besides the four main zones, two more zones are available, but are used only in advanced setups: The OpenVPN clients zone (sometimes called PURPLE), and the HA zone. These are two special zones that are used as networks for the OpenVPN remote users that should connect to the Panda Gatedefender Appliance and for the HA service. By default, they use the `192.168.15.0/24` and `192.168.177.0/24` networks respectively, so those networks ranges should not be used in the main zones, especially when planning to use either of these services. Indeed, those networks would overlap, possibly causing undesirable effects. The IP ranges of these two zones can however be modified during the set up of the OpenVPN or HA services.

To each zone corresponds an (*network*) *interface* and an *IP address*. The *interface* is the (ethernet or wireless) port through which the network traffic flows to the zone, so *RED interface* it the port through which you can reach the RED zone and the Internet. The IP

address of the interface is the <Zone>IP. For example, the factory setting for the GREEN zone is the 192.168.0.15/24 network, hence the GREEN interface will have IP 192.168.0.15, which is referenced to as the GREENIP.

See also

High availability

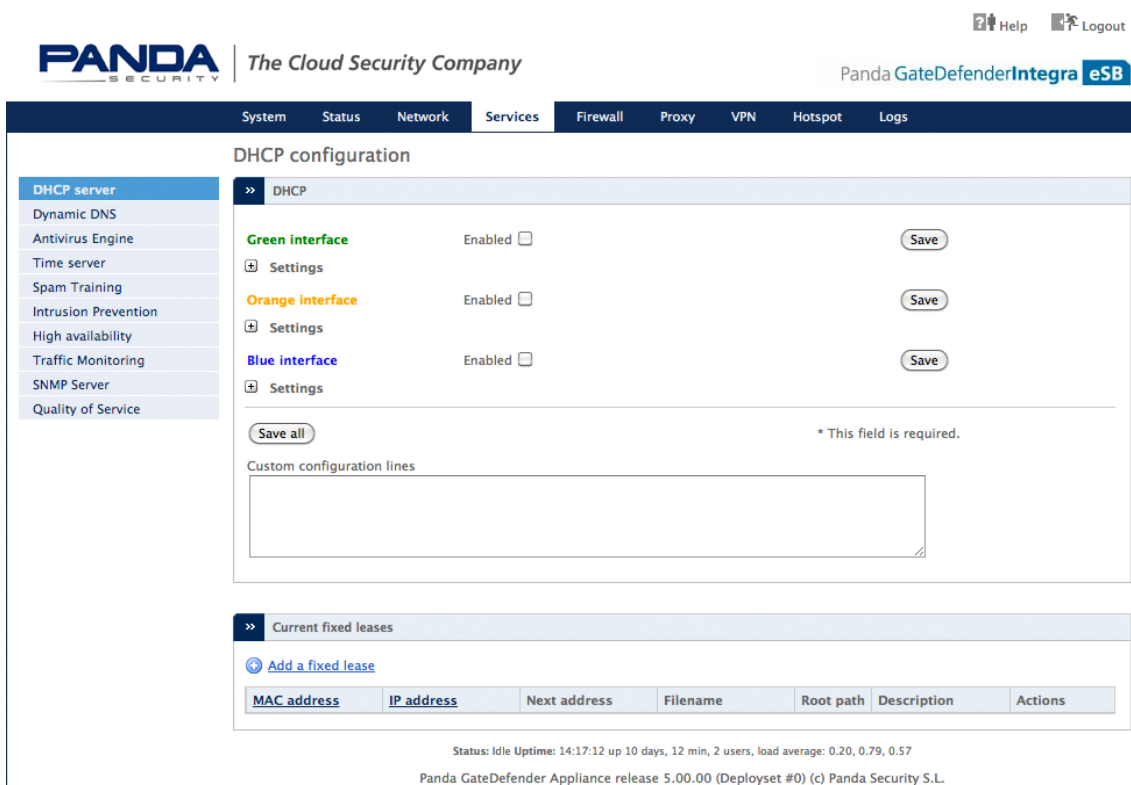
for a description of High Availability

VPN

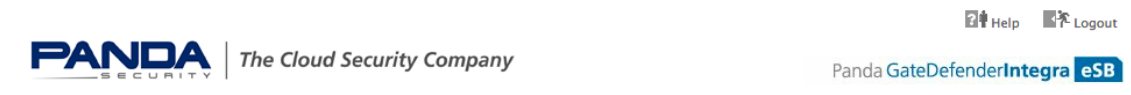
for a description of OpenVPN

## The Panda Gatedefender Appliance Management Interface

The GUI of the Panda Gatedefender Appliance has been designed to be easy to use, and consists of five main parts: The header, the main menubar, the sub-menu, the main area, and the footer. A sample screenshot of the Service module can be seen below.



The header



The header of the page contains the Panda logo and the Panda Gatedefender Appliance version on the left, while on the right-hand side appear two links: one to logout from the GUI and one to the online documentation, which is context-dependent (i.e., from each page the correspondent help will be displayed). This part is static and does not change.

The footer

Status: Connecting... main Uptime: 14:14:12 up 10 days, 9 min, 2 users, load average: 1.68, 1.30, 0.66  
Panda GateDefender Appliance release 5.00.00 (Deployset #0) (c) Panda Security S.L.

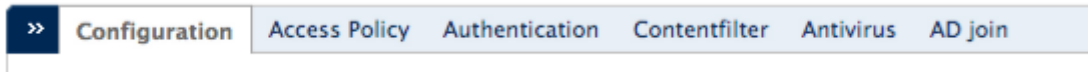
The footer is placed at the very bottom of the page. It consists of two lines of text with a few information on the running Panda Gatedefender Appliance. The top line shows (Status:) whether an uplink is connected or connecting and which one (if there are more





The main area contains all the information and settings encompassed by the current selection of the menu/sub-menu combination. Some of the pages (e.g., the Dashboard or parts of the *Service* and *Logs* modules) are simply informative, showing the current status of the Panda Gatedefender Appliance either graphically or textually, in the latter case conveying the output of linux commands on the screen. The vast majority of the pages, however, shows a table containing various information about the current configured settings, allowing to modify or delete existing items and settings and to add new ones. Particularly elaborate services like e.g., the HTTP proxy or the firewall, contain so many configuration options that a single page does not suffice to present them all, so the available settings are grouped together and organised in tabs.

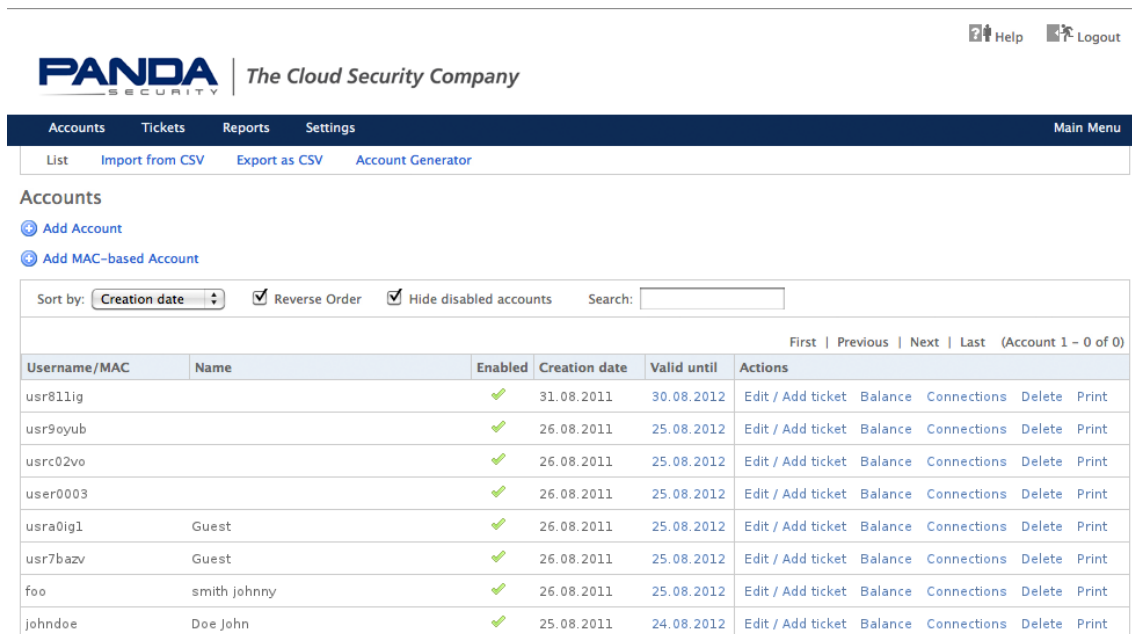
## HTTP proxy: Configuration



Within tabs, often the configuration options are packed in one or more boxes, that gather together settings that refer to a common part of the overall configuration.

### The Hotspot Administration Interface

The only exception to the layout of the Panda Gatedefender Appliance GUI is the Hotspot Administration Interface, pictured in the screenshot below, which has no footer, places the submenu under the main menubar, and presents on the far right of the menubar a *Main menu* link to go back to the main menu.



**Accounts**

[Add Account](#)  
[Add MAC-based Account](#)

Sort by:   Reverse Order  Hide disabled accounts Search:

Username/MAC	Name	Enabled	Creation date	Valid until	Actions
usr81lig		✓	31.08.2011	30.08.2012	Edit / Add ticket Balance Connections Delete Print
usr9oyub		✓	26.08.2011	25.08.2012	Edit / Add ticket Balance Connections Delete Print
usrc02vo		✓	26.08.2011	25.08.2012	Edit / Add ticket Balance Connections Delete Print
user0003		✓	26.08.2011	25.08.2012	Edit / Add ticket Balance Connections Delete Print
usra0ig1	Guest	✓	26.08.2011	25.08.2012	Edit / Add ticket Balance Connections Delete Print
usr7bazv	Guest	✓	26.08.2011	25.08.2012	Edit / Add ticket Balance Connections Delete Print
foo	smith johnny	✓	26.08.2011	25.08.2012	Edit / Add ticket Balance Connections Delete Print
john doe	Doe John	✓	25.08.2011	24.08.2012	Edit / Add ticket Balance Connections Delete Print

Note that when referring to items under the Hotspot Administration Interface, the initial *Menubar* is usually omitted.

### The Icons


Many icons are used throughout the pages served by the Panda Gatedefender Appliance to denote either an action that can be quickly carried out, or convey some meaning to the settings shown.





Switches are used to entirely enable or disable a service and are present on the top of the main area. The gray switch suggests that the service is disabled and inactive, with the main area showing no settings or configuration options. Upon clicking on it, the service and the daemons that are necessary for its proper functioning are started and initialised. After a few seconds, the switch's color turns blue and all the configuration options available will appear. To disable the service, click again on the switch: This causes all the daemons to be stopped, the switch to turn grey, and the settings to disappear.


### Policies


These icons are found in those services that require some form of access policies or traffic control, like, e.g., firewall rules or proxy specifications. Whenever a packet matches a rule, the policy specified for that rule is applied, determining if and how the packet can pass or not.

 Accept the access with no restriction.

 Allow the access but only after the packets have positively passed the IPS. This policy is only available in firewall rules.


 Blocks the packets and discards it.


 Blocks the packets, but a notification is sent to the source.

 Partial accept the rules. This is only found on the heading of a list of policies, to give at a glance the idea that some of the policies in the list are accepted and some are rejected, like e.g., in Menubar › Proxy › HTTP › Contentfilter.

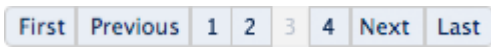
### Other icons

Additional icons that can be found on the Panda Gatedefender Appliance.

 Expands a panel, revealing its content.

 Closes a panel, hiding its content.

### Navigation bar





In most places where a long list of item appears, a navigation bar appears to ease the listing of the items, which is composed of several cells: *First* and *Previous* on the left, *Next* and *Last* on the right, which enclose a variable amount of cells containing the page numbers. Clicking on the various cells leads to either the page indicated by the number, to the first or last page, or to the previous and next page.





### Common Actions and Tasks


There are two types of actions that can be performed within the GUI: Actions on a single item in a list of configuration settings (i.e., one firewall rule), and 'global' actions to save, store, and apply all the settings in a list, a box, or a page.


### Actions and icons


These icons are placed in the *Actions* column on the right of the various tables that appear on the pages and usually show a list of the items defined, like e.g., the firewall rules or the OpenVPN users. The actions' icons allow to execute one task on the element of the list to which they correspond. Some action is only available on some type of lists:


 and  indicate the status of an item, enabled and disabled respectively. You can change the status by clicking on the icon. After that, a callout may notify you to restart service, if this is needed, to let the daemons reload the configuration and activate the changes.



 and  are available only in lists where the order is important, e.g., firewall rules, and allow to modify the order by moving up  or down  the corresponding item.

 allows to modify the current item. Clicking on this icon will open the appropriate editor for that item.

 causes the selected item to be removed from the list and from the configuration. A message will appear, asking for confirmation before the item is definitely deleted.

 allows to download the item (usually an archive).

 is used in limited locations, e.g., in Menubar › Services › Spam Training to test the connection of an item to a remote servers.

 and  appear in the IPS (Menubar › Services › Intrusion Prevention) and allow to log the packets that are allowed to pass or are blocked after they have matched a rule.

### 'Global' Actions

At the bottom of every page that allows the customisation of one or more options, there is the option to *Save* and store the new configuration on disk or to *cancel* the customisation done so far. In the latter case, no further action is required, since the configuration did actually not change. In the former case, however, it proves necessary to restart the service just modified, and perhaps also a few other related or dependant services, for the new settings to be reloaded and used in the running

configuration. For the sake of convenience, when this action is required, a callout is displayed after the settings have been saved, with an *Apply* button, to be clicked to restart the service.

Whenever a Multiselect box is used (e.g., in Menubar > Hotspot Settings), *Add all* and *Remove all* can be clicked as shortcut to add or remove all the available entries from the list of the available items or the selected and active items, respectively.

### Multiple entries in one configuration option

In several places, several values can be entered for a single configuration item, for example the source or destination of a firewall rule. In those cases, either a textarea or a drop-down menu is shown. In the former case it is possible to enter one value per line, like e.g., it a MAC address, a network range (in CIDR notation), or an OpenVPN user. In the latter case, the choice is limited among a number of predefined values, that can be selected by holding the **Control** key on the keyboard and clicking on the values to be selected.

### IPv4 and CIDR notation.

An IPv4 address is a network address whose length is 32 bits, divided in four, 8-bits long octets. In decimal, each octet can assume any value between 0 and 255 ( $2^8 = 256$ ).

When specifying a network range, the IP address of the first host on the network along with the subnet mask, or netmask for short, is given, which defines the number of hosts available in that network. The subnet is defined as the length of the network prefix, i.e., that part of the address shared by all the hosts in a network.

There are two possibilities to denote the network/netmask pair:

explicitly, i.e., both are given in quad dotted notation. For example:

```
network 192.168.0.0
netmask 255.255.255.0
```

This is a network starting at the address 192.168.0.0 with 256 host available, i.e., the network range from 192.168.0.0 to 192.168.0.255. The first three octet in the netmask are 255, showing that there are no free host (or that this part of the address is the network prefix), while the fourth is 0, meaning that all hosts ( $256 - 0 = 0$ ) are available.

in CIDR notation, a more compact way to show the network range, in which the free bits instead of the free hosts are given. The same network range as above is expressed as:

```
192.168.0.0/24
```

This notation shows the length in bits of the shared part of the IP address. 24 means that the first three octets (each consisting of 8 bits) are shared, while the fourth octet is free, giving a number of free hosts that is equivalent to  $32 - 24 = 8$  bits, i.e., 256 hosts.

The same line of reasoning can apply to an IPv6 address, with the only difference that IPv6 addresses are 128 bits long.

## Accessing the Panda Gatedefender Appliance

There are several ways to access the Panda Gatedefender Appliance: The most intuitive and straightforward one is from the web-based GUI. There are also console-based access via SSH and serial console, although they are suggested to advanced users only.

### The Panda Gatedefender Appliance GUI

Hint

The default IP address of the Panda Gatedefender Appliance is 192.168.0.15.

The recommended access to the Panda Gatedefender Appliance GUI is very simple: Start the browser and enter the GREENIP address, whether or not this is the first time the Panda Gatedefender Appliance is used.

The browser will be redirected to a secure HTTPS connection on port 10443. Since Panda Gatedefender Appliance uses a self-signed HTTPS certificate, the browser might ask 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 received from the reseller or, if the Panda Gatedefender Appliance has already been customised, insert the password that provided during the installation.

After entering the password, the Dashboard of the Panda Gatedefender Appliance GUI is displayed, and it is possible to immediately start exploring the information available on this interface or further browse and configure the appliance. The rest of this manual follows the layout of the main navigation bar: Each item in the main menu-bar represents a different section of the Panda Gatedefender Appliance and is presented in a separate chapter, with sub-menu items and tabs having sub- and sub-sub-sections headings markup respectively.

## Console-based access

Console-based access to the Panda Gatedefender Appliance is suggested only to users that are acquainted with the Linux command line.

Two possibilities are available to reach the CLI: Using SSH access or via serial console. SSH access is by default disabled, but can be activated under Menubar > System > SSH access, while Serial Console access is enabled by default on all appliances with the following parameters:

- port: ttyS0
- bit, parity bit, stop bit: 8, N, 1
- speed: 115200 baud

The connection using the serial console requires:

- A suitable terminal program like minicom for Unix/Linux boxes or putty for MS Windows.
- A workstation with a serial interface
- A nullmodem cable to connect a workstation to the appliance

or

- Terminal program.
- Networked Serial-to-Ethernet adapter.
- Serial-to-Ethernet cable to connect the appliance to the adapter.

### Note

In case the network is not configured properly, the serial console may represent the only way to access the Panda Gatedefender Appliance.

# 2. The System Menu

---

The System menu provides several information about the Panda Gatedefender Appliance and its status, and allows to define the network setup and some access modalities (e.g., via SSH or for the Panda support).

The sub-menu on the left-hand side contains the following items, which allow for some basic administration tasks and to monitor the running activities of the Panda Gatedefender Appliance.

- Dashboard - overview of the system and of the connections status
- Network configuration - network and network interface configuration
- Event notifications - set up of notification via e-mail or SMS
- Updates - management of system updates
- Support - support request form
- Panda Networky - Panda Perimetral Management Console registration information
- Passwords - set system passwords
- Web console - a console shell on the browser
- SSH access - enable/configure SSH access to the Panda Gatedefender Appliance
- GUI settings - web interface language settings
- Backup - backup or restore Panda Gatedefender Appliance settings as well as reset to factory defaults
- Shutdown - shutdown or reboot the Panda Gatedefender Appliance
- License Agreement - a copy of the User License Agreement

The remainder of this section will describe the various parts that compose the System menu items.

## Dashboard

The Dashboard is the default page, the one that is displayed upon every login. It encompasses several boxes (“plugins”) organised in two columns that provide a complete overview of the running system and of its health. The top of each box reports the name of the box. The Dashboard has lately undergone some changes in its usability and new features have been added to improve the interaction with the user. The information visible on screen are updated at regular intervals.

The available plugins and the information they display are described here.

### System Information Plugin

It shows several information about the installed system. It usually presents the hostname and domainname of the Panda Gatedefender Appliance in the title.

*Appliance:* The appliance type.

*Version:* The version of the firmware.

*Kernel:* The current running kernel.

*Uptime:* The time since the last reboot.

*Update status:* A message depending on the Panda Gatedefender Appliance status:

- “up to date”. No updates are available.
- “update required”. New packages can be installed: A click on the message leads to the [Updates](#) page where it is possible to review the list of new packages.
- “Register for enterprise”. The system has not yet been registered to Panda Perimetral Management Console: A click on the message will open the [Panda Perimetral Management Console](#) page, in which to compile a form to complete the registration.

*Maintenance:* The remaining days of validity of the maintenance support.

*Support access:* Whether the support team can access the Panda Gatedefender Appliance or not. In the former case, it is also shown the date until the access is granted.

This plugin also shows the remaining days of validity of the additional modules *Panda Antivirus* and *Commtouch*, if purchased.

### Hardware Information Plugin

It shows the main hardware information of the Panda Gatedefender Appliance and the resource availability. All the information are provided with the absolute value (graphically with a small bar and in number at the end of a line) and the percentage of their use. The only exception is the CPU load, which shows only the percentage of use, in graphic and numbers.

*CPU x*: The load of the CPU, where *x* represents the CPU number, for those appliance that have more than one CPU.

*Memory*: The amount of the RAM memory used.

*Swap*: How much swap disk space is used. A high percentage here usually means there is something not working correctly.

*Main disk*: The usage of the root partition.

*Temp*: The space used in the `/tmp` partition.

*Data disk*: the usage of the `/var` partition.

*Configuration disk*: The space occupied by the partition containing all the Panda Gatedefender Appliance services and settings.

*Log disk*: The amount of space used in the partition containing the logs.

The latter values, showing disk space availability, can vary depending on the appliance, since the data, system, and log partitions may be located in different places.

#### Warning

A partition on the hard disk (e.g., main disk, data disk, `/var/log`) shall never have a usage of 95% or more, as this can cause malfunctioning and data loss.

### Service Information Plugin

Information about the most important services installed on the Panda Gatedefender Appliance, along with their actual status, are displayed by this plugin. For each service is shown the status, either ON or OFF, and a summary of the tasks accomplished during the last hour and the last days. A click on the service's name expands or collapses additional information on the tasks carried out by the service. For running services, there is the possibility to open in a new window the respective Live Logs. Hence, if some number in the summaries sounds strange (e.g., a number of email rejected that is twice as normal) or not common compared to the normal activities (e.g., the IDS has detected some attack), the logs can be controlled to search for some useful message that has been recorded. The services currently supported by this plugin are:

*Intrusion Detection*: The number of attacks logged by snort.

*SMTP Proxy*: Statistics about the e-mails processed. The number of e-mail currently in the postfix-queue, of the received e-mails and how many of them were clean, the number of viruses found, and how many e-mails were blocked.

*HTTP Proxy*: The numbers of cache misses and hits of squid and of the viruses found.

*POP3 Proxy*: Statistics about the received, blocked, and virus-containing e-mails that went through the POP3 Proxy.

#### Hint

Inactive services are marked with a red *OFF* message.

### Network Information Plugin

It shows information about the network interfaces of the firewall and the traffic. The upper part of this plugin shows several data about the network interfaces of the Panda Gatedefender Appliance: Their name, type, link (*Up* if a connection is established, *Down* otherwise) and status (*Up* if the device is activated, *Down* if not), and the In- and Outgoing traffic. The latter two data are updated in real-time. When ticking the checkbox near the device name, that device is shown in the graphs underneath. The devices' name is coloured according to the zone they serve.

The lower part of the plugin contains two charts: The first one shows the incoming traffic, while the second one the outgoing traffic on each of the interfaces chosen. The traffic of each interface is coloured according to the zone it belongs to, different interfaces serving the

same zone have different nuances. Bridges built on one device are shown in the same colour as the device. Like the traffic data in the upper part, both charts are updated in real-time.


Hint

Up to six interfaces can be selected and shown in the charts.

### Signatures Information plugin

This plugin shows information about the actual status of those services requiring the download of signatures that are installed and enabled on the Panda Gatedefender Appliance. In case no signature has been downloaded and no service has already been enabled, the message *No recent signature updates found* is displayed, otherwise the plugin presents the signatures installed for the various daemons and the timestamp (date and time) of the last download. The list includes the signatures for the anti-spyware, antivirus, contentfilter, and intrusion prevention services.

### Uplink Information Plugin

This plugin shows a table detailing the uplinks' connection status. For each defined uplink are shown name, IP address, status, uptime, whether it is active  or not , managed  or manual . The circular arrow , when clicked, allows to immediately reconnect the corresponding uplink. Of particular interest is the *Status* field of each individual uplink, which can be:

*Stopped:* Not connected.

*Inactive:* Not connected.

*Connecting:* Not yet connected, but a connection is ongoing.

*Connected or UP:* The connection has been established and it is fully operational.

*Disconnecting:* The uplink is closing the connection. The Panda Gatedefender Appliance keeps pinging the gateway and announces when it becomes available.

*Failure:* There was a failure while connecting to the uplink.

*Failure, reconnecting:* There was a failure while connecting to the uplink, but the Panda Gatedefender Appliance is now trying again.

*Dead link:* The uplink is connected, but the hosts that were defined in the uplink configuration (Menubar › Network › Interfaces, option *Check if these hosts are reachable* in the Uplink editor) to check the connection could not be reached. In other words, the uplink is not operational.

### Managed and manual uplink.

Each uplink can be operated in either managed mode, which is the default, or manual mode. In managed mode, the Panda Gatedefender Appliance monitors and restarts the uplink automatically when needed. If managed mode is disabled, the uplink has to be activated or deactivated manually: This implies that there will be no automatic reconnection attempt if the connection is lost, but clicking on *Reconnect* is required to restart a nonoperational uplink. The management mode of an uplink can be selected under Menubar › Network › Interfaces.

While an uplink should always be managed to allow for a quick reconnection in case of a connection loss, the manual mode proves useful for troubleshooting or testing connections before actually establishing them.

## Network configuration

The configuration of the networks and of the network interfaces serving the zones is fast and easy with this 8-step wizard. It is possible to freely navigate back and forth the step, using the <<< and >>> buttons and even decide at any moment to cancel the actions done so far. Only at the last step it is required to confirm the new settings: In that case, all the changes made will be applied. Note that while applying the new settings, the web interface might not respond for a short period.

The Stealth Uplink mode.

The Stealth Uplink mode represents a new possibility to seamlessly integrate the Panda Gatedefender Appliance into an existent network infrastructure without the need to modify the existent routing or firewalling rules.



The Stealth Uplink mode requires a Panda Gatedefender Appliance equipped with at least two NIC serving the same zone, which can be GREEN, ORANGE, or BLUE. One of these interfaces routes all the traffic directed from the zone to a gateway and in practice represents the Panda Gatedefender Appliance's 'uplink'.

The presence of an explicit interface designated as 'uplink' allows to distinguish a direction for the traffic flowing outside the zone served by the Stealth Uplink and to filter it using the outgoing firewall. This is the main difference with the *no uplink* mode (previously known as *Gateway mode*) in which there is no possibility to filter outgoing traffic and therefore the application control was not applicable.

The Stealth Uplink operating mode requires a particular set up in the Panda Gatedefender Appliance's firewall setup.

- System access rules are handled normally.
- Port forwarding and Destination NAT rules can also be configured normally. However, being the outgoing interface in the same zone as the internal network, the rules will be applied from both sides of the zone.
- Source NAT is not applied for outgoing connections in this setup as otherwise the behaviour would not be transparent anymore.
- The outgoing firewall is used for all the traffic that flows from the zone served by the Stealth Uplink through the NIC designated as uplink, allowing to exploit the abilities of the application control.
- The interzone firewall is employed for all the remaining traffic between the other zones, if defined. If the Stealth Uplink bridge is composed by three or more interfaces, and hence two or more serve the corresponding zone, also the traffic among these and the other zones can be filtered by the interzone firewall.

Due to the availability of this uplink mode, also the GUI of the network configuration wizard has changed, especially in the first page of the wizard, to clarify the differences among the various uplinks and the configuration options available for each of them.

The 8 steps in which the wizard is divided are:

## 1/8 - Choose network mode and uplink type

The first page of the network configuration wizard contains two boxes: *Network modes*, in which to choose the operating mode of the uplink, and *Uplink type*, in which to select the uplink.

### Network modes

The first box allows to choose the operating mode of the uplink used by the Panda Gatedefender Appliance, among three possible, mutually exclusive choices. When selected or when the mouse hovers over one of the options, a brief description appears.

- Routed. This choice corresponds to the classical uplinks available in Panda Gatedefender Appliance, except for the *Gateway mode*.
- Bridged. The new Stealth Uplink mode.
- No uplink. This choice corresponds to the mode previously known as *Gateway mode*.

#### Note

When in *No uplink* mode, rules defined in the outgoing firewall, which filters the traffic going from the Panda Gatedefender Appliance through the uplink, are not taken into account.

The next box appears only upon selection of the *Routed* option, since in the other cases the mode automatically determines the RED interface.

### Uplink type (RED zone)

At installation time, the Panda Gatedefender Appliance receives a default GREEN IP. This screen allows to choose the type of the RED interface (i.e., the type of uplink) among those supported by the Panda Gatedefender Appliance.

#### ETHERNET STATIC

The RED interface is in a LAN and has fixed IP address and netmask, for example when connecting the RED interface to a simple router but with the convenience that the Panda Gatedefender Appliance be always reachable at the same IP address.

#### *ETHERNET DHCP*

The RED interface receives its network configuration via (dynamic) DHCP from a local server, router, or modem, i.e., the RED interface is connected to a simple router but without the need to have a fixed address.

#### *PPPoE*

The RED interface is connected to an ADSL modem. This option is only needed when the modem uses bridging mode and requires to use PPPoE to connect to the provider. This option should not be confused with the *ETHERNET STATIC* or *ETHERNET DHCP* options, used to connect to ADSL routers that handle the PPPoE themselves.

#### *ADSL (USB, PCI)*

The RED interface connects to an ADSL modem via a USB or PCI cable, not via an Ethernet one.

#### *ISDN*

The RED interface is an ISDN connection.

#### *ANALOG/UMTS Modem*

The RED interface is an analog (dial-up) or UMTS (cell-phone) modem.

A small box recalling the number of network interfaces available on the system is shown to the right of the available choices. The RED interface can be fully configured during step 4.

## 2/8 - Choose network zones

The Panda Gatedefender Appliance separates the networks connected to it into four main zones, as described in this section. At this point the two most important zones - *GREEN* and *RED* - have already been encountered during the installation: This step allows to enable one or two additional zones, depending on the services that should be provided by the Panda Gatedefender Appliance: *ORANGE* -used as the DMZ network portion- and *BLUE* -used as segment for wireless clients. Their full configuration will be possible in the next step.

#### Note

In the Panda Gatedefender Appliance, one network interface is reserved for the GREEN zone and another one has possibly been assigned to the RED zone, if the RED interface requires a network card. This might limit the choices here to the point that the ORANGE or BLUE zone cannot be enabled, due to lack of additional network interfaces.

## 3/8 - Network Preferences

This step concerns the configuration of the GREEN zone, if needed, and of any zone chosen in the previous step. For each of the zones enabled, the following options can be configured:

#### *IP address*

The IP address (such as 192.168.0.1) of the interface, which should not be already in use in the network.

#### Hint

Good practice suggest that the last octet be 1, since the interface will gather the traffic of the whole subnet.

Remember also that a change in the IP addresses of an Panda Gatedefender Appliance, especially in a production environment, might require to adjust additional settings elsewhere, for example the HTTP proxy configuration in the workstations, otherwise the web browsers will not work correctly.

#### Warning

When configuring the interfaces of the GREEN zone, make sure to not remain locked out of the web interface! This situation may occur for example when changing the GREEN IP address into one that is not reachable from the current GREEN segment and then saving the settings. In this case the only access to the Panda Gatedefender Appliance is via serial console.

#### *Network mask*

Define the network mask from a drop-down menu containing the possible masks (e.g., /24 - 255.255.255.0).

#### Hint

All the devices connected To the same subnet shall have the same netmask to communicate properly.

#### *Additional addresses*




Additional IP addresses for different subnets can be added to the interface here.

### Interfaces

Map a network interface to a zone, with the following rules:

1. Each interface can be mapped to only one zone and each zone must have at least one interface.
2. When more than one interface is assigned to a zone, these interfaces will be bridged together and act as if they were part of a switch.

For each available interface these information are shown:

- A colored checkbox, showing which zone the interface serves. No color means that the interface is not assigned to any zone.
- *Port*, the number of the port.
- *Link*, shows the current status by means of icons:  -the link is active,  -no link or no cable plugged in,  -no information from the driver.
- *Description*, the interface's PCI identification string, as returned by `lspci`. The string is trimmed, but it can be shown by moving the mouse on the?.
- *MAC*, the interface's MAC address.
- *Device*, the logical name of the device.

#### Note

Internally, the Panda Gatedefender Appliance handles all zones as bridges, regardless of the number of the assigned interfaces. Therefore, the Linux name of the interfaces is `brx`, not `ethx`.

Finally, the system's host name and domain name can be set in the two text boxes at the bottom of the screen.

### Private IP Addresses

It is suggested to follow the standard described in [RFC 1918](#) (which has been recently been updated by [RFC 6761](#)) and to use for the zone's setup only the IP addresses contained in the network segments reserved for private use by the IANA, which are:

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

This choice avoids incurring in DNS resolution errors, as IP addresses not falling within these ranges are likely to have been reserved by other organisations as their public IPs. Moreover, different IP ranges must be used in the 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

Note also the first and the last IP address of a network segment (which are usually .0 and .255) are reserved as the network address and the broadcast address respectively, and must not be assigned to any device.

## 4/8 - Internet access preferences

This step allows the configuration of the RED interface chosen in step 1, that connects to the Internet or to any other untrusted network outside Panda Gatedefender Appliance.

#### Note

If *Routed* mode was chosen in step 1/8, only the choice of the default gateway is available here.

Depending on the type of the selected RED interface, different configuration options will be available, as required by each interface type. At the bottom of the page appear two options that are commonly available, namely *MTU* and *Spoof MAC address with*, described below, and the choice of the DNS resolver, available for almost all interface types, which is wither *Dynamic* or *Manual*. In the latter case, one valid IP address of a DNS server must be provided manually in the next step. The other configuration options are:

### ETHERNET STATIC

The IP address and network mask of the RED interface, as well as the IP address of the default gateway, that is, the IP address of the gateway that connects the Panda Gatedefender Appliance to the Internet or to another untrusted network. Optionally, the Ethernet hardware address (MAC address) of the interface can be specified.

### ETHERNET DHCP

Only one available option, namely the DNS choice.

### PPPoE

To configure PPPoE, fill in the form with the username and password assigned by the provider, and the authentication method. Optionally, the provider's service and concentrator name can be configured, though this is usually not needed.

#### Hint

If unsure whether to select PAP or CHAP authentication, keep the default option.

### ADSL (USB, PCI)

There are 3 sub-screens for this choice.

1. In the first one, select from the drop-down menu the appropriate driver for the modem, among the possibilities offered.
2. In the second one, choose the *ADSL type* from the drop-down menu among the four choices: PPPoA, PPPoE, static IP, or DHCP.
3. Finally, depending on the selection made in the previous two steps, some of the following settings are required, which can be asked to the ADSL provider:
  - VPI/VCI numbers* and the encapsulation type
  - the *username* and *password* assigned by the provider and the *authentication method* (if unsure, keep the default PAP or CHAP)
  - the IP address and network mask of the *RED interface*,
  - the IP address of the *default gateway* (required for static IP only);

#### Note

If PPPoE was chosen at point 2. above, then the configuration is exactly like explained in the previous paragraph, PPPoE.

### ISDN

To configure the ISDN connection, the modem driver, phone numbers (the provider's number and the number used to dial out), as well as the username and password that have been assigned by the provider, and the authentication method are needed (if unsure, keep the default PAP or CHAP). Also specify whether the IP address of the DNS should be assigned automatically or set manually.

### ANALOG/UMTS Modem

While Panda Gatedefender Appliance supports most modern UMTS modems, some care is required when using them in conjunction with Panda Gatedefender Appliance. On one side, some UMTS modems are USB mass storage devices as well and usually register two devices (e.g., `/dev/ttyUSB0`, `/dev/ttyUSB1`): In this case the first device `/dev/ttyUSB0` is the modem, the second one is the storage. These types of modem can cause problems when restarting the firewall because the Panda Gatedefender Appliance tries to boot from the USB mass storage device. On the other side, some SIM cards require a personal identification number (PIN) to work, but this is not supported. To allow those cards to work with Panda Gatedefender Appliance, the PIN should be removed from the card.

There are 2 sub-screens for this choice.

1. In the first one, specify to which serial port the modem is connected to and whether it is an analog modem or an UMTS/HSDPA modem.

#### Hint

The `/dev/ttyS0` device is reserved for the serial console and is therefore not available as port for modems.

2. In the second one, configure the modem's bit-rate, the dial-up phone number or access point name, the username and password that have been assigned by the provider and the authentication method (if unsure, keep the default PAP or CHAP). For UMTS modems it is also necessary to specify the access point name.

## GATEWAY

The IP address of the default gateway - that is, the IP address of the gateway that connects the Panda Gatedefender Appliance to the Internet or another untrusted network.

The common options are:

## MTU

The MTU size of the packets send over the network.

## Spoof MAC address with

Specify a custom MAC address for the RED interface. This setting is required for the proper failover of slave devices in an HA setup. See High availability for more information about the RED address in HA setups.

## The MTU size.

While the vast majority of the ISPs uses a standard value of 1500 bytes, in some circumstances the standard MTU size results too high. If that happens, some strange network behaviours will noticed, like e.g., downloads which always stop after a while or connections which will not work at all.

If the ISP does not use a standard MTU size, it is easy to discover the correct one, by sending special ICMP packets with a specific value, that can be lowered until no errors are encountered: At theist point, the MTU size is correct and this value should be entered in the configuration options.

In order to send the icmp packets do the following:

Log in to the EFW and choose a host which can be actually reached (e.g., the ISP's DNS, which should always be reachable) and ping that host with the following command:

**ping -c1 -M do -s 1460 <host>** (please refer to the ping(8) manpage for more info).

If the MTU size 1460 is correct, ping replies like the following one are received:

```
PING 10.10.10.10 (10.10.10.10) 1460(1488) bytes of data.  
1468 bytes from 10.10.10.10: icmp_seq=1 ttl=49 time=75.2 ms
```

If however the current MTU size is still too big for packets of the size 1460, an error message like this will appear:

```
PING 10.10.10.10 (62.116.64.82) 1461(1489) bytes of data.  
ping: sendmsg: Message too long
```

Retry with different packet sizes (i.e., the value after the -s option), until the correct size has found and no error is displayed. The value shown within brackets in the **ping** command's output is the MTU size. In this example the output is 1460(1488), therefore 1488 is the value to select for the MTU size.

An MTU value lower than 1500 may cause problems also in the OpenVPN setup and require to adjust some setting there.

## 5/8 - Configure DNS resolver

This step allows to define up to two IP addresses for the DNS server, unless they are assigned automatically: In this case, no configuration option can be set and it is safe to move to the next one. If only one DNS server should be used, the same IP address must be entered twice. The IP address(es) of the DNS must be accessible from the Panda Gatedefender Appliance, otherwise URL and domain resolution will not work.

See also

Changes to the RED interface, i.e., the uplink, and the DNS server can be modified later, separately from the other network configuration:

Uplink editor

Menubar › Network › Interfaces › [edit uplink]

## 6/8 - Configure default admin mail

The configuration of a global administrator e-mail address that will be used by all services to send e-mails, is done here. The administrator e-mail address is then used for notifications, in case of problems or emergencies. These email addresses will be used by the [Event notifications](#).

There are three fields to configure.

#### *Admin email address*

A valid e-mail address to which the system e-mails should be sent.

#### *Sender email address*

A valid e-mail address that appears as the sender address. A custom sender address proves useful if the recipient wants to filter messages sent by the Panda Gatedefender Appliance.

#### *Address of smarthost*

The SMTP server through which the email should be sent.

#### Hint

Although all the fields may be left blank, it is suggested to supply at least one valid *Admin e-mail address*.

## 7/8 - Apply configuration

This step informs that the network setup is now finished and all the new settings have been gathered. Clicking on the *OK, apply configuration* button will save the settings and apply the configuration by restarting all the necessary services and daemons.

## 8/8 - End

In the last step, all the configuration files are written to the disk, all the devices are reconfigured and the network-depending services and daemons (e.g., the firewall and ntpd) are restarted as necessary. The whole process may take up to 20 seconds, during which the connection to the administration interface and through the Panda Gatedefender Appliance may not be possible.

The administration interface will then reload automatically. If the GREENIP address has changed, the GUI will be reloaded at the new IP address. In this case or in case the hostname changed, a new SSL certificate is generated to identify the new host.

#### Note

To change later only some of the settings in the network configuration (e.g., the hostname or the network range of a zone), simply start the network configuration, skip all the steps until the one in which to make the desired changes, edit the appropriate values, then proceed to the last step and finally save.

## Event notifications

Whenever some critical event takes place on the Panda Gatedefender Appliance (e.g., a partition is filling up, or there are updates available), there is the option to be immediately informed by e-mail about it and to promptly take some actions to solve a problem, if required.

Systems that feature the hotspot use also SMSs for the activation of new accounts or for the purchase of new tickets. Three tabs are available in the page: *Settings*, *SMS Notifications*, and *Events*.

## Settings

The default tab serves for the configuration of the email notification:

#### *Email notifications*

Select from a drop-down menu how to use the notification system. Available options are:

- *notify using default email address*: the default administrator e-mail address (as specified in the Installation wizard or in step 6 of Menubar › System › Network configuration)
- *notify using custom email address*: an alternate e-mail address to which the notification e-mail shall be sent. In this case, three more options must be configured, namely:

**Mail sender address**

The e-mail address that appear as the sender of the e-mail.

**Mail recipient address**

The e-mail address to which the e-mail will be delivered.

**Mail smarthost**

The SMTP server that will be used to send the notification e-mail.

- *do not notify*: no notifications will be sent

## SMS

SMS notifications are used by the hotspot, to activate accounts or tickets.

This box is divided into two parts: at the top there it is possible to add SMS bundles, while at the bottom some information about the SMS contingent is displayed.

**Enter Activation Code ...**

To add a new SMS bundle, it must be first purchased on the Panda Perimetral Management Console, after which an activation code will be generated. This activation code must be supplied in this textbox.

**Activate**

After supplying a valid activation code, clicking on this button will add an SMS contingent that will be used for sending the notifications.

**Available SMS**

The number of SMS that are at disposal.

**Reserved SMS**

The number of SMS that have already been used, but not yet delivered to the recipient. This event may occur for example if the recipient was not reachable.

## Events

This tab shows a list of all the events that can produce a notification message and allows to configure the actions to be done when each of the events takes place. Right above the list there is a small navigation bar and a search field: The latter can be used to filter only the relevant items.

The list contains three columns:

**ID**


The 8-digit ID *ABBCCCCD* code of the event, which is built as follows:


- A represents the layer number, i.e., in which system's component the event has taken place: 1 means kernel, 2 the system itself, 3 services, 4 configlayer, and 5 the GUI.
- BB is the module number
- CCCC is a sequential number assigned to the event
- D is the severity of the event, i.e., the degree of badness of the event. The lower the number, the worst the severity: 0 is a critical event, 4-5 neutral, 9 is a positive event.

**Description**

A short description of the event.

**Actions**

The actions that can be performed for each event. All e-mail notifications are enabled by default (this is shown by the  icon), but to disable notifications for one event, click on the mail icon in that event's row (this causes also the icon to change

into ). To later re-activate the notification, it suffices to click again on the icon. After changing an action, remember to click on the *Apply* button that appears within the green callout above the events' list.

## Updates

The management of the software updates is done from here. It is possible at any time to manually check for available updated packages, or to schedule a periodic check.

In this page there are two boxes: One with the current status of the system and one to schedule a routine check for updates.

### Status

The *Status* box informs whether the system needs updates or not. In the former case, a list of available packages is presented, while in the latter the message “Your Panda Gatedefender Appliance is **up to date!**” is displayed. Moreover, additional messages inform of the last date and time when a check for updates and the last upgrade have been carried out. These options are available:

#### *Check for new updates*

A manual check for updated packages is started, and any upgradable package found is listed here. Individual packages can be chosen from the list and installed.

#### *Start update process NOW*

The update process is launched: The system downloads the updated packages which are then installed, replacing the old ones.

#### Note

In order to check for updates, a valid maintenance is required, otherwise no update will show up, even if available.

### Schedule for retrieving the update list

The *Schedule* box allow to set up a periodic job, governed by the **cron** daemon, that retrieves the list of updated packages. The available, mutually exclusive, options are *Hourly*, *Daily*, *Weekly*, and *Monthly*. Moving the mouse over the small ? next to each option shows a tool-tip with the exact time at which the job will run.

## Support

In this page it is possible to manage requests for assistance to the Panda support.

#### Note

To be able to submit a support request, the system must be registered to the Panda Perimetral Management Console. If not, the “Currently no running maintenance available.” message will be displayed.

The page is divided in two boxes with different purposes: The first one contains a link to open the support's home page, while in the second one it is possible to grant SSH access to the support team.

### Visit Support Web Site

This box contains only a hyperlink to the home page of the support.

#### *Please visit our Support Web Site*

By clicking on this link, a new tab in the browser will open, where it is possible to find directions on how to fill in an assistance request to the support team.

### Access for the Panda Support Team

Optionally, access to the firewall can be grant via SSH, a secure, encrypted connection that allows a member of the support staff to log in to the Panda Gatedefender Appliance, verify its configuration and inspect it to find out where the problem lies. The box contains an informative message, the status of the access, which is either *DENIED* or *ALLOWED*. When the status is *DENIED* a button appears at the bottom of the box:

#### *Allow access*



Clicked on this button to grant 4 days of access to the Panda Gatedefender Appliance to the support team.

When the support team access is allowed, a new message appears under the status message: *Access allowed until:* followed by the date and time when access to the Panda Gatedefender Appliance will be revoked. Moreover, there are two buttons at the bottom of the box.

#### *Deny access*

Immediately revoke the grant to access the Panda Gatedefender Appliance.

#### *Extend access for 4 more days*

If the support team needs more time to inspect the Panda Gatedefender Appliance, a click on this button extends the access grant by four more days.

#### Note

When enabled, the support team's public SSH key is copied to the system and access is granted via that key. The support team will not authenticate with username/password to the Panda Gatedefender Appliance. The root password of the Panda Gatedefender Appliance is never disclosed in any way to the support team.

## Panda Perimetral Management Console

The Panda Network, short for Panda Perimetral Management Console, is the Panda solution for an easy and centralised monitoring, managing, and upgrading of all the registered Panda Gatedefender Appliance systems, with just a few clicks.

This page is organised into two tabs, namely *Subscription* and *Remote Access*.

### Subscription

If the firewall has not yet been registered to the Panda Perimetral Management Console, the registration form is shown, that can be filled in before submitting the request for registration. After the registration has been completed, the Subscriptions tab shows three boxes:

#### **System information**

Basic data about the Panda Gatedefender Appliance: Serial number, activation code, model of the appliance, and the maintenance package chosen.


#### **Registration Status**

A summary of the Panda Perimetral Management Console support status: System name, organisation for which the Panda Gatedefender Appliance is registered, system ID, and the date of the last update.

#### **Your Activation Keys**

To receive updates from and to participate in the Panda Perimetral Management Console, at least one valid (i.e., not expired) activation key is required. There is a key for each support channel, but typically just one, shown with the validity time and the days of maintenance left. An expired key is shown by its channel name stricken-through and by the *expired* string in the corresponding *Days left* column.

### Remote Access

The Remote Access tab allows to choose whether the Panda Gatedefender Appliance can be reached through the Panda Perimetral Management Console and by which protocol. To allow access, click on the grey switch on  the top of the page: Its color will turn blue, and two access options can be chosen, by ticking the checkbox:

#### *Enable HTTPS access ...*

The Panda Gatedefender Appliance can be reached via the web interface.

#### *Enable SSH Access ...*

Login via a secure shell to the Panda Gatedefender Appliance is allowed. Activating this option automatically activates the [SSH access](#).

## Passwords

In this page passwords can be changed for each of three default users, by writing each new password twice and then by pressing the corresponding *Change Password* button:

### *Admin*

the user that can connect to the web interface for administration.

### *Dial*

A special user that can only manage uplinks, with a limited interface access.

### *Root*

the user that can login to the shell for administration. Logins can be made either via the serial console, or remotely with an SSH client.

### Hint

Passwords need to be at least 6 characters long.

## Web Console

The web console provides an applet which emulates a terminal within the browser window, that serves as a CLI to carry out administrative tasks.

The functionalities of the web console are the same found upon logging in via serial console or SSH. On the bottom left of the applet, a message shows the status of the console: *Connected* or *Disconnected*. It is possible to exit at any time by typing **exit** in the console and then pressing **Enter** on the keyboard, like in any normal console.

When disconnected, click again on the *Web console* sub-menu item to reconnect. On the bottom right of the applet, two hyperlinks show up:

### *Enable virtual keyboard.*

When clicking on this link, a keyboard applet appears below the console, that can be used to type and execute commands by clicking the mouse on the various *keys*.

### Note

When the web console is disconnected, this applet does not communicate with the console.

### *Disable input*

This link toggles the possibility to send input from the keyboard to the web console.

### Hint

This option has no effect on the virtual keyboard.

## SSH access

This screens allows to enable remote SSH access to the Panda Gatedefender Appliance. This is disabled by default and it is the recommended setting. There are two boxes in the page: *Secure Shell Access Settings* and *SSH host keys*.

### Secure Shell Access Settings

The SSH access is activated by clicking on the grey switch . The SSH service is started, and after a few seconds, some configuration options are displayed:

Example SYS-1 - Traffic Tunnelling over SSH.

Assume that a service such as telnet (or any other service that can be tunneled through SSH) is running on a computer inside the GREEN zone, say port 23 on host *myhost* with IP address 10.0.0.20. To setup a SSH tunnel through the Panda Gatedefender Appliance to access the service securely from outside the LAN, i.e., from the RED zone. While GREEN access from the RED interface is in general not recommended, it might prove useful in some cases, for example during the testing phase of a service.

1. Enable SSH and make sure the host can be accessed, i.e., configure the firewall in Menubar › Firewall › System access for *myhost* to be reachable from the outside.
2. From an external system connect to the Panda Gatedefender Appliance using the command `ssh -N -f -L 12345:10.0.0.20:23 root@appliance` where `-N` tells SSH not to execute commands, but just to forward traffic, `-f` makes SSH run in the background and `-L 12345:10.0.0.20:23` maps the external system's port 12345 to port 23 on *myhost*, as it can be seen from the Panda Gatedefender Appliance.
3. The SSH tunnel from port 12345 of the external system to port 23 on *myhost* is now established. On the external system now it suffices to telnet to port 12345 on localhost to reach *myhost*.

#### SSH protocol version 1

This is only needed for old SSH clients that do not support newer versions of the SSH protocol.

#### Warning

The activation of the SSH version 1 is strongly discouraged, since this version is not maintained anymore, deprecated, and contains well known vulnerabilities that could be exploited by malicious users. SSH clients nowadays shall always use version 2 of SSH, which is more secure and reliable.

#### Allow TCP forwarding

Ticking this option lets other protocols be tunneled through SSH. See [SYS-1](#) example for a sample use case.

#### Allow password based authentication

Permit logins using password authentication.

#### Allow public key based authentication

Logins with public keys are allowed. The public keys of the clients that can login using key authentication must be added to the file `/root/.ssh/authorized_keys`.

#### Save

Click on this button at the bottom of the box to save the setting of the above four options.

#### Note

The SSH access is automatically activated when at least one of the following options is true:

- Panda support team access is allowed in Menubar › System › Support.
- High availability is enabled in Menubar › Services › High Availability.
- SSH access is enabled in Menubar › System › Panda Network › Remote Access.

#### SSH host keys

At the bottom of the page, a box details the public SSH host keys of the Panda Gatedefender Appliance, that have been generated during the first start of the openSSH server, along with their fingerprints and their size in bits.

## GUI Settings

Two configuration options for the GUI are present here. The first option is the language that will be used for the section names, the labels, and all the strings used in the web interface and can be selected from a drop-down menu. The languages currently supported are: English, German, Italian, Simplified Chinese, Japanese, Portuguese, Russian, Spanish, and Turkish.

The second option is to display the hostname of the Panda Gatedefender Appliance in the browser's window title, activated by ticking the checkbox *Display hostname in window title*.

## Backup

In this section the management of the backups can be carried out: Creation of backups of the current Panda Gatedefender Appliance configuration and system rollback to one of these backups when needed. Backups can be saved locally on the Panda Gatedefender Appliance host, on a USB stick, or downloaded to a workstation.

It is also possible to reset the configuration to factory defaults, to create fully automated backups, and to carry out various other administrative tasks concerning backups.

This section is organised into two tabs, *Backup* and *Scheduled backups*: The former is used to manage manual backups, while the latter to set up automatic, scheduled backups.

## Backup

In the *Backup* tab there are four boxes, that allow to manage the manual backups.

### Backup sets

The first box contains a list of the backups stored on the Panda Gatedefender Appliance - both manually and scheduled ones, an option to create a new backup, and the legend of the symbols that accompany each backup. If a USB stick is plugged in in the Panda Gatedefender Appliance and detected, also backups stored on it are displayed.

When clicking on the *Create new Backup* button, a dialogue box opens up in which to select the data to be included in the backup.

#### *Current configuration*

The backup contains all the configuration settings, including all the changes and customisation done so far, or, in other words, all the content of the `/var/efw` directory.

#### *Include database dumps*

The content of the database will also be backed up.

#### Warning

The database dumps may contain sensitive data, so whenever a backup contains a database dump, make sure that it is stored in a safe place.

#### *Include log files*

Include the current log files (e.g., `/var/log/messages`, but not log files of the previous days).

#### *Include log archives*

Include also older log files, that have been rotated, like e.g., `/var/log/messages.YYYYMMDD.gz`, etc. Backups created with this option may become very big after some time.

#### *Remark*

A comment about the backup, that will appear in the *Remark* column of the table. Hence, it should be meaningful enough to allow a quick recall of the content.

At least one of the checkbox must be ticked to create a new backup.

The format and name of the backup files.

Backup files are created as **tar.gz** archives, using standard Linux's tools **tar** and **gzip**. The files stored in the archive can be extracted using the **tar xzf archivename.tar.gz** or **tar vzf archivename.tar.gz** to see all the file processed and extracted and see some informative message on the screen, the **v** option meaning *verbose*. The name of the backup file is created to be unique and it conveys the maximum information possible about its content, therefore it can become quite a long string, like e.g., **backup-20130208093337-myappliance.mydomain-settings-db-logs-logarchive.tar.gz**, in which `20130208093337` is the timestamp of the backup's creation, in the form `YYYYMMDDHHMMSS` -in this example, 8th of February 2013 at 9:33:37 AM. This choice allows the backups to be lexicographically ordered from the oldest one to the most recent one; `myappliance.mydomain` are the Panda Gatedefender Appliance's hostname and domainname as set in Step 3 of the [Network configuration](#) (Menubar › System › Network configuration), and `settings-db-logs-logarchive` represent the content of the backup. In this case it is a full backup, since all four parts appear in the name. For example, a backup containing only settings and logs will be identified by the string `settings-logs`.

In order to create a backup on a USB external drive, a USB drive (even a stick) must be plugged in in the Panda Gatedefender Appliance. It is suggested to use a FAT32/VFAT filesystem, as this maximises portability to other systems. When the stick is detected,

the message *USB stick detected* will appear on the right-hand side of the box, along with a new option *Create backup on USB stick*. The checkbox next to this option must be ticked for the backup to be stored on the stick.

Click on the *Create Backup* button to create the backup. After a short time, during which the files required by the backup are gathered and assembled into the archive, the new backup appears in the list. The end of the backup process is marked by a yellow callout that appears above the box, showing the message *Backup completed successfully*.

The list of available backups, which is initially empty, presents for every backup the creation date, the content shown by a set of letters, the remark, and the list of actions available on each backup file. Automatic backups are marked with the string *Auto - backup before upgrade*.

The content of each backup is marked by at least one of the following letters or symbols, corresponding to the option specified during its creation:

A, Archive. The backup contains archived log files.

C, Cron. The backup has been created automatically by a scheduled backup job.

D, Database dumps. The backup contains a database dump.




E, Encrypted. The backup file is encrypted.

L, Log files. The backup contains today's log files.

S, Settings. The backup contains the configurations and settings.

U, USB. The backup has been saved to a USB stick.

!, Error. Something did not succeed while sending the backup file by email.

The available actions are to export  an archive to the local workstation, to delete it , or to restore it  on the Panda Gatedefender Appliance.


### Encrypt backup archives

The second box makes available the option to encrypt all the backups by providing a GPG public key. Select the GPG public key by clicking on the *Choose file* button to upload the key file from the local file system. Make sure the checkbox *Encrypt backup archives* is ticked, then upload the key file by clicking on *Save*.

Hint

Encrypt backup archives whenever saving sensible data in the backup file, like for example the passwords of users stored in the database or hotspot's users data and billing information.

### Import backup archive

The third box lets a previously saved backup archive be uploaded to the Panda Gatedefender Appliance. The backup file can be selected by clicking on the *Choose file* button and then choosing the backup file from the local file system. Optionally, some note to the backup can be added in the *Remark* field. Finally, the backup is uploaded by clicking on the *Import* button. The backup appears after a short period in the backup list at the top of the page, and can be restored by clicking on the restore icon .

Note

It is not possible to import encrypted backups on the Panda Gatedefender Appliance: Any encrypted backup must be decrypted before being uploaded.

### Reset configuration to factory defaults and reboot

The fourth box allows to wipe out all configurations and settings done so far and reboot the system with the default configuration. This result is achieved by clicking on the *Factory defaults* button: The configuration of the Panda Gatedefender Appliance is reset to the factory defaults and rebooted immediately, right after a backup copy of the current settings has automatically been saved.

## Scheduled backups

Automated backups of the system can be enabled and configured in the *Scheduled backups* tab, which contains two boxes.

### Scheduled automatic backups

In the first box, automatic backups are enabled and configured. When enabled, the elements of the Panda Gatedefender Appliance to be included in the backup can be chosen as seen in the [Backup Sets](#) box in the other tab. The only difference is that for scheduled backups there is no possibility to specify a remark. Additional options are:

#### *Enabled*

Enable scheduled backups.

#### *Keep # of archives*

Choose from the drop-down how many backups to keep on the Panda Gatedefender Appliance (from 2 up to 10, but they can be exported to save space).

#### *Schedule for automatic backups*

The frequency between backups, either hourly, daily, weekly, or monthly.

### Send backups via email

In the second box, the system can be configured to send or not the backups by e-mail. The following options are available.

#### *Enabled*

Allows backup archives to be sent via e-mail.

#### *email address of recipient*

The e-mail address to which to send the e-mail with the backup.

#### *email address of sender*

The e-mail address that will appear as the sender's e-mail address, which proves useful when backups should appear to have been sent from a special address (say, backups@myappliance.mydomain), and must be provided if the domain or hostname are not resolvable by the DNS.

#### *Address of smarthost to be used*

The address of a smarthost to be used to send the e-mails, which is needed in case the outgoing e-mails should go through a SMTP server, like, e.g., the Company's SMTP server, rather than to be sent directly by the Panda Gatedefender Appliance.

#### Hint

The explicit address of a smarthost is needed if the SMTP proxy (Menubar -> Proxy -> is not enabled. SMTP) is disabled.

#### *Send a backup now*

A click on this button will save the settings and immediately try to send an e-mail with the backup's archive as attachment, an action that serves also as a test for the correctness of the data supplied.

## Shutdown

Option to either shutdown or reboot the Panda Gatedefender Appliance, by clicking on the *Shutdown* or the *Reboot* button respectively, are provided in this page.

#### Warning

The shutdown or reboot process starts immediately after clicking on the respective button, with no further confirmation request.

After a reboot, it is possible to continue to use the GUI without the necessity of an authentication.

## License Agreement

This section displays the license agreement between Panda and the owner of the Panda Gatedefender Appliance.

#### Note

After an upgrade, if the license agreement changes, at the first login it is necessary to accept the new license agreement before accessing the upgraded system and being allowed to use the Panda Gatedefender Appliance

# 3. The Status Menu

---

The status menu provides a set of pages that display information in both textual and graphic views about various daemons and services running on the Panda Gatedefender Appliance. No configuration option is available in this module, which only shows the current and recent status of the Panda Gatedefender Appliance.

The following items appear in the sub-menu on the left-hand side of the screen, each giving detailed status information on some functionalities of the Panda Gatedefender Appliance:

- System status - services, resources, uptime, kernel
- Network status - configuration of network interfaces, routing table, ARP cache
- System graphs - graphs of resource usage
- Traffic Graphs - graphs of bandwidth usage
- Proxy graphs - graph of HTTP proxy access statistics in the last 24 hours (week, month, and year)
- Connections - list of all open TCP/IP connections
- OpenVPN connections - list of all OpenVPN connections
- SMTP mail statistics - graphs about the SMTP service.
- Mail queue - SMTP server's mail queue

## System Status

The default page that opens when clicking on Menubar › Status is the *System status* page, which gives a quick overview of the running services, memory, disk usage, uptime and users, loaded modules, and the kernel version, each in its own box. At the top of the page, there are hyperlinks to each box. In more details, these are the information presented in each box, which are usually the output of some Linux command.

### Services

The status -marked as either *Stopped* or *Running* by a red or green square- of each service installed on the Panda Gatedefender Appliance is shown here. A service might appear as stopped because the corresponding daemon or script is not enabled.

### Memory

The output of the Linux **free** command supplies the data shown here. All data are represented with the real amount in kilobytes, and with a bar to ease the visualisation of the memory used. The first line shows the total used RAM memory, for which is normal to be close to 100% for a long time running system, since the Linux kernel uses all available RAM as disk cache to speed up I/O operations. The second line shows the memory actually used by processes: Ideally this value 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. If the memory usage remains for long periods of time over 80%, RAM should be added to improve performances. 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

The output of the Linux **df** command shows the disk devices -physical disks and partitions, their mount point and the space of each disk partition. Depending on the type of the Panda Gatedefender Appliance, the data displayed in this box differ. Usually, they are:

- The main disk `/dev/hda1`.
- The data disk `/dev/mapper/local-var`.
- The configuration disk, where all the Panda Gatedefender Appliance settings are stored `/dev/mapper/local-config`.
- The log disk `/dev/mapper/local-log`.
- The shared memory, `/dev/shm/`.

### Note

The data disk and the log disk may grow over time, so there should be reserved enough space for them - especially the log disk. Remember also that disks shall never be full above the 95%, since this may hinder the correct working of the system.



### Uptime and users

This box shows the output of the Linux **w** command, which reports the current time, information about how long the system has been running since last reboot, the number of console users that are currently logged into the system (though normally there should be none) and the system load average for the past 1, 5, and 15 minutes. Additionally, if any console user is logged into the system, some information about the user is displayed (like the remote host from which she is logged in or what is she doing). More details can be found on the [w\(1\)](#) manual page.

### Loaded modules

The output of the Linux **lsmod** command. It shows the kernel modules currently loaded into memory. This information should be useful to advanced users only.

### Kernel version

The output of the Linux **uname -r** command, which shows the current kernel version.

## Network status

This page contains several information about the running state of the network interfaces. Four boxes are present on the page, and, like for the System status, hyperlinks are provided at the top of the page for a quicker access. The boxes contain the following information, representing the output of different shell commands.

### Interfaces

The first box reports the output of the **ip addr show** command which provides for each network interface the associated MAC address, IP address, and additional communication parameters. The active interfaces are highlighted with the colour of the zone they are serving. The interface can be an ethernet interfaces, a bridge, or a virtual device.

### NIC status

The running configuration and capabilities of each of the NIC are shown here. Each interface is highlighted with the colour of the zone it is serving and is labelled as **[Link OK]** to indicate that it is working. Interfaces that are not used are labelled with **[NO Link]**. The command providing the output is **ip link show**.

### Routing table entries

The kernel routing table, as provided by the **route -n** command. Typically, there should be one line per active interface, which correctly routes the traffic within the zones served by the Panda Gatedefender Appliance, plus a default route (recognisable by the 0.0.0.0 Destination field) that allow the traffic to reach the Internet.

### ARP table entries

The last box shows the output of the **arp -n** command and shows the ARP table, i.e., a table containing the MAC address associated to each known IP address in the local network.

## System graphs

The graphs displayed in this page present the usage of resources during the last 24 hours: CPU, memory, swap, and disk usage, each accompanied with a legend of the data included in the graph, their associated colour, and a summary of the maximum, average, and current percentage of use. Moreover, a message informs of the time and date of the last update to the graphs, which matches the last access to the page.

When clicking on one of the graphs, a new page will open, with summaries of the usage graphs for the last day, week, month, and year. In these pages, a click on the *BACK* button allows to return to the previous page.

### Note

The *nan* (short for "Not A Number") string that may appear in the summaries designate that there are not enough data to calculate the usage of the selected resource. It can appear for example in the "per year usage" when the Panda Gatedefender Appliance is used for only a few weeks.

### CPU graph

In this box is shown the CPU usage per day of the Panda Gatedefender Appliance, measured in percentage of the CPU time used by the various processes. The output is provided by the **top** command. Different colors are used to denote the type of running processes:

- White - idle, i.e., time the CPU is not used by any process.
- Green - nice processes, i.e., user processes which have changed their default priority.
- Blue - user processes with default priority.
- Orange - time spent by the CPU waiting for I/O tasks to complete.
- Red - system (kernel) processes
- Pink - softirq, i.e., the time spent for software interrupts
- Brown - interrupt, i.e., is the time spent for hardware interrupts
- Black - steal meaningful only if running as a virtual machine, is the time used by the hypervisor to run the VM.

### Memory graph

This graph shows the memory usage during the last 24 hours. The following colours are used to denote the types of memory:

- Green - unallocated memory, that can be allocated to new processes.
- Blue - cache memory, copy of recent data used by processes.
- Orange - buffer memory, a temporary portion of memory that stores data to be sent to -or received from- external devices.
- Red - used memory.

### Swap graph

The usage of the swap area, located on the hard disk, is displayed in this box.

- Green - unallocated swap.
- Blue - cached swap.
- Red - swap space used.

### Disk usage graphs

Graphs showing the usage of the disk are split into four boxes, each showing the usage of a partition. In each of them, the green colour shows the free space, while the red colour shows the disk space used.

## Traffic graphs

This page contains the traffic graphs for the last 24 hours, divided by zone. Hence, depending on the zones enabled and configured, this page will contain 2, 3, or 4 boxes, each with one graphs. Like for the *System graphs*, the graphs are accompanied with a legend of the data displayed:

- Green - the outgoing traffic.
- Blue - the incoming traffic

Below the graphs, also the summary of the average, maximum, and current amount of data transmitted and received is displayed and updated in real time.

When clicking on one of the graphs, a new page will open, with summaries of the data flown through the Panda Gatedefender Appliance for the last day, week, month, and year. The data shown are the same in all the graphs: Incoming and outgoing traffic in blue and green respectively. In

Hint

To go back to the page with all the zone's graphs, click on the *BACK* hyperlink on the bottom of the page.

## Proxy graphs

The access statistics of the HTTP proxy during the last 24 hours are shown here. There are no graphs in this page if the HTTP proxy service is not active and has never been enabled. However, if the service has been running even for a short period during the last year,

the data produced are still accessible by clicking on the graph. Similarly to the other graphs, older statistics are shown for the last day, week, month, and year. In this page, a click on the *BACK* hyperlink on the bottom allows to go back to the main page.

Note

To show the proxy graphs, HTTP proxy logging must be enabled under Proxy › HTTP › Configuration › Log settings, by ticking the *Enable logging* checkbox. Also *queried terms* and *useragents* can be logged to produce more detailed logs and graphs.

After the HTTP proxy has been enabled, the four boxes show the following data:

- *Total traffic per day*: the amount of data flown through the Panda Gatedefender Appliance's proxy service. In green is show the outgoing traffic, while in blue the incoming traffic.
- *Total Accesses per Day*: The number of HTTP requests, depicted in blue, received by the Panda Gatedefender Appliance.
- *Cache hits per day*: The number of cache data requested
- *Cache hits ratio over 5 minutes per day*: The number of cache data requested during a five minutes period.

## Connections

This page shows a table containing the list of current connections from, to, or going through the Panda Gatedefender Appliance. The data shown here are devised by the kernel conntrack table. The following colours are employed in the table and used as the background of the cells in the table to denote the source and destination of the connection.

- Green, red, orange, and blue are the zones governed by the Panda Gatedefender Appliance.
- Black is used for connections involving the firewall, including daemons and services, like e.g., SSH or web accesses).
- Purple shows connections using VPN or IPsec.

The data displayed in the table are the following.

*Source IP*

The IP from which the connection has originated.

*Source port*

The port from which the connection has originated.

*Destination IP*

The IP to which the connection is directed.

*Destination port*

The port to which the connection is directed.

*Protocol*

The protocol used in the connection, which is typically tcp or udp.

*Status*

The current status of the connection, meaningful only for TCP connections. They are defined in [RFC 793](#), significant states are *ESTABLISHED* (connection is active) and *CLOSE* (no connection).

*Expires*

How long will the connection remain in that particular status.

Hint

The page refreshes automatically every 5 seconds.

Each IP address and each IP port in the table can be clicked to obtain useful information. Clicking on the IP address will launch a [whois](#) query that will display who the owner of the IP address is and where it is located. Clicking on the port number will open the Internet Storm Center web page, with information about the port (i.e., the purpose for which it is used) and about which services or malware (e.g., Trojans, viruses) may exploit that port and the number of attacks received on those ports by various servers worldwide.

## VPN connections

When you use the Panda Gatedefender Appliance there are OpenVPN or IPsec servers running, this page shows the connected users, along with the service they rely on for the connection (OpenVPN, L2TP, IPsec Xauth), the time stamp since they are connected, and the possible actions that can be carried out. Currently, only to disconnect the user.

## SMTP mail statistics

Four boxes appear on this page showing graphs about the email sent by the local SMTP server on the Panda Gatedefender Appliance for the current day, week, month, and year.

Hint

Neither information nor graphs are displayed if the SMTP server is not enabled.

Each box contains two graphs, both of which present on the y-axis the number of e-mail per minute and on the x-axis the time, whose unit of measure changes according to the type of graph: A two hours span in the *Day graphs*, one day in the *week graphs*, one week in the *Month graphs* and one month in the *year graphs*.

The graph on the top shows a summary of the number of message per minute sent (in blue) or received (in green) by the Panda Gatedefender Appliance. The graph at the bottom can be seen as a more fine-grained version of the other graph, since it displays the e-mails that have been rejected (in red) or bounced (in black), those that have been intercepted because they contain viruses (in yellow), and those that have been recognised as spam (in grey).

Below each graph, there are also textual information concerning each category of email (sent, received, rejected, bounced, virus, and spam) about the total number, the average, and the highest number of e-mail ("*msgs*") processed, plus the timestamp (date and time) of the latest update to the page.

## Mail queue

When the SMTP proxy is enabled, this page shows the current e-mail queue. With no e-mails in the queue, the message *Mail queue is empty* is displayed, but when some e-mail is there, it is possible to flush the queue by clicking on the *Flush mail queue* button. With the SMTP proxy disabled, only the message recalling its disabled status is shown.

# 4. The Network Menu

---

The network menu can be used to tweak the network configuration by adding specific hosts and routes, or configuring the uplink and adding VLANs. This menu should not be confused with the Network configuration wizard available at [Menubar > System > Network Configuration](#), that allows to configure interfaces, zones, and to define uplinks. Many settings and configuration options, especially under [Interfaces](#) below are however the same found under the network wizard, to which to refer for a more detailed help.


The sub-menu on the left-hand side of the screen contains these items, each of which groups several configuration options:

- Edit hosts - define hosts for local domain name resolution
- Routing - set up static routes and policy routing
- Interfaces - edit the uplinks or create VLANs

## Edit hosts

The page contains the list of hosts previously defined. Each line contains an IP address, the associated hostname, and the domain name, if specified. Two available actions are available for each entry: To edit it or to delete it.

### Warning

Deleting an host entry by clicking on the small  icon does not require any confirmation and is not reversible. If deleted by mistake, an entry must be re-added manually.

A new entry in the file can be added by clicking on the *Add a host* link right above the table. A simple form will replace the table, in which to enter the following options:

#### *IP address*

The IP address of the remote host.

#### *Hostname*

The hostname associated to the IP address.

#### *Domain name*

An optional domain name.

### Note

Unlike in the `/etc/hosts` file (see below), each IP address added here corresponds to one hostname and viceversa. To add two hostnames to a same IP, add two entries with the same IP address.

The choice can be confirmed by clicking on the *Add Host* button. To associate more hostnames to the same IP address, repeat the procedure by inserting the same IP address but a different name.

Hosts management, dnsmasq and `/etc/hosts`.

The dnsmasq application is used in small networks as DNS server for local hosts and as a DNS forwarder and caching server for worldwide DNS servers. The Panda Gatedefender Appliance uses dnsmasq to be able to correctly resolve and answer DNS requests coming from the GREEN, ORANGE, and BLUE zones. It is sometimes desirable (e.g., for testing purposes on a remote website) to override some entries in dnsmasq, or to add some local server to dnsmasq's cache, for local clients to be able to connect to it.

The hosts added in this page are stored in a dnsmasq's settings file and merged with the `/etc/hosts` file at every restart of the daemon. Host added to that files directly via CLI will not persist after a reboot of the Panda Gatedefender Appliance or a restart of dnsmasq.

The `/etc/hosts` file contains the so-called static lookup table, in the form:

```
IP1 hostname1 [hostname2]
IP2 hostname3 [hostname4] [hostname5]
```

Here, *IP1* and *IP2* are unique (numerical) IP addresses and *hostname1*, *hostname2*, *hostname3*, *hostname4*, and *hostname5* are custom names given to those IPs. Names within square brackets are optional: In other words, each IP address can be associated with one or more names of known hosts. Custom host entries can be added to the file, that will then be resolved for all the clients connecting through the Panda Gatedefender Appliance. On a typical Panda Gatedefender Appliance, the `/etc/hosts` file contains at least the following entries:

```
127.0.0.1    localhost.localhost localhost
172.20.0.21  myappliance.localdomain myappliance
172.20.0.21  spam.spam spam
172.20.0.21  ham.ham ham
172.20.0.21  wpad.localdomain wpad
```

Here, 127.0.0.1 is the IP address of the loopback device, *localhost*, which is a mandatory entry for the correct work of any Linux system; while 172.20.0.21 is the IP address of the GREEN interface. The entries listed for that IP have the following meaning and purposes:

*myappliance.localdomain*

The hostname and domainname of the Panda Gatedefender Appliance, as set up during the Network configuration.

*spam.spam spam* and *ham.ham ham*

These two entries combined are used for the training of the spamassassin e-mail filter.

*wpad.localdomain wpad*

A facility for some browsers to detect and apply proxy settings automatically without the user's interaction when the proxy is not transparent.

## Routing

Besides the default routing table, that can be seen in Menubar > Status > Network status, the routing on the Panda Gatedefender Appliance can be improved with static and policy routing rules. This page displays a unique table that contains all the custom routings, although new rules are added from the two different tabs that present on this page. Indeed, static and policy routing rules require slight different settings. The table contains a summary of the rule: the source and destination networks or zones, the gateway, a remark, and the list of available actions: Enable or disable, edit, and delete a rule.

Whenever a modification is carried out on the routing table, it is required that the changes be saved and the service be restarted.

### Static routing

A static route allows to associate specific source and destination networks with a given gateway or uplink. A click on the *Add a new route* link above the table allows create new routes by defining the following fields in the form that will appear:

*Source Network*

The source network, in CIDR notation.

*Destination Network*

The destination network, in CIDR notation.

*Route Via*

Four options are available to define through which means should the traffic be channeled: *Static Gateway*, *Uplink*, *OpenVPN User*, or *L2TP User*. In the case the *Static Gateway* is selected, the IP address of a gateway should be provided in the text box on the right. Otherwise, a drop-down will appear, proposing the choice among the available uplinks, OpenVPN users, or L2TP users.

*Enabled*

A ticked checkbox means that the rule is enabled (default). If unchecked, then the rule is only created but not activated: It can always be enabled later.

*Remark*

A remark or comment to explain the purpose of this rule.

A click on one of the icons will trigger an action on the respective item:

- - toggle the status of the item, enabled or disabled.
- - modify the item's property.
- - remove the item

### Policy routing

A policy route rule allows to associate specific network addresses, zones, or services (expressed as port and protocol) with a given uplink.

The table shows all the already defined rules for both static and policy routing, with some of their properties: Source, Destination, TOS, Gateway, Service, Remark, and the available actions:

- - move a rule
- - toggle the status of the item, enabled or disabled.
- - modify the item's property.
- - remove the item

Hint

The TOS column appears only if at least one rule with that field has been defined.

Rules that appear higher in the table have higher priority.

Policy routing, HTTP proxy, and uplink.

The interaction between these three components of the Panda Gatedefender Appliance might produce some behaviour that may appear strange or even wrong when clients in the zones try to access the Internet. There are indeed three steps to highlight, for a correct understanding how traffic flows to the Internet when both HTTP proxy is enabled and there are policy routing rules defined:

1. An HTTP proxy uses the *main* uplink (i.e., it accesses the RED zone and the Internet using the main uplink).
2. An HTTP proxy "breaks" a connection from a client to a remote server in two connections: One from the client to the Panda Gatedefender Appliance and one from the Panda Gatedefender Appliance to the remote server.
3. Policy routing rules are taken into account *after* the traffic goes through the HTTP proxy.

When clicking on the *Create a policy routing rule* link, a form will open, which seems rather more complicated than the one for static routes and very similar to the firewall rule's editor. However, this policy rule editor is much like the previous one, but gives more control over the definition of the rule. Additionally, the setup of the rule is guided by several drop-down menus, to simplify entering the data in the following fields:

#### *Source*

The first drop-down menu allows to choose the source of the traffic. More entries, one per line, are accepted, but all must belong to the same type, either: A zone or interface, OpenVPN or L2TP users, IPs or networks, or MAC addresses. Depending on the choice, different values shall be supplied. To apply the rule to all sources, select <ANY>.

#### *Destination*

The second drop-down menu permits the choice of the destination of the traffic, in form of a list of IPs, networks, OpenVPN or L2TP users. Again, by selecting <ANY> the rule will match every destination.

#### *Service/Port*

The next two drop-down menus allow to specify the service, protocol, and a destination port for the rule when the TCP, UDP, or TCP + UDP protocols are selected. Some predefined combinations service/protocol/port exists, like HTTP/TCP/80, <ALL>/TCP+UDP/0:65535, or <ANY>, which is a shortcut for *all services, protocols, and ports*. *User defined* permits to specify a custom protocol and the ports to block, an option that proves useful when running services on ports different from the standard ones.

#### *Protocol*

The type of traffic that is interested by the rule: *TCP*, *UDP*, *TCP+UDP*, *ESP*, *GRE*, and *ICMP*. TCP and UDP are the most used, GRE is used by tunnels, ESP by IPsec, and ICMP by the **ping** and **traceroute** commands.

#### *Route Via*

How the traffic should be routed for this rule. Four options are available:

1. Static gateway: In this case an IP Address shall be provided
2. Uplink: The uplink that should be used for this rule. There is the option, when the uplink becomes unavailable, that the routing be carried over to the backup link corresponding to the selected uplink. This option is enabled when the checkbox next to the drop-down menu is ticked.
3. OpenVPN user: An OpenVPN user, chosen from those available in the drop-down menu.
4. L2TP user: An L2TP user, chosen from those available in the drop-down menu.



### Type Of Service

The type of service (TOS) can be chosen here. Four values can be chosen, depending on what is the most important characteristic of the traffic interested by that rule: *default*, *lowdelay*, *reliability*, or *throughput*.

### Remark

A remark or comment to explain the purpose of this rule.

### Position

The position in which to insert the rule (relative position in the list of rules).

### Enabled

Tick this checkbox to enable the rule (default). If unchecked, the rule is created but not active: A rule can be enabled later.

### Log all accepted packets

This checkbox must be ticked to log all the packets affected by this rule.

### Warning

The activation of this option may cause the size of the log files to dramatically improve.

## Interfaces

The uplinks manager allows to carry out a number of tasks that are related with the uplink and the interfaces, and in particular to define custom VLANs on the network interfaces.

### Uplink editor

By default, the uplink editor shows the available uplinks that have been created and the actions that can be executed on each of them, by clicking on the icons in the last column, *Actions*:

- - toggle the status of the item, enabled or disabled.
- - modify the item's property.
- - remove the item

### Hint

The main uplink can not be deleted.

Additional uplinks can be defined by clicking on the *Create an uplink* hyperlink above the list of uplinks. A rather long page, full of configurable options will open, that should be filled with appropriate values -very similar to those in the network configuration. Depending on the type of uplink chosen, the available settings will differ.

### Note

Not all the available options are described here: They are the same that are present in the network configuration wizard and depend on the type of the uplink chosen, so please refer to that section for the full explanation of each option.

### Description

A description of the uplink.

### Type

The selection of the type of RED connection includes one additional protocol, compared to those available in the network configuration wizard: **PPTP**. PPTP can be configured to work in static or in DHCP mode, selectable from the respective value from the "PPTP method" drop-down. The IP address and netmask must be defined in the appropriate textfields if the static method has been chosen, in which case additional IP/netmask or IP/CIDR combinations can be added in the field below if the checkbox is ticked. Phone number, username, and password are not required but may be needed for some configurations to work, depending on the provider's settings. The authentication method can be either PAP or CHAP: if unsure, keep the default value "PAP or CHAP".

### Uplink is enabled

Tick this checkbox to enable the uplink.

### *Start uplink on boot*

This checkbox specifies whether an uplink should be enabled at boot time or not. This option proves useful for backup uplinks which are managed but do not need to be started during the boot procedure.

### *Uplink is managed*

Tick this checkbox for the uplink to be managed. See the Uplink Information Plugin under Menubar › System › Dashboard for a discussion about managed and manual modes.

### *if this uplink fails activate*

If enabled, an alternative connection can be chosen from a drop-down menu, which will be activated when this uplink fails.

### *Check if these hosts are reachable*

Tick this option to enter a list of IP or hostnames that will be **ping**-ed when the uplink fails, to check whether it has reconnected.

Hint

One of those hosts could be the provider's DNS server or gateway.

In the advanced settings panel, two other options can be customised:

### *Reconnection timeout*

The time interval (in seconds) after which an uplink tries to reconnect if it fails. This value depends on the provider's settings. If unsure, leave this field empty.

### *MTU*

A custom value for the MTU size. See here for a discussion about the reasons to modify the default value.


See also

Network configuration, steps 1, 4, and 5.

Menubar › System › Network Configuration

## **VLANs**

The idea behind offering VLAN support in Panda Gatedefender Appliance is to allow arbitrary associations of VLAN IDs to the zones and to provide an additional level of separation (and therefore adding another level of security) between the zones. The existing VLANs are shown in the table, if any had already been created. The only action available is:

-  - remove the VLAN. A pop-up window will open, that requires a confirmation for the deletion.

A new VLAN can be defined by clicking on the *Add new VLAN* hyperlink above the VLAN list. In the form that will open a few clicks suffice to create an association between an interface and a VLAN, by specifying a few values:

### *Interface*

The physical interface to which the VLAN is connected to. Only the available interfaces can be chosen from the drop-down menu. The menu also shows the status of the link of the interface.

### *VLAN ID*

The VLAN ID, which must be an integer number between 0 and 4095.

### *Zone*

The zone to which the VLAN is associated with. Only the zones that have been defined in the network configuration wizard can be selected. The option "NONE" can be chosen, if that interface is used as a High Availability management port.

### Warning

It is not possible to define a VLAN that serves one zone (e.g., a VLAN on BLUE) on an interface that already serves another zone (e.g., eth1 serving GREEN). When trying to do so, the form closes and a red callout appears, informing that the VLAN can not be created.

Whenever a virtual LAN is created, a new interface is created and named as **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 and will show up as a regular interface in the various sections that report network information, like Menubar › Status › Network Configuration or in the Dashboard, where it can be selected to be drawn in the graph.

# 5. The Services Menu

---

The Panda Gatedefender Appliance includes many useful services to prevent threats and to monitor the networks and the running daemons, whose activation and set up is explained in this section. In particular, among them, we highlight the various proxy services, such as the antivirus engine, as well as the intrusion detection system, high availability, and traffic monitoring. The available services appear as items in the sub-menu list on the left-hand side of the screen.

- DHCP server - DHCP server for automatic IP assignment
- Dynamic DNS - Client for dynamic DNS providers such as DynDNS (for home / small office use)
- Antivirus Engine - configure the antivirus engine used by the e-mail, web, pop, and FTP proxies
- Time server - enable and configure the NTP time server, set the time zone, or update the time manually
- Mail Quarantine - manage quarantined emails
- Spam Training - configure training for the spam filter used by the mail proxies
- Intrusion Prevention - configure snort, the IPS
- High availability - configure the Panda Gatedefender Appliance in a high availability setup
- Traffic Monitoring - enable or disable traffic monitoring with ntop
- SNMP Server - enable or disable support for the Simple Network Management Protocol
- Quality of Service - IP traffic prioritisation.

## DHCP server

The DHCP server is used by the clients (workstations and servers) in the zones controlled by the Panda Gatedefender Appliance to receive an IP address ("lease"), and allows to control the IP address assigned to them in a centralised way. Two types of leases can be assigned to clients: Dynamic and fixed. The DHCP server page is divided into two or three boxes, namely *DHCP*, in which to configure the DHCP server, *Current fixed leases*, showing the fixed leases, and *Current dynamic leases* that shows up only if at least one client has obtained a dynamic lease. Dynamic leases are assigned on a network basis within a given range that is configured in the first box, whereas fixed leases are assigned on a per-host basis and are configured in the second box.


### DHCP

When a client (be it either a host or another device such as networked printer) joins the 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, which is sometimes called "automatic network configuration", and is often the default setting on most workstations. Dynamic leases are configured on a zone basis: for example, it is possible to enable them only for clients in the GREEN zone, while the other active zones receive only fixed leases.

It is however possible to let also devices in the ORANGE (DMZ) or BLUE (WLAN) zone to receive dynamic leases.

#### Note

If the BLUE zone is enabled but managed by the hotspot, the message *DHCP configuration is managed by hotspot* appears, preventing to configure it here.

To customise the DHCP parameter for each zone, click on the small icon  next to the *Settings* label. These are the available options:

#### *Enabled*

Enable the DHCP server in the zone.

#### *Start address, End address*

The range of IP addresses to be supplied to the clients. These addresses have to be within the subnet that has been assigned to the corresponding zone. If some hosts should receive a fixed lease, (see [below](#)), make sure their IP addresses are included *neither* in this range *nor* in the range of the OpenVPN address pool (see Menubar › VPN › OpenVPN server) to avoid conflicts.

Leaving these two fields blank will use the whole IP range of the zone for dynamic leases.

#### *Allow only fixed leases*

Tick this checkbox to use fixed leases *only*. No dynamic lease will be assigned.

#### *Default lease time, Max lease time*

The default and the maximum time in minutes before the assignment of each lease expires and the client requests a new lease from the DHCP server.

#### Domain name suffix

The default domain name suffix that is passed to the clients and that will be used for local domain searches.

#### Default Gateway

The default gateway that the clients in the zone will use. If left blank, the default gateway is the Panda Gatedefender Appliance itself.

#### Primary DNS, Secondary DNS

The DNS used by the clients. Since the Panda Gatedefender Appliance contains a caching DNS server, the default value is the firewall's own IP address in the respective zone, though a second server or even the primary value can be changed.

#### Primary NTP server, Secondary NTP server

The NTP servers used by the clients, to keep the clocks synchronised.

#### Primary WINS server, Secondary WINS server

The WINS servers used by the clients. This option is only needed for the Microsoft Windows networks that use WINS.

Advanced users might want to add some custom configuration lines to be added to the `dhcpd.conf` file (e.g., custom routes to subnets) by writing them in the text area at the bottom, marked with the *Custom configuration lines* label.

#### Warning

No syntax check on these lines is carried out: the lines are appended to the configuration file. Any mistake here might inhibit the DHCP server from starting!

Example SRV-1 - PXE boot and `dhcpd.conf` configuration.

The customisation of the DHCP server proves useful in different networks configuration.

One common use case is for VoIP telephones that need to retrieve their configuration files from an HTTP server at boot time. In this case, the files may also reside on the Panda Gatedefender Appliance, so the configuration of the tftp server can be passed as extra lines like the following:

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

Note the use of `$GREEN_ADDRESS` which is a macro that is replaced in the `dhcpd.conf` file with the GREENIP of the Panda Gatedefender Appliance.

#### Current fixed leases

It is sometimes necessary or desirable for certain devices to always use the same IP address while still using DHCP, for example servers that provide services like a VoIP box, a SVN repository, a file server, or devices like printers or scanners. A fixed lease is usually referred to as *Static IP Address*, since a device will always receive the same IP address when requesting a lease from the DHCP server.

This box reports the list of all the fixed leases currently active in the local network, providing several information about that lease. By clicking on the *Add a fixed lease* link, new fixed leases can be assigned to a device and insert all the information that will be displayed in the list. The devices are identified by their MAC addresses.

#### Note

Assigning a fixed lease from the DHCP server is very different from setting up the IP address manually on a device. Indeed, in the latter case, the device will still contact the DHCP server to receive its address and to announce its presence on the network. When the IP address required by the device has already been assigned, however, a dynamic lease will be given to the device.

The following parameters can be set for fixed leases:

#### MAC address

The client's MAC address.

#### IP address

The IP address that will always be assigned to the client.

#### Description

An optional description of the device receiving the lease.

#### Next address

The address of the TFTP server. This and the next two options are useful only in a few cases (see below for an example).

#### Filename

The boot image file name. Option needed only for thin clients or network boot.




#### Root path

The path of the boot image file.

#### Enabled

If this checkbox is not ticked, the fixed lease will be stored but not written down to the file `dhcpd.conf`.

The actions available for each fixed lease in the table are:

-  - toggle the status of the lease, enabled or disabled.
-  - modify the property of the lease.
-  - remove the lease.

A use case for a fixed lease.

A use case that shows the usefulness of a fixed lease is the case of thin clients or disk-less workstations on the network that use PXE, i.e., boot the operating system from an image supplied by a networked tftp server. If the tftp server is hosted on the same server with the DHCP, the thin client receives both the lease and the image from the same server. More often, however, the tftp server is hosted on another server on the network, hence the client must be redirected to this server by the DHCP server, an operation that can be done easily adding a fixed lease on the DHCP server for the thin client, adding a next-address and the filename of the image to boot.

Besides the information supplied during the fixed lease creation, the list allow each lease to be enabled or disabled (by ticking the checkbox), edited, or deleted, by clicking on the icons in the *Actions* column. Editing a lease will open the same form as the creation of a new lease, whereas deleting a lease will immediately remove it from the configuration.

Note

All leases assigned by the DHCP server are stored by default in the `/var/lib/dhcp/dhcpd.leases` file. Although the DHCP daemon takes care of cleaning that file, it may happen that the file stores lease that have already been expired and are quite old. This is not a problem and does not interfere with the normal DHCP server working. A typical entry in that file is:

```
lease 192.168.58.157 {
starts 2 2013/06/11 13:00:21;
ends 5 2013/06/14 01:00:21;
binding state active;
next binding state free;
hardware ethernet 00:14:22:b1:09:9b;
}
```

#### Current dynamic leases

When the DHCP server is active, and at least one client has received a (dynamic) IP address, a third box appears at the bottom of the page, containing the list of the currently assigned dynamic IP addresses. This list report the IP address, the MAC address, the hostname, and the expiry time of the lease associated to each client.

## Dynamic DNS

A DNS server provides a service that allows to resolve the (numeric) IP address of a host, given its hostname, and vice versa, and works perfectly for hosts with *fixed* IP address and hostname.




DDNS providers, like DynDNS or no-IP, offer a similar service when the IP addresses is dynamic, which is normally the case when using residential ADSL connections: Any domain name can be registered and associated to a server with a dynamic IP address, which communicates any IP address change to the DDNS provider. To be compatible and to integrate with the root DNS servers, each time IP address changes, the update must then be actively propagated from the DDNS provider.

The Panda Gatedefender Appliance includes a dynamic DNS client for 14 different providers and if enabled, it will automatically connect to the dynamic DNS provider to communicate the new IP address whenever it changes.

Note

If no dynamic DNS account has been set up, detailed instruction to register a new one, detailed online helps and howtos are available on the web site of the providers.

This page displays the list of the Dynamic DNS accounts. Indeed, more than one DDNS provider can be used. For each account, the list shows information about the service used, the hostname and domain name registered, if the anonymous proxy and the wildcards are active, if it is enabled, and the possible actions:

-  - toggle the status of the lease, enabled or disabled.
-  - modify the property of the lease.
-  - remove the lease.

New accounts can be created by clicking on the *Add a host* link, providing the following parameters:

#### *Service*

The drop-down menu shows the available DDNS providers.

#### *Behind a proxy*

This option only applies to the no-ip.com provider. The checkbox must be ticked if the Panda Gatedefender Appliance is connecting to the Internet through a proxy.

#### *Enable wildcards*

Some dynamic DNS providers allow *all* the sub-domains of a domain point to the same IP address. This is a situation in which two hosts like `www.example.myddns.org` and `second.example.myddns.org` are both located on the same IP address. Ticking this box enables the feature, making all the possible sub-domains redirect on the same IP address. The feature must be configured also in the account on the DDNS provider server, if available.

#### *Hostname and Domain*

The hostname and domain as registered with the DDNS provider, for instance "example" and "myddns.org"

#### *Username and Password*

The credentials given from dynamic DNS provider to access the service.

#### *behind Router (NAT)*

Activate this option if the Panda Gatedefender Appliance is not directly connected to the Internet, i.e., there is another router or gateway before accessing the Internet. In this case, the service at <http://checkip.dyndns.org> can be used to find the IP address of the router.

#### *Enabled*

Tick this checkbox to enable the account, which is the default.

#### *Note*

It is still necessary to export a service to the RED zone to be able to use the domain name to connect to the Panda Gatedefender Appliance from the Internet using its dynamic IP address, since the dynamic DNS provider only resolves the domain name and not the associated services. Exporting a service might typically involve setting up port forwarding (see Menubar › Firewall › Port forwarding / NAT).

After making a change in the configuration or to immediately update the dynamic DNS for all the defined accounts, click on the *Force update* button. This proves useful for example when the uplink has been disconnected and the REDIP has changed: When this happens, updating all the DDNS accounts is required, otherwise the services offered via DDNS will be unreachable.

## Antivirus Engine

The antivirus engine on Panda Gatedefender Appliance is Panda, which will be used for the research of viruses and malware within files and documents that pass through the Panda Gatedefender Appliance via one of the running proxy services. There is only one tab in this page: *Panda Antivirus*.

#### Archive bomb and DoS.

Archive bombs are archives that use a number of tricks to overload an antivirus software to the point that they hog most of the resources of the computer hosting it, an action called DoS attack. These tricks include: 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); multiple nested archives (i.e., zip files inside zip files); archives that contain a large number of empty files, and so forth. Decompressing archive files with any of those

characteristic poses a serious challenge to the normal activities of a server or a workstation, since a lot of resources are needed (especially RAM and CPU) and taken away from users' availability.

## Panda Antivirus

The Panda Gatedefender Appliance features the Panda Antivirus Engine to protect internal networks against viruses and malware.

The first option available is to select the update cycle of the anti-virus signatures, which can be: *hourly*, *daily*, *weekly*, or *monthly*.

The scan options to be configured are grouped in 3 sections:

### File content analysis

The following options relate to the search for and the scan of various types of malware programs that may infect the workstations and server which lay behind the Panda Gatedefender Appliance.

#### *Clean infected files*

Tick the checkbox to enable the automatic cleaning of files during the anti-malware scan. When disabled, the option causes the deletion of the infected file, without trying to heal the file.

#### *Scan for known jokes*

Enable the scan of malware *jokes*, i.e., small programs that cause panic in the users without damaging or harming the user's workstation.

#### *Scan for known dialers*

Enable the scan of malware *dialers*, programs that try to dial telephone numbers without your consent.

#### *Scan for known spyware/adware*

Enables the search for spyware and adware programs.

#### *Scan for known hacking tools*

Tick the checkbox to enable the search for hacking tools malware.

#### *Scan for known security risks*

Enable the scan of malware known as Security Risks.

#### *Scan for known MIME vulnerabilities*

Tick the checkbox to enable the search for MIME vulnerabilities.

#### *Enable heuristic analysis*

Use the heuristic analysis of malware, to search for new types of malware that may not have been yet included in signatures.

#### *Heuristic level*

Choose the desired sensitivity level of the heuristic analysis, among the three available, *low*, *medium*, and *high*.

### Packaged and/or compressed files

These options concern the behaviour of the anti-virus when dealing with compressed files. More information about [here](#).

#### *Analyze compressed/packed files*

Tick the checkbox to enable the analysis of the content of compressed files.

#### *Maximal recursion level*

The Maximal recursion level within the compressed files.

#### *Control decompression size*

Tick the checkbox to activate the control of the size of decompressed files.

#### *Maximum decompression size*

The maximum size in kilobytes of decompressed files allowed for uncompressed items.

#### *Maximal nesting level*

The highest nesting level allowed for compressed files.

### File extensions

#### *White list extensions*



Upon ticking the checkbox, a textarea appears right underneath the option, in which to write a list of file extensions. Files ending with one of those extensions will pass through the anti-virus engine without being scanned.

#### *Blacklist extensions*

Upon ticking the checkbox, a textarea appears right underneath the option, in which to write a list of file extensions. Files ending with one of those extensions will be blocked by the anti-virus engine without being scanned.

## Time server

The Panda Gatedefender Appliance uses NTP to keep its system time synchronised with time servers on the Internet. The settings available are grouped into two boxes.

### **Use a network time server**

A number of time server hosts on the Internet are preconfigured and used by the system, but custom time servers can be specified after ticking the *Override default NTP servers* checkbox. This might prove necessary when running a setup that does not allow the Panda Gatedefender Appliance to reach the Internet. Several time servers addresses can be supplied, one per line, in the small form that will show up.

This box also shows the current time zone setting, that can also be changed by choosing a different one from the drop-down menu. An immediate synchronisation can be done by clicking on the *Synchronize now* button.

### **Adjust manually**

The second box gives the possibility to manually change the system time. While this is not recommended, this action proves useful when the system clock is way off and an immediate update of the Panda Gatedefender Appliance's clock to the correct time is needed.

Automatic synchronisation using time servers is not done instantly, but the clock is "slow down" or "speed up" a bit to recover and align to the correct time, hence a system with a significant error in its time may require a long period to be corrected. In those cases, forcing a manual synchronisation represents a more drastic but immediate solution.

## Mail Quarantine

The mail quarantine is a special place on the Panda Gatedefender Appliance hard disk where all the e-mails that the SMTP proxy recognises as containing spam, malware, viruses, or with suspicious attachments are stored instead of being delivered. Here, those e-mails can be safely analysed and actions can be taken to manage them. To activate the mail quarantine, go to Menubar › Proxy › SMTP › Configuration and in the SPAM settings, Virus Settings, and File settings boxes, choose the option "move to default quarantine location" from the drop down menus.

The mail quarantine page contains a table with the list of all mail moved to the quarantine, above which there is a navigation bar to browse the e-mails

The table contains the following information about the mail saved in the quarantine.

#### *Select*

A checkbox that allows to select one or more messages at a time and carry out an action on all of them.

#### *Reason*

The reason for which the e-mail's delivery has been blocked, which can be one of *Malware* - the e-mail contains viruses or other types of threats, *Spam* - the e-mail contains spam, *Banned* - the e-mail has an attachment that can not be sent, and *Bad Header* - the information contained in the header are not valid.

#### *Date*

The date and time when the e-mail was moved in the quarantine.

#### *Size*

The size of the e-mail.

#### *From*

The sender of the e-mail.





#### *Subject*

The subject of the e-mail.

#### *Attachment*

The number of the attachments to the e-mail.

#### Actions

The four icons present in this column represent the available actions:  View the message,  download the message,  release the message and delivery it to the original recipient, and  deletes the email. See below for more details.

Underneath the table, two buttons allow to carry out actions when more than one message is selected in the table.

#### Release

Releases the selected messages, scheduling them for immediate delivery.

#### Delete

Permanently removes the selected e-mails.

When clicking on the *view message* icon, the list of emails is replaced with a 3-boxed page, showing various details about the selected e-mail.

#### Quarantined Email

This box presents a more detailed view of the e-mail's data reported in the e-mail list: The reason why the e-mail ended in the quarantine, the sender and recipients, along with carbon copy (CC) addressee, subject, date and time of receipt, and e-mail's size.

#### Headers

The full, original header of the Email, which can give useful information, among which for example the path followed by the e-mail.

#### Payload

If the email has one or more attachments, they are shown here along with their details. Moreover, every HTML attachment is shown with its full source code.

At the bottom, there is an option available:

#### *Delete from Quarantine after release*

The e-mail will be removed from the quarantine after its release to the original recipient.

## Spam Training

The Panda Gatedefender Appliance includes SpamAssassin as the engine to find and fight spam e-mails. While it is successful in the vast majority of the cases, SpamAssassin needs to be trained to improve its abilities to intercept spam e-mails. The configuration of the training for the antispam engine can be done in this page: Indeed, SpamAssassin can learn automatically which e-mails are spam and which are not (the so called ham mails). To be able to learn, it needs to connect to an IMAP host and check the pre-defined folders for spam and ham messages.

The page for SpamAssassin consists of two boxes, one that contains a list of IMAP hosts used for learning, with the possibilities to manage them at various levels, and another one to modify the scheduling of the updates.

#### Current spam training sources

The first box allows the configuration of the training sources, by means of two links that, after clicking, will reveal two panels in which to specify the various configuration values. The default configuration, which is initially empty, is not used for training, but only provides values that are later inherited by the real training sources which can be added right below. By clicking on the *Edit default configuration* link, these settings can be configured:

#### *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 a folder that contains only ham messages. It can be, for example, a dedicated folder that stores only 'clean' messages, or even the Inbox.

#### *Default spam folder*

The name of a folder that contains only spam messages.

#### *Schedule an automatic spam filter training*

The time interval between two consecutive checks, which can either be disabled or be an hourly, daily, weekly, or monthly interval. The exact time scheduled is shown when moving the mouse cursor over the question marks. If disabled, the antispam engine must be manually trained.

Additional spam training sources can be added in the panel that appears upon clicking on the *Add IMAP spam training source* link. The options for the additional training hosts are the same as the default configuration options, except for the scheduling, which is always inherited from the default configuration, and for three new available options.

#### *Enabled*

The training source will be used whenever SpamAssassin is trained. If not enabled, the source will not be used during the automatic training, but only for manual ones.





#### *Remark*

A comment about this source.

#### *Delete processed mails*

Whether the e-mails should be deleted after they have been processed.

The other options can be defined just like in the default configuration and, when specified, they override the default values. To save the configuration of a source it is necessary to click on the *Add Training Source* button after all the desired values have been set. Several actions can be carried out on a training source:

-  - toggle the status of the IMAP host, enabled or disabled.
-  - modify the property of the IMAP host.
-  - remove the IMAP host.
-  - test the connection to the IMAP host.

It can be enabled, disabled, edited, removed, or the connection tested by clicking on the appropriate icon.

Two additional actions are available and will be performed on all the connections, by clicking on one of the buttons located on the top right of the box.

#### *Test all connections*

To check all the connections at once. This operation can take some time if many training sources have been defined or the connection to the IMAP servers is slow.

#### *Start training now*

Immediately starts the training. It is important to note that training can take a very long time, depending on many factors: The number of the sources, on the connection speed, and most importantly on the number of e-mails that will be downloaded.

#### Note

The antispam engine can be also trained in another way if the SMTP Proxy is enabled for incoming as well as for outgoing mails: This is done by sending spam mails to the special addresses *spam@spam.spam* and non-spam mails to *ham@ham.ham*. The hostnames *spam.spam* and *ham.ham* are added to the network configuration right after the network setup and are aliases for localhost. If these two addresses are not present, they can be added to the host configuration in Menubar › Network › Edit hosts › Add a host on the Panda Gatedefender Appliance.

#### **SpamAssassin Rule Update Schedule**


In this box it is possible to schedule the automatic download of SpamAssassin signatures among the four options: *Hourly*, *daily*, *weekly*, and *monthly*.

## Intrusion Prevention

The Panda Gatedefender Appliance includes the well known intrusion detection (IDS) and prevention (IPS) system *snort*, which is directly built into iptables, to intercept and drop connections from unwanted or distrusted sources.

The page contains three tabs, *Intrusion Prevention System*, *Rules*, and *Editor*.

## Intrusion Prevention System

If snort is not active, a grey switch  next to the *Enable Intrusion Prevention System* label appears on the page and can be clicked on to start the service. A message appears, informing that the service is being restarted and after a short interval, the box will contain some options to configure the service.

### *Automatically fetch SNORT Rules*

Ticking this box will let the Panda Gatedefender Appliance automatically download the snort rules from the Panda Perimetral Management Console.

#### Note

If the Panda Gatedefender Appliance is not registered, rules are downloaded from the Emerging Threats web page. An informative message is also shown at the bottom of the page.

### *Choose update schedule*







The frequency of download of the rules: A drop-down menu allows to choose one of the *hourly*, *daily*, *weekly*, or *monthly* options. This option appears only if the previous option has been activated.

### *Custom SNORT Rules*

A file containing custom SNORT rules that should be uploaded. Pick one file from the file selection window that opens upon clicking the *Browse* button, and upload it by clicking on the *Upload custom rules* button.

## Rules

On the *Rules* tab appears the list of rule sets that are stored on the Panda Gatedefender Appliance, along with the number of rules they contain and the actions that can be done on them:

-   - toggle the status of the rule set, enabled or disabled.
-   - The policy applied to packets, either they are allowed to pass or not.
-  - modify the property of the rule set.
-  - remove the rule set.

#### Note

When editing a ruleset in the *Rules* tab, the *Editor* page (see below) will open with that ruleset already selected.

All the actions, except for editing, can be carried out on more than one rulesets at once, by selecting them (tick the checkbox on the left of their filename) and pressing one of the button underneath the list.

By default, the policy for all the rulesets is set to *alert*. This behaviour can be changed by clicking on the alert icon to toggle the policy into *block* and the icon into a red shield. After clicking on the *Apply* button, that ruleset will not cause alerts anymore, but all the traffic that matches its rules will be blocked.

A ruleset can be deleted by clicking on the trash can icon, while a click on the pencil icon redirects to the *Editor* page in which to edit each rule independently.

## Editor

At the top of the *Editor* page are shown the rulesets that can be edited. To chose more than one ruleset at once, hold the **CTRL** key and click on the rulesets.

After selecting and clicking on the *Edit* button, the list of the rules included in the selected ruleset(s) is shown. The list can be narrowed down by entering some terms in the text box next to the *Search* label. Like in the *Rules* page, the policy of every entry can be changed.

#### Warning

Turning on the IPS only implies that snort is running, but it does not yet filter the traffic. For snort to filter packets, the *Allow with IPS* Filter policy must be selected for the rules defined in the various Firewall configuration pages.

## High availability

The Panda Gatedefender Appliance can be run in an HA mode, that can easily be setup using at least two Panda Gatedefender Appliances, one of which assumes the role of the active (i.e., master) firewall, while the remaining are standby (i.e., slave) firewalls.

If the master firewall fails, an election among the slaves takes place and one of them will become the new master, providing for transparent failover. If there is only one slave, though, it will immediately take over the master's duties and allows a seamless failover transition to the secondary Panda Gatedefender Appliance in the event of a hardware failure on the primary appliance. This provides unparalleled hardware availability and redundancy for critical network operations and security.

In order to start up the HA service, at least one master and one slave Panda Gatedefender Appliances must be configured according to the following guidelines.

### Note

The high availability module requires at least two completely identical Panda Gatedefender Appliances.

An important point to focus on when deploying high availability is that a duplication method for each and every connection to the Panda appliance must be provided. Every connection of the primary unit (e.g., WAN, LAN, etc.) must be replicated across the standby unit(s) to ensure that complete replication capabilities exist.

In this scenario, each network on the Panda Gatedefender Appliance (WAN, LAN, etc.) is connected to an external managed switch which has a unique VLAN assigned to each network. This deployment option consumes the least amount of network ports and provides for enhanced extensibility. Another option is to replace a single managed (VLAN capable) switch with smaller, separate switches for each network (WAN, LAN, etc.). This setup however may not be cost-effective and could be less reliable since the failure of any switch could break failover partially or completely.

### Warning

Since the HA runs automatically over the GREEN network, the heartbeat can be configured to run over the switch connection or alternatively, an additional Ethernet port can be assigned to the GREEN network to directly connect the master device to the slave unit. The advantage of adding a direct connection is that it removes the switch (and thus possible sources of problems, improving the overall reliability) from the failover equation. The decision on whether to implement this setup may largely depend on the overall reliability of the managed switch (dual power, port failure rate, warranty terms, etc.) – so the more reliable/redundant is the switch configuration, the less critical having a direct connection can become.

In this page, there is only one box, which initially contains only one option:

### *Enable High Availability*

Enable HA on the Panda Gatedefender Appliance, by default it is disabled.

After enabled, a second drop-down menu appears, *High Availability side*, that allows to configure the Panda Gatedefender Appliance as master or slave. Depending on this choice, different configuration options are available. Configuring a slave unit, however, requires that a Master unit have already been set up.

For the **master side**, the following options are available:

### *Management network*

The special subnet to which all Panda Gatedefender Appliance that are part of a same HA setup must be connected and defaults to `192.168.177.0/24`. Unless this subnet is already used for other purposes, there is no need to change it.

### *Master IP Address*

The first IP address of the management network. It is automatically set to 1 on the network chosen, and defaults to `192.168.177.1`.

*Notification: recipient email address, Notification: sender email address, Notification: email subject, Notification: SMTP server to be used*

These options can be filled in to be notified by e-mail when a failover event occurs. They are configured the same way as they were configured for other event notifications in Menubar > System > Event notification: A custom sender, recipient, and subject of the email and the SMTP smarthost used to send the email.

### *Enable STP*

Choose from the drop-down menu whether to enable or not the spanning tree protocol, STP. This option and the next one are important when the Panda Gatedefender Appliance is in gateway mode.

### *STP Bridge Priority*

The priority of the bridge. It must be 1 on the master side.

A second box will appear after HA has been activated, with the list of the slaves with their IP address, a link to access their management GUI, and the possibility to delete a slave.

The HA management network.

The Panda Gatedefender Appliance uses a special network to connect the master to slave unit(s): 192.168.177.0/24. If this network has already been used in other zones, none of the already defined network(s) is deleted nor any change should be made to them. Indeed, in such a case, simply assign to the HA management network a different range of IP addresses, like, e.g., 172.19.253.0/24 or 10.123.234.0/28. It is important to note that the only requirement of the management network is that it must be large enough to accommodate the master and all the slaves, so if there are only a master and a slave devices, even a network as small as 192.168.177.0/29 should suffice. The management network will be created as an interface on the GREEN network, and it will show up on the device or when viewing the network status.

### *Warning*

Make sure that the management network can be reached from the current LAN setup, or it will not be possible to login to the master unit!

After the master unit has been configured, the second Panda Gatedefender Appliance, that is going to be the slave, can be set up. The same procedure shall be followed for every additional slave to configure.

### *Warning*

It is strongly suggested to make a backup of the slave unit before configuring it and saving it on a safe place, since it may become useful to restore a slave unit after it is removed from its role.

For the **slave side** the following are the available options.

### *Master IP address*

The IP address of the master unit, which defaults to 192.168.177.1/24 if the management network had not been changed. This value **must** match the one that appears as value of the *Master IP Address* option on the master unit.

### *Master root password*

The password of the console *root* user (**not** the graphic administration interface!) on the master.

These data will be used by the slave to retrieve from the master all the information needed and to keep the synchronisation.

### *Enable STP*

Choose from the drop-down menu whether to enable or not the spanning tree protocol, STP. On the slave side, this option must have the same value as in the master side.

### *STP Bridge Priority*

The priority of the bridge. On the slave side, it must be a digit or number higher than the one on the master side.

Upon saving the setup, the connection to the device will be temporarily lost, since the management network is created and then the two devices (the master and the currently defined slave) begin to synchronise.

After the synchronisation process is complete, the slave itself cannot be reached anymore via its old IP address (be it its factory default or its previous GREENIP address), since it has gone in standby mode and is connected to the master only through the management network. Any change made on the primary unit (the activation of a service, the change of one setting, the deletion of a VPN user, and so on) will automatically be synced to the slave unit(s) with the exception of updates, upgrades, or device backups (these have to be performed manually on the slave unit).

Moreover, the slave Panda unit will automatically appear on the master's list of slaves and switch to an informational-only web interface that can be accessed from the master, by following the *Go to Management GUI* link next to each of the entries of the list of slaves.

### *The RED MAC Address*

During the HA failover, the RED interface MAC address is not replicated onto the slave unit. This can represent a problem if the ISP requires to use the *Sticky IP* setup. In this situation, the IP address assigned from the ISP is determined from the MAC address of the client's network interface, similarly to a fixed IP assigned from a DHCP server to a client. It may not be possible to reconnect with the slave unit. To avoid this situation, it is necessary to utilise the spoofed MAC address feature on the RED interface in order for HA to work properly. This will ensure that when the HA is activated the MAC address will carry over to the standby unit and will not require manual intervention. This can be achieved on the slave, before activating it, by ticking the option *Use custom MAC address* under Menubar > Network > Interfaces > Edit main uplink > Advanced settings and specifying the MAC address of the RED interface on the Master. Alternatively, the MAC address can be entered in the step 4 of the network installation wizard, writing the master's MAC address in the *Spoof MAC address with* option.

## Traffic Monitoring

Traffic monitoring is done by ntopng and can be enabled or disabled by clicking on the main switch on this page. Once traffic monitoring is enabled a link to its new *administration interface* appears in the lower section of the page. The traffic can be visualised and analysed by host, protocol, local network interface and many other types of information: All these operations can be carried out directly from the Traffic Monitoring module in The Logs and Reports Menu.

## SNMP Server

The SNMP is used to monitor network-attached devices, and can be used e.g., to control the status of the internal infrastructure.

To enable the SNMP Server is sufficient to click on the grey switch next to the *Enable SNMP server* label: Once done so, a few options will appear in the *Settings* box.

### *Community String*

A key that is needed to read the data with an SNMP client.

### *Location*

An identification string that can be set to anything, but it is suggested that it describe the location of the Panda Gatedefender Appliance.

### *Override global notification email address*

The SNMP Server requires to configure an e-mail address as the system contact, and the global e-mail address provided during the installation procedure is used by default. Nonetheless, to use a custom e-mail address, tick the checkbox and supply it into the *System contact email address* field that will activate right below.

## Quality of Service

The purpose of the QoS module is to prioritise the IP traffic that is flowing through the Panda Gatedefender Appliance depending on the service. In other words, the QoS is a convenient way to reserve a given amount of the available bandwidth (both incoming and outgoing) for a given service. Applications that typically need to be prioritised over bulk traffic are interactive services such as SSH or VoIP.

The QoS configuration options are arranged into three tabs: *Devices*, *Classes*, and *Rules*.

### Devices

The *Device* tab is also the starting page for the QoS and is initially empty. Once populated, a table showing a list of all the Quality of Service devices appears and for each device, some parameters and the available actions are displayed.

New QoS devices can be added by clicking on the *Add Quality of Service Device* link above the list and by configuring a few options.

### *Target Device*

The network interface that will be used by this device. Choices are among the network interfaces or zones enabled on the system and can be selected from a drop-down menu.

### *Downstream Bandwidth (kbit/s)*

The downstream speed of the interface.




### *Upstream Bandwidth (kbit/s)*

The upstream speed of the interface.

### *Enabled*

Enable the QoS (default) or not.

The actions available on the devices are:

-  - enable or disable the device.
-  - modify the properties of the device.
-  - remove the device.

When editing a device, the same form opens as when adding a new device, in which to modify the current device's parameters.

For every device added, four items will appear under the *Classes* tab: Three for high, medium, and low priority, respectively, and one for bulk traffic (see below).

## Classes

This tab shows a list of all Quality of Service classes that have been created, if any. For each entry, several data are shown. New items can be added by clicking on the *Add Quality of Service Class* link above the list of classes. The parameters to configure are the same shown in the list:

### *Name*

The name of the Quality of Service class.

### *QOS Device*

The drop down menu allows to choose the Quality of Service device for which the class was created.

### *Hint*

at least one QoS device must have been created before defining a QoS class.

### *Reserved*

The percentage of bandwidth that has been reserved for this class from the device's overall available bandwidth.

### *Limit*

The maximum percentage of bandwidth this class may use.

### *Priority*

The priority of the class, from 0 (low) to 10 (high), selected from a dropdown menu

### *Note*

The sum of reserved percentages can not be greater than 100 per device. Moreover, the *reserved* bandwidth can not be higher than the *limit* bandwidth.

The actions available are: \*  - modify the properties of the device. \*  - move the class in the list. \*  - remove the device.

Classes can be moved up or down the list: Items closer to the top of the list are the first to be processed when the bandwidth does not suffice for all the traffic and the Panda Gatedefender Appliance needs to choose which traffic should be prioritised.

## Rules

The third tab displays a list of the already defined Quality of Service Rules and allows to specify which type of traffic should belong to each of the classes. To add a new Quality of Service rule click on the *Add Quality of Service Rule* link. In the form that will open, which is very similar to the one used to define firewall rules, several values should be configured. Many drop-down menus are employed here to ease the choices and guide through the configuration.

### *Source*

Choose from the drop-down menu the traffic source, either a Zone or interface, a network, an IP or MAC address. Depending on this choice, different values can be specified: A zone or interface from the available ones from those that will be displayed, or one or more IP addresses, networks, or MAC addresses.

### *Destination Device/Traffic Class*

Choose the device/class from the drop-down menu and then the destination IP addresses or networks, to be written in the text-area on the right-hand side.

### *Service/Port, Protocol*

The next two drop-down menus are used to define the service, protocol, and a destination port for the rule (when choosing one of TCP, UDP, or TCP + UDP protocols). Some predefined combinations Service/Protocol/Port exists, like HTTP/TCP/80,



<ALL>/TCP+UDP/0:65535, or <ANY>, which is a shortcut for all services, protocols, and ports. Finally, in the *Destination port*, one or more custom port number can be supplied (this proves useful when some service does not run on a standard port).

#### *TOS/DSCP*

The type of TOS or DSCP value to match.

#### *Match Traffic*

Choosing *TOS* or *DSCP class* in the previous drop-down menu allows to choose a suitable value for the traffic to match from another drop-down menu. Otherwise, the choice *DSCP Value* allows to enter a custom value that should match the rule.

#### *Enabled*

Tick the checkbox to enable the rule.





#### *Comment*

A comment to identify the rule.

#### **Note**

If there is more than one service in a Quality of Service class, then all these services together will share the reserved bandwidth.

The actions available on the rules are:

-   - enable or disable the rule.
-  - modify the properties of the rule.
-  - remove the rule.



# 6. The Firewall Menu

---

This section allows to set up rules that specify if and how the network traffic flows through the Panda Gatedefender Appliance. The firewall on the Panda Gatedefender Appliance is divided in different modules, each monitoring and allowing or blocking one specific type of traffic. The modules available are the following:

- Port forwarding / NAT - port forwarding and abbr:*NAT (Network Address Translation)*.
- Outgoing traffic - outgoing traffic, i.e., towards the RED interface
- Inter-Zone traffic - traffic between zones.
- VPN traffic - traffic generated by VPN users.
- System access - grant access to the Panda Gatedefender Appliance host itself.
- Firewall diagrams - pictures that show which traffic is intercepted by each type of firewall.

Within each of the sub-menus, in which all the corresponding existing rules are listed, any customised rules can be added, for any type of service or every port/protocol. The various parts of which the firewall is composed refer to different types of traffic (e.g., OpenVPN governs the traffic from/to the VPN users, inter-zone traffic the one flowing from zone to zone) and are designed to avoid any overlapping or even contrasting rules. In other words, there is no way to write two rules in two different firewall modules whose combined effect causes an unwanted block or access of packets.

The choice to separate the networks controlled by the Panda Gatedefender Appliance allows also for an easier management of the firewall, whose configuration may become very complex. Indeed, each of the modules can be considered as an independent firewall, and their combined effect covers all possible packet flows through the Panda Gatedefender Appliance.

Additionally, for any of the modules listed above, one or more rule may exist, that can neither be disabled nor removed. These are the so-called *Rules of system services* (or *System rules*) whose purpose is to allow the correct interoperability of the services running on the Panda Gatedefender Appliance with the Panda Perimetral Management Console infrastructure.

The rules that are defined here will be transformed into **iptables** commands, the standard Linux firewall tool since the 2.4 kernel, and therefore organised into tables, chains, and rules. For a more in-depth description of the various elements that compose a firewall rule, or even to learn how to fine-tune and to manage a complex firewall, it is suggested to read either the *iptables(8)* manual page on any Linux box, or some of the countless online resources or tutorials available on the Internet.

## Common configuration items

When adding a rule, most of the values to configure in the various modules are of the same type (e.g., the source or destination interfaces), since in the end they are all setup with **iptables**. Therefore, in order to keep this section short and readable, all the configuration items that are common to all modules of the firewall are grouped here and defined only once. There will be some more explanation only in case of significant differences with the descriptions given here.

- *Source or Incoming IP*. Usually in the form of a drop-down menu, this setting is the type of the source or incoming connection that should be matched. Depending on the type chosen, the selection of different connections from the small box underneath the menu will be possible: *Zone/VPN/Uplink* is either the source zone, VPN client, or uplink to which this rule should be applied, *Network/IP/Range* the IP address or range or the network addresses, *OpenVPN User* and *L2TP User* the OpenVPN or 2TP users, respectively.
- *Destination or Target*. Also this setting comes in the form of a drop-down menu and allows the choice among three types of destination that should be matched, which are the same as in the *Source* drop-down menu: *A Zone/VPN/Uplink*, *Network/IP*, *OpenVPN User* or *L2TP user*, except for some small change (e.g., for some type of rules, the target can not be an OpenVPN or L2TP user).
- *Service, Port, and Protocol*. A service is usually defined as a combination of a port and a protocol. For example, the SSH service runs by default on port 22 and uses the TCP protocol. These three options control the port and protocol to which to apply the rule and consist of two drop-down menus, from which to choose either a pre-defined *Service*, that will also set the protocol and the port range in the text area, or one *Protocol* and optionally a port or a port range. Available protocols are: TCP and UDP - the most used, GRE - used by tunnels, ESP - used by IPsec, and ICMP - used by the **ping** and **traceroute** commands.

### Note


There exist dozens predefined services that can be chosen from the drop down menus and should suffice to allow the most common services to access the Internet. An user defined combination of port and protocol should be used only if a service is

not running on a standard port (e.g., an SSH server listens to port 2345 or a web server runs on port 7981) or if a service is using a particular port (e.g., a multiplayer game on the Internet).

- *'Access from' sub-rule.* Almost every rule can be further detailed by adding several *Access from* rules to it, for example to limit access to a client depending on the zone from which it connects to the Panda Gatedefender Appliance. *Access from* rules can be configured when the advanced mode is selected (see below). As a consequence, a rule can appear split on two or more lines, depending on the number of access policies defined. Each *access from* sub-rule can be deleted individually, without changing the main rule. Each of the sub-rules can even have a different filter policy.
- *Policy, Filter Policy.* The action to carry out on the packets that match the current rule. The drop-down menu allows to select among four options: *Allow with IPS* -let the packet pass but analyse it with the Intrusion Prevention System, *Allow* - let the packets pass without any check, *Drop* - discard the packet, and *Reject* - discard the packet and send an error packet in response.
- *Enabled.* Every rule created is by default enabled, but it can be saved and not activated by unticking the checkbox, i.e., it will not be taken into account for packet filtering. Disabling a rule may prove useful for troubleshooting connections' problems.
- *Log, Log all accepted packets.* By default, no log entries is written when traffic is filtered. To enable logging for a rule, tick the box.




#### Warning

If there is a lot of traffic and packets to be analysed, the size of the log files will likely grow rapidly, so in this case remember to check the log directory regularly to avoid running out of space!

- *Remark.* A description or a remark about the rule, to remember the purpose of the rule.
- *Position.* Recall that the **iptables** rules are processed in the order they appear on the list and that some is a "terminating" rule, i.e., it may drop or reject a packet and stop the processing of the subsequent rules. This drop-down menu allows to choose in which position this rule should be saved.
- *Actions.* On all rules several actions can be carried out:
  -  - move the rule upwards or downwards in the list.

#### Hint

Remember that the ordering matters! The firewall rules are processed in the order they appear in the page, top to bottom.

-  - enable or disable the rule.
-  - modify the rule.
-  - remove the rule.

Finally, after every change has been saved in the firewall rules, the firewall should be restarted to reload the configuration. A clickable *Apply* button will appear to recall this necessity.

## Port forwarding / NAT

The Port forwarding / NAT module is composed by three tabs: Port forwarding / DNAT, Source NAT, and Incoming routed traffic. Its purpose is to manage all the traffic that flows through the uplink, from the RED zone to the Panda Gatedefender Appliance and the NAT-ed traffic, both incoming and outgoing.

## Port forwarding / Destination NAT

Destination NAT is usually employed to limit network accesses from an untrusted network or to redirect the traffic coming from the untrusted network and directed to a given port or address-port combination. It is possible to define which port on which interface should be forwarded to which host and port.

The list of the configured rules shows several information: The ID (#) showing the order in which the rules are matched against the traffic, the *Incoming IP* address, the *service* (i.e., port and protocol) to which the traffic is directed, the *Policy* applied to the traffic, the *Translate to* address (i.e., the host and port where to redirect the traffic), a custom *Remark*, and the available *Actions*.

When editing a rule, the same form open as when adding a new rule, by clicking on the *Add a new Port forwarding / Destination NAT rule*. A link on the top right of the form allows to chose between a *Simple mode* or an *Advanced mode*. The latter mode allows also to fine-tune the *Access from*, the policy, and the type of *Translate to*.

Besides the [common options](#), these other settings can be configured:

### Translate to

This part of the form changes depending on the current active editing *mode*, simple or advanced. If the mode is set to *advanced*, besides adding *Access from* sub-rules, there is an additional *Type* drop-down menu that allows to chose among different types of translations.

1. The first one is *IP* and corresponds to the only one available in *simple mode*. Here should be written the destination IP address (besides port and NAT), the port or port range to forward to and if to apply NAT or not to the incoming packets.
2. *OpenVPN User*: choose one OpenVPN user as the destination target for the traffic.
3. *Load Balancing*: specify a range of IP addresses to which traffic will be split, to avoid bottlenecks or the overloading of a single IP.
4. *Map the network*. Insert a sub-network to which translate the incoming traffic

#### Note

The Map network translation statically maps a whole network of addresses onto another network of addresses. This can be useful for companies whose subsidiaries all use the same internal network. Indeed, in this case all these networks can be connected to each other through network mapping.

An example would be:

```
original network 1: 192.168.0.0/24
mapped   network 1: 192.168.1.0/24
original network 2: 192.168.0.0/24
mapped   network 2: 192.168.2.0/24
```

5. *L2TP User*: choose one L2TP user as the destination target for the traffic.

Except when selecting the *Map the network* option, it is always possible to define the port or port range to which the traffic should be sent to, and if to apply NAT on the traffic or not. If *Do not NAT* is chosen, it is not allowed to define a *Filter policy* under the *Access From* (advanced mode).

#### Warning

When selecting *IP*, *OpenVPN User*, *L2TP User* or *Load balancing*, keep in mind that port ranges will not be mapped 1 to 1, but rather a round robin balancing is performed. For example, mapping incoming ports 137:139 to destination ports 137:139 will result in these ports being used randomly: The incoming traffic to port 138 can unpredictably be redirect to either 137, 138, or 139. Leave the translation *Port/Range* field empty to avoid such occurrences!

### Troubleshooting port-forwarding.

There are mainly two reasons why port-forwarding may not work.

1. The Panda Gatedefender Appliance is behind a NAT device.

In this case there is a device like a router or like another firewall between the Panda Gatedefender Appliance and the Internet, which disallows direct incoming connections. The solution is to configure a port forwarding also on that device to the RED IP of the Panda Gatedefender Appliance, if this is possible.

2. The destination server has wrong default gateway.

The server set as the destination of a port-forwarding rule is configured with a wrong or no default gateway. Connections will be directed to the target IP address but due to a wrong default gateway, packets will not be directed through the Panda Gatedefender Appliance. The solution is to correct the server's gateway.

## Source NAT

In this page can be defined rules that apply SNAT to outgoing connections. The list of already defined rules is also displayed, for each of which the source and destination IP addresses, the service, the NAT status, a custom description of the rule, and the available actions are shown.

Source NAT can be useful if a server behind the Panda Gatedefender Appliance has an own external IP and the outgoing packets should therefore not use the RED IP address of the firewall, but the one of the server. To add a new rule, click on *Add a new source NAT rule* and proceed like in the case of adding a port forwarding rule. Besides the [common options](#), only one other setting can be configured:

### NAT

Select to either apply *NAT*, *No NAT*, or *Map Network*. The choice to use SNAT allows the selection of the IP address that should be used among those presented in the drop-down menu. The *Auto* entries will automatically choose the IP address corresponding to the outgoing interface.

SNAT and a SMTP server in the orange zone.

In certain cases it is preferable to explicitly declare that *no Source NAT* be performed. An example would be a SMTP server in the DMZ, configured with an external IP, but whose outgoing connections should have the REDIP as the source. Configuring an SMTP server running on the IP 123.123.123.123 (assuming that 123.123.123.123 is an additional IP address of the uplink) in the DMZ with Source NAT can be done as follows:

1. Configure the ORANGE zone with any subnet (e.g., 192.168.100.0).
2. Setup the SMTP server to listen on port 25 on an IP in the ORANGE zone (e.g., 129.168.100.13).
3. In the Menubar › Network › Interfaces section, add a static Ethernet uplink with IP 123.123.123.123 to the Panda Gatedefender Appliance.
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 NAT-ed source IP address to 123.123.123.123.

## Incoming routed traffic

This tab allows to redirect traffic that has been routed through the Panda Gatedefender Appliance. This is very useful when having more than one external IP addresses and some of them should be used in the DMZ without the necessity to use NAT. The fields shown for every rule in the list are the traffic source and destination, the service, the policy to apply, a remark, and the available actions.

No other setting can be configured besides the [common options](#).

## Outgoing traffic

The Panda Gatedefender Appliance comes with a pre-configured set of rules for outgoing traffic, i.e., to allow traffic flow of specific services, ports, and applications from the various zones to the RED interface and therefore the Internet. These rules are needed to ensure that the most common services always be able to access the Internet and work correctly. Two boxes are present on this page, one that shows the current rules and allows to add new ones, and one that allows to set the outgoing firewall options.

### Note

Rules defined in the outgoing firewall are disregarded when the Panda Gatedefender Appliance is in *no uplink* mode. When operating in *Stealth uplink* mode, only part of the traffic from the zone behind the Panda Gatedefender Appliance to the outside is considered as outgoing, see the description of the stealth uplink.

Panda Gatedefender Appliance and Application Firewall (Application Control).

Application firewalls are a recent development and improvement to stateful firewalls, that combine the ability of the latter to keep track of the connection's origin and path with those of Intrusion Prevention Systems to inspect packets' content, with the purpose to provide higher security from worm, viruses, malware, and all types of threats. The final result from the user experience point-of-view is that firewalls can block not only traffic between ports and IP addresses, but also traffic generated by single applications. This requires however, more efforts from the firewall: While traffic between IP addresses only needs that the first packet be inspected to block or allow

the whole flow, to correctly recognise traffic generated by application, it is sometimes necessary the analysis of a few packets -usually not more than 3- of the flow.

Starting with version 5.50, every Panda Gatedefender Appliance is equipped with [nDPI](#), an open source library implementing Deep Packet Inspection, thus allowing the deployment of rules for application firewalling. nDPI is deployed as a kernel module and interacts with iptables for the packet analysis.

Hence, there are now two different types of rules that can be defined on the outgoing firewall:

- *Stateful* firewall rules, that filter traffic between IP addresses and ports.
- *Application Rules*, i.e., rules that filter traffic generated by application.

When no application rules have been defined, the behaviour of the firewall is exactly the same as in previous version. Whenever an application rule has been defined, however, the stateful rules preceding it behave normally, while all the rules after undergo nDPI.

It is worth noting that the use of nDPI might present some subtleties, illustrated by the following example, and therefore might produce some unwanted side effect.

Suppose that a company wants to allow all HTTP traffic, except for youtube and gmail. The first default rule defined in Panda Gatedefender Appliance is to allow all HTTP traffic, with no restriction. This rule must therefore be disabled as first step. Then, two rules must be defined:

1. an application rule blocking the gmail and youtube protocols
2. a stateful rule allowing all http traffic.

If rule 2. were an application rule with protocol HTTP, then only traffic recognised as HTTP by nDPI would be allowed, but other protocols using HTTP, like e.g., Yahoo and FaceBook would pass, since nDPI does not consider them as being HTTP, but independent protocols.

#### **Current rules**

In detail, these are the services and protocols allowed by default to access the REDIP from the zones and shown in the top box:

GREEN: HTTP, HTTPS, FTP, SMTP, POP, IMAP, POP3s, IMAPs, DNS, ICMP

BLUE: HTTP, HTTPS, DNS, ICMP

ORANGE: DNS, ICMP

Everything else is forbidden by default except for the *System rules* which allow access to the services in the Panda Perimetral Management Console. The system rules are defined even if the corresponding zones are not enabled.

Possible actions on each rule are to enable or disable it, to edit it or delete it. Additional rules can be added by clicking on the *Add a new firewall rule* link at the top of the page. Please remember that the order of rules is important: the first matching rule decides whether a packet is allowed or denied, regardless of how many matching rules follow. The order of the rules can be changed by using the up and down arrow icons next to each rule.

The following settings differ from the default [common options](#).

#### *Source*

It can be one or more Zone/Interfaces, Network/IP, or MAC addresses.

#### *Destination*

Can be the RED zone, one or more uplinks, or one or more network/host addresses accessible outside the RED interface.

#### *Application*

This search widget allows to select the applications that should be part of the rule. Applications are dividend into categories (e.g., Database, filesharing, and so on).

Hint

Enter at least one letter to show all applications whose name starts with that letter.

#### **Outgoing Firewall Settings**

It is possible to disable or enable the whole outgoing firewall by clicking on the *Enable Outgoing firewall* switch. When disabled, all outgoing traffic is allowed and no packet is filtered: This setting is however strongly discouraged and the recommendation is to keep the outgoing firewall enabled.

#### *Log accepted outgoing connections*




Ticking this checkbox causes all the accepted connections to the RED interface to be logged.

Proxy and outgoing firewall.

Whenever the proxy is activated for a given service (e.g., HTTP, POP, SMTP, DNS), the firewall rules in the outgoing firewall will take no effect, because of the nature of the proxy.

With the proxy activated, whenever a connection starts from a client to the Internet, it will either be intercepted by the proxy on the Panda Gatedefender Appliance (in transparent mode) or go directly to the firewall, but never go *through* the firewall. The proxy then starts a new connection to the real destination, gets the data and sends it to the client. Those connections to the Internet always start from the Panda Gatedefender Appliance, which hides the clients internal IP address. Therefore, such connections never go through the outgoing firewall, since in fact they are local connections.

## Inter-Zone traffic

This module permits to set up rules that determine how traffic can flow between the local network zones, excluding therefore the RED zone (traffic through the RED zone can be filtered in [Outgoing traffic](#) and [Port forwarding / NAT](#)). To activate the inter-zone firewall, click on the grey switch . Two boxes are present on this page, one that shows the current rules and allow to add new ones, and one that allows to set the inter-zone firewall options.

Note

When the Panda Gatedefender Appliance is configured in *no uplink* mode, all the network traffic shall be filtered using the interzone firewall. Also when in *Stealth uplink mode* with more than one zone defined, all the traffic not routed through the gateway is filtered with the interzone firewall. See ref:*the stealth uplink description <stealth>* for more information.

### Current rules

The Panda Gatedefender Appliance comes with a simple set of pre-configured rules: traffic is allowed from the GREEN zone to any other zone (ORANGE and BLUE) and within each zone, with everything else forbidden by default.

Analogously to the outgoing traffic firewall, rules can be disabled/enabled, edited or deleted by clicking on the appropriate icon on the right side of the table. New rules can be added by clicking on the *Add a new inter-zone firewall rule* link at the top of the page. Only the [common options](#) can be configured.

### Inter-Zone Firewall Settings

The inter-zone firewall can be disabled or enabled by using the *Enable Inter-Zone firewall* switch. When disabled, all traffic is allowed among all the BLUE, GREEN, and ORANGE zones. Disabling the inter-zone firewall is strongly discouraged.

#### *Log accepted Inter-Zone connections*

Ticking this checkbox causes all the accepted connections among the zones to be logged.

## VPN traffic

The VPN traffic firewall allows to add firewall rules applied to the users and hosts that are connected via OpenVPN.

The VPN traffic firewall is normally not active, which means that, on the one side, the traffic can freely flow between the VPN hosts and the hosts in the GREEN zone, and on the other side, 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. Two boxes are present on this page, one that shows the current rules and allow to add new ones, and one that allows to set the VPN firewall options.

### Current rules

The handling and definition of the rules is identical to the outgoing traffic firewall, so please refer to that section and to the [common options](#) for directions on the definition and handling of the firewall rules in this module.

### VPN Firewall settings

The VPN firewall can be disabled or enabled using the *Enable VPN firewall* switch.

#### *Log accepted VPN connections*

Ticking this checkbox causes all the accepted connections from the VPN users to be logged.

## System access

This section governs the rules that grant or deny access to the Panda Gatedefender Appliance itself.

There is a list of pre-configured rules that cannot be changed, whose purpose is to guarantee the proper working of the firewall. Indeed, there are services, among those supplied by the Panda Gatedefender Appliance, that require to be accessed from clients in the various local zones. Examples include using the DNS (which requires that the port 53 be open) to resolve remote hostnames or using the administration web interfaces (which uses port 10443): Whenever one of these services is activated, one or more rules are automatically created to allow the proper efficiency of the service itself.

The list of the pre-defined rules is shown when clicking on the *Show rules of system services* button at the bottom of the page.

More system access rules can be added by clicking on the *Add a new system access rule* link. The setting specific to this module of the firewall are:

### *Log packets*

All packets that access or try to access the Panda Gatedefender Appliance are logged when this checkbox is ticked. This option proves useful to know who accessed -or tried to access- the system.

### *Source address*

The MAC addresses of the incoming connection.

### *Source interface*

The interface from which the system can be accessed

### Note

There is no *Destination* address, as it is the IP address of the interface from which the access is granted or attempted.

Actions are to disable/enable, edit, or delete a rule from the list of rules.

## Firewall Diagrams

This page shows, for each of the modules described in this page, a diagram that shows how the traffic flows among the zones, and which is the firewall module that takes charge of the various flows. The green arrowed lines show which traffic is allowed in each zone and in which directions. In the case of VPN, the arrows from/to the RED interface are marked with a red 'X', meaning that the traffic is not possible between them.

When an image is clicked, it will be opened into a gallery that allows to browse all of them like in a slide show.

# 7. The Proxy Menu

---

To improve on-line security, the Panda Gatedefender Appliance offers several services combining their abilities with those of the proxy. The sub-menu on the left-hand side of the page grants access to their configuration pages and options, which are summarised as follows:

- HTTP - the web proxy: access policies, authentication, content filter, and antivirus
- POP3 - the proxy for retrieving mail: spam filter and antivirus
- FTP - files downloaded via FTP: anti-virus
- SMTP - the proxy for sending or retrieving mail: spam filter and antivirus
- DNS - the caching DNS: anti-spyware

Each proxy service can be configured and enabled/disabled independently of the other, and will also start any other service required for its proper functioning. For example, when the SMTP proxy is configured and started, also the SMTP service will be started if it is not already running. Therefore, it is required that the SMTP service be configured before using the SMTP proxy.

In version 5.50, the whole proxy architecture has changed.

The old and new HTTP proxy architecture

In the release 5.50 of the Panda Gatedefender Appliance, a lighter, but more powerful architecture for the HTTP proxy has been implemented and deployed.

The previous HTTP proxy architecture was based on the so called *proxy chaining*, that is, whenever a client requested a remote resource, that had not been cached before, a 5 step process took place:

1. The HTTP proxy -squid- sent a GET request to the server, receiving an HTML page as answer.
2. The whole HTML page was sent to the content filtering daemon -dansguardian- and analysed.
3. Dansguardian then sent the page to the antivirus daemon -havg- and analysed for virus and other malware.
4. Finally, if no virus or malicious content was found, the whole HTML page was sent back to squid, otherwise an HTML error message ("*error page*") would have replaced the original page.
5. squid saved the HTML page (or the error page) for future requests, and delivered it the client that originally requested the HTML page.

The major drawback -and bottleneck- of this architecture is its resource intensiveness. The whole HTML page, indeed, sequentially moved through the whole chain, step by step with no possibility to speed up the process. The HTML page was received from squid and sent to dansguardian to be analysed for content. At this point, even if the content filter found malicious content, meaning that the page could not be served to the client requesting it, the HTML page continued to go down the chain to the havg, then back to squid. Only at this point squid sent an error page to the original client.

Therefore, it was decided to tackle this problem differently, adopting an entirely new approach that ensures more reliability and is far less resource consuming. The HTTP proxy is now backed up by an *ICAP* server and, while this might at a first sight represent a more complex architecture, it represents a significant performance improvement.

In a nutshell ICAP is a protocol, defined in [RFC 3507](#), that allows to manipulate the content of a web page and serve it back to the client. While this ability can be exploited in several ways, in Panda Gatedefender Appliance it is deployed with [c-icap](#), to provide content filtering analysis and anti-virus scan of remote resources (HTML pages, but also audio, video, and text documents, images).

Thanks to c-icap, there are two areas whose performances were boosted:

1. From squid to c-icap:  
  
c-icap receives two parallel request from the HTTP proxy
2. between cicap and the daemons.




See also

More information about ICAP along with its specifications can be found on the [icap forum](#) web page.

## HTTP

The HTTP proxy employed in the Panda Gatedefender Appliance is [squid](#), whose primary ability is to cache web requests to speed up future requests of the same page, though it has many more functionalities that allows its seamless integration with the other services described in the remainder of this section. The HTTP proxy settings page is composed of six tabs that organise a myriad of options: *Configuration, Access Policy, Authentication, Web Filter, AD join, and HTTPS Proxy.*

### Configuration

A click on the *Enable HTTP Proxy* switch  enables the HTTP proxy. After some seconds, necessary to start all required services, a number of controls appear in the *Configuration* tab, grouped into six panels: Each panel has a title, followed by a ? that shows a tooltip, and can be expanded or collapsed by clicking on the  or  icons located on the left of the labels.

The first setting is to select from a drop-down menu how the users in each enabled zone -GREEN, ORANGE, BLUE- can access the proxy (No drop-down menu is available for non-enabled zones):

#### *not transparent*

The proxy server is available to anyone with no need to log in, but the clients need to configure their browser manually or tell the browser to search for a proxy (i.e., using either PAC or the WPAD protocol to set up the browser's proxy settings).

#### *transparent*

The proxy server is available to anyone and no browser configuration is needed: All the HTTP traffic is intercepted and forwarded to the proxy server, that is in charge of retrieving the requested web pages and serve them to the clients.

#### Note

Some browsers, including Internet Explorer and Firefox, are able to automatically detect proxy servers by using the WPAD. Most browsers also support PAC, through a special URL. When using an Panda Gatedefender Appliance as the proxy server, the URL looks like this: `http://<GREENIP>/proxy.pac`.

#### Disabling HTTP proxy per zone

To disable completely the proxy for a certain zone, the zone's proxy must be set to transparent and the zone's subnet (whose value can be found in Menubar > Services > DHCP server) must be added to the *Bypass transparent proxy from SUBNET/IP/MAC* field that shows up when expanding the *Bypass transparent proxy* panel.

#### Proxy settings

In the *Proxy settings* panel there are some global configuration options for the proxy services:

##### *Port used by proxy*

The TCP port on which the proxy server is listening for connections, which defaults to 8080.

##### *Error Language*

The language in which error messages are displayed, which defaults to the one chosen in Menubar > System > GUI settings.

##### *Visible Hostname used by proxy*

The hostname assumed by the proxy server, also reported at the bottom of error messages.

##### *Email used for notification (cache admin)*

The email address shown by the proxy server in error messages.

##### *Maximum download size (incoming in KB)*

The limit for HTTP file downloads. 0 means unlimited.

##### *Maximum upload size (outgoing in KB)*

The limit for HTTP file uploads (e.g., those used by HTML forms with file uploads). 0 means unlimited.

#### Allowed ports and ssl ports

Configuration option for the ports the clients are allowed to use when browsing:

##### *Allowed Ports (from client)*

The TCP destination ports to which the proxy server will accept connections when using HTTP. One port or one port range per line are accepted, comments are allowed and start with a #.

#### *Allowed SSL Ports (from client)*

The TCP destination ports to which the proxy server will accept connections when using HTTPS. One port or port range per line are accepted, comments are allowed and start with a #, ending at the end of the line.

#### **Log settings**

Configuration option to enable the logging facility and choosing what to log.

#### *HTTP proxy logging*

Log all the URLs being accessed through the proxy. It is a master switch, hence the following four options are enabled and can be configured only if logging is enabled, which is not by default (recall that the more is logged, the more space on the Panda GateDefender Appliance's hard disk is needed).

#### *Query term logging*

Log the parameters in the URL (such as `?id=123`)

#### *Useragent logging*

Log the user agent sent by each browser.

#### *Contentfilter logging*

Log when the content of web pages is filtered

#### *Firewall logging (transparent proxies only)*

Let the firewall log the outgoing web accesses, i.e., those directed through the RED interface to the Internet. This options only works for transparent proxies.

#### **Bypass transparent proxy**

In this panel some exception to the transparent proxy (see also [above](#)) can be defined, i.e., which sources (i.e., clients) and destinations (i.e., remote servers) should be ignored by the proxy, even if it is enabled in that zone.

#### *Bypass transparent proxy from SUBNET/IP/MAC*

The sources that should not be subject to the transparent proxy.

#### *Bypass transparent proxy to SUBNET/IP*

The destinations that are not subject to the transparent proxy.

Hint

Use CIDR notation to enter subnets.

#### **Cache management**

Configuration options for the space occupied on disk by the cache and the size of the objects stored.

#### *Cache size on harddisk (MB)*

The amount in megabytes that the proxy should allocate for caching web sites on the harddisk.

#### *Cache size within memory (MB)*

The amount in megabytes of memory that the proxy should allocate for caching web sites in the system memory.

#### *Maximum object size (KB)*

The upper size limit in megabytes of a single object that should be cached.

#### *Minimum object size (KB)*

The lower size limit in megabytes of a single object that should be cached.

#### **Note**

Objects whose size does not fall within the above defined ranges will never be stored on disk, but downloaded each time they are requested by some client.

#### *Enable offline mode*

When this option is enabled (i.e., the checkbox is ticked), the proxy will never try to update cached objects from the upstream web server - clients can then browse cached, static websites even after the uplink went down.

#### **Warning**

This option proves useful to surf the Internet while the uplink is down, if the page requested has been cached before. However, this option may cause some trouble when trying to refresh a page, even with a working uplink, since the HTTP

proxy would always serve the cached page. The only possibility to have a refreshed copy of a web page is in this case to clear the cache of the proxy server.

#### *Clear cache*

When this button is clicked, the cache of the proxy is erased.

#### *Do not cache these destinations*

The domains whose resources should never be cached.

### **Upstream proxy**

If there is another proxy server in the LAN, it can be contacted before actually requesting the original resource. This panel contains configuration options for the connection between the Panda Gatedefender Appliance and the upstream proxy.

#### *Upstream proxy*

Tick this checkbox to enable an upstream proxy and show more options. When enabled, before retrieving a remote web page that is not already in its cache, the Panda Gatedefender Appliance's proxy contacts the upstream proxy it to ask for that page.

#### *Upstream server*

The hostname or IP address of the upstream server.

#### *Upstream port*

The port on which the proxy is listening on the upstream server.

#### *Upstream username / password*

If authentication for the upstream proxy is required, specify the credentials here

#### *Client username forwarding*

Tick the checkbox to forward the username to the upstream proxy.





#### *Client IP forwarding*

Tick the checkbox to forward the client IP address to the upstream proxy.

## **Access policy**

The accesses policies are applied to every client that is connecting through the proxy, regardless of its authentication. An access policy rule is a time-based scheme that permits or prohibits accesses depending on diverse parameters about the user (e.g., the source or destination of the traffic), and the client used or the content downloaded (e.g., the user agent, the mime types, virus scanning, and content filtering).

A list of the already defined rules is displayed on the page. Any rule can specify if the web access is blocked or allowed, and in the latter case a filter type can be activated and selected. The table carries the following information for every rule listed therein: The progressive identification number (#), the name (`), the source and destination interested, the authentication type, if required, the periods in which is active, the user agents matched, and the available actions:

-  - modify the policy.
-  - remove the policy.
-  - move the policy upwards or downwards in the list.
-  - enable or disable the policy.

To add a new access policy rule, simply click on *Add Access policy*. A form will open, in which to configure all the parameters:

#### *Source Type*

The sources of the traffic to which this rule applies. It can be <ANY>, a zone, a list of networks, IP addresses or MAC addresses.

#### *Destination Type*

The destinations of the traffic to which this rule will be applied. This can be either <ANY>, a zone, or a list of networks, IP addresses, or domains.

#### *Authentication*

The type of authentication to apply to the clients. It can be *disabled*, in which case no authentication is required, *group based* or *user based*. One or more users or groups, to which to apply the policy, can then be selected among the existent ones from the list that will show up.

Hint

Authentication is only local, hence before being able to use it, at least one user or group must be created in the [Authentication](#) tab.

#### *Time restriction*

Decide whether the rule has effect on specific days and/or a time period. By default a rule is always active, but its validity can be limited to either an interval or to some days of the week. By ticking the checkbox, the following options become available:

#### *Active days*

Select one or more days of the week.

Hint

To select two or more days, hold the `CTRL` keys and click the mouse button on the name of the day.

#### *Start hour, Stop hour, Start minute, Stop minute*

To fine-tune the interval of the day during which the access policy is active, select the start and end times from the drop-down menus.

#### *Useragents*

The allowed clients and browsers, as identified by their user agent, i.e., their identification string.

#### *Mimetypes*

A list of the MIME types of incoming files that should be blocked, one per line. MIME types can only be blocked (i.e., blacklisted) but not allowed (i.e., whitelisted), therefore this option is only available in *Deny* access policies. This option allows to block any files not corresponding to the company policy (e.g., multimedia files).

Note

The list of the available MIME types can be found in the `/etc/mime.types` file on any Linux box, on the official IANA [web page](#), and also in [RFC 2045](#) and [RFC 2046](#).

#### *Access policy*

Select whether the rule should allow or deny the web access from the drop-down menu. If set to *Deny*, the *Mimetypes* option above is activated.

#### *Filter profile*

This drop-down menu, available when the *Access policy* has been set to *Allow access*, allows to select what type of check should the rule perform. Available options are: none for no check and virus detection only to scan only for viruses. Moreover, if any content filter profile has been created (see [below](#)), it can be applied to the rule.

#### *Policy status*

Whether the rule is enabled or disabled. Disabled rules will not be applied, the default is to enable the rule.

#### *Position*

The place where the new rule should be inserted: Lower positions have higher priority.

The available actions allow to change priority, edit, enable/disable or delete each rule from the list of rules.

## **Authentication**

The Panda Gatedefender Appliance's proxy supports four different authentication types, that are shown in the drop-down menu at the top of the page: *Local Authentication (NCSA)*, *LDAP (v2, v3, Novell eDirectory, AD)*, *Windows Active Directory (NTLM)* and *RADIUS*. The NCSA type stores the access credentials on the Panda Gatedefender Appliance, whereas the other methods rely on an external server: In those cases it is mandatory to provide all the necessary information to access that server.

Underneath the drop-down menu from which to select the authentication type, two panels are present. The one above, *Authentication settings* contains common configuration items, while the one below changes upon the selection of the authentication type, presenting the settings that are peculiar to each method.

### **Authentication settings**



The common items that can be configured in this panel are:

#### *Authentication realm*

The text shown in the authentication dialog and used as the realm of kerberos or winbind when joining an Active Directory Domain. When Windows Active Directory is used for authentication, the FQDN of the PDC should be used.

Hint

If the server name is `localauth` and the domain name is `example.org`, the FQDN is `localauth.example.org`.

#### *Number of Authentication Children*

The maximum number of authentication processes that can run simultaneously.

#### *Authentication cache TTL (in minutes)*

The time in minutes during which the authentication data should be cached, before being deleted.

#### *Number of different IPs 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 an IP address is associated with the logged in user.

Once the common configuration form have been filled in, depending on the authentication type chosen it is possible to configure the specific settings for the authentication type selected. [Local Authentication \(NCSA\)](#), [Windows Active Directory \(NTLM\)](#), [LDAP \(v2, v3, Novell eDirectory, AD\)](#), [RADIUS](#).

### **NCSA authentication parameters**

#### *NCSA user management*

When clicking on the *manage users* button the management GUI for the users is opened, which consists of a simple list of the existing users, if any was created, and of an *Add NCSA user* link to add more users. A user is added by entering username and password in the form, and can later be either edited or deleted.

Hint

The password shall be at least 6 characters long.

#### *NCSA group management*

When clicking on the *manage groups* button the management GUI for the groups is opened which consists of a simple list of the existing groups and their members, if any was created, and of an *Add NCSA group* link to add more groups. A group is created by entering a group name and selecting one or more users that should belong to that group. A user may belong to more than one group.

Warning

While the same user can be legally part of one or more groups, care must be taken that the the groups the user belongs to do not define contrasting access policies. As an example, consider a user member of two groups, one with the policy to allows access to the website `www.example.org`, while the second group's policy blocks the access to that web page. In this case, it is not easy to predict whether that user will be granted or not access to the site `www.example.org`. The management of these issues is left to the designer of the access policies.

#### *Min password length*

The minimum length for the local user's password.

### **Windows Active Directory authentication parameters.**

#### *Domainname of AD server*

The active directory domain to join. The server's FQDN should be used.

#### *Join AD Domain*

Click on the *join domain* button to join the domain. This action should be done only after the authentication settings have been saved and applied.

#### *PDC hostname of AD server, PDC IP address of AD server*

The hostname and the IP address of the PDC. Both hostname and IP address are needed to create the DNS entry.

#### *BDC hostname of AD server and BDC IP address of AD server*

The hostname and the IP address of the BDC, if any. Both hostname and IP address are needed to create the DNS entry.

Requirements for the use of NTLM.

In order to be able to use Windows' native authentication with active directory (NTLM), a few conditions must be satisfied:

- The authentication settings need to be saved and applied before trying to join the domain.
- The Panda Gatedefender Appliance must join the domain.
- The system clocks on the Panda Gatedefender Appliance and on the active directory server must be synchronised.
- The authentication realm must be a FQDN.
- The PDC hostname has to be set to the netbios name of the Active Directory server.

Hint

The Panda Gatedefender Appliance clock can be synchronised with the clock of the Active Directory server by issuing the following command from the shell:

```
net time set -S IP_OF_AD_SERVER
```

NTLM authentication with Windows Vista and Windows 7.

The HTTP Proxy in the Panda Gatedefender Appliance uses *negotiated* NTLMv2, while both Windows Vista and Windows 7 allow by default only straight NTLMv2. As a result, a client installing those operating systems may fail to authenticate to the HTTP proxy even when supplying the correct credentials. The following changes to the client configuration are required to correctly authenticate:

1. Start › gpedit.msc (run as administrator)
2. Go to: Computer configuration › Windows Settings › Security Settings › Local Policies › Security Options
3. Find the configuration option *Network Security: LAN MANAGER Authentication Level*
4. Select the value "Send LM \* NTLM - use NTLMv2 session security if negotiated"

After applying these changes the client browser should correctly authenticate using the AD Login Name / Credentials for the HTTP Proxy.

#### **LDAP authentication parameters.**

##### *LDAP server*

The IP address or FQDN of the LDAP server.

##### *Port of LDAP server*

The port on which the server is listening. The default value is 389.

##### *Bind DN settings*

The base distinguished name, this is the start point of the search.

##### *LDAP type*

This drop-down menu allows the choice of the type of the authentication server among *Active Directory*, *Novell eDirectory*, *LDAP version 2*, or *LDAP version 3*.

##### *Bind DN username*

The fully distinguished name of a bind DN user, which must have the permission to read user attributes

##### *Bind DN password*

The password of the bind DN user.

##### *user objectClass*

The objectClass that the bind DN user must belong to.

##### *group objectClass*

The objectClass that the bind DN group must belong to.

#### **RADIUS authentication parameters.**

##### *RADIUS server*

The IP address or URL of the RADIUS server.

##### *Port of RADIUS server*

The port on which the RADIUS server is listening.

### Identifier

An additional identifier.

### Shared secret

The password to be used.



## Web filter

The Panda Gatedefender Appliance's content filter abilities are based on the Cyren (former Commtouch) URL filtering solution, that uses two filtering techniques which can be defined per filter profile.

The first one consists of an advanced method of web pages categorisation, based on their content, while the second method uses a combination of white- and blacklists URLs and domains: All the URLs requested by a client are looked up in this list and are only served if they are found in the whitelist.

A *profile* is needed to be able to use the content filter. There is a *Default profile* available, which allows access to every web page and shall not be deleted. Additional profiles, that are needed in the definition of an [Access policy](#), can easily be created. Hence, an access policies requiring a specific profile can be created only after that profile.

On the page, there is a list of the existing profiles, accompanied by a remark and by the available actions:

-  - edit a profile.
-  - delete a profile.



Above the table, there is a *Create a profile* link: When clicked, the link is replaced by the *Profile Editor*, that is used to configure a new profile, with the list of existing profiles shifting to the bottom of the page. The following settings can be defined:

### Profile name




The name given to the profile.

### Activate antivirus scan

Enable the antivirus in the content filter.

The next settings come in form of panels, that can be expanded or collapsed by clicking on the  or  icons to the left of their title. On the far right, a small arrow shows if the contained items are all, none, or partially allowed. Those arrows can be clicked to quickly toggle the status of all the contained items.

## URL Filter

The categories to activate for applying the content filter. Each category contains additional sub-categories, that can be individually allowed or not. A green arrow  means that the (sub-)category's items are used for content filter, while a  icon means that those items are not used. A  icon near the category name shows that only some of the sub-categories within it are used for content filtering.

## Custom black- and whitelists

Here personalised lists of web pages can be added as always allowed (whitelist), i.e., they will always be served to the clients, or denied (blacklist), i.e., they will never be served to the clients.

Content filtering may cause both false positives and false negatives, hence list domains that should always be blocked or allowed can be entered here. This policy will be applied regardless of the results of the content filter's analysis.

## AD join

In this section it is possible to supply the credentials required to join the Active Directory Server, an operation that is only possible if in the [Authentication](#) tab the option *Windows Active Directory (NTLM)* has been selected.

### Username of ADS admin

The username of the Active Directory Server.

### Password of ADS admin

The password of Active Directory Server. It is not shown by default, but it can be displayed by ticking the checkbox on the right of the text field.

## HTTPS Proxy

In this page it is possible to configure the proxy server for the scan of SSL-encrypted traffic, i.e., traffic through the 443 port. When enabled, squid will intercept all clients' requests and forward them to the remote server, like in the case of HTTP requests. The only difference is that for HTTPS requests, an 'intermediate' certificate is needed for the client to connect via HTTPS to the Panda Gatedefender Appliance, which then can deliver the request, retrieve the remote resource, control it, and then send it to the client who requested it.

There are three available settings in this page, divided in two parts: The first one allows the set up the HTTPS proxy, whereas the second one is used to manage the Panda Gatedefender Appliance's certificate.

### *Enable HTTPS Proxy*

Tick this checkbox to activate the HTTPS proxy. The next option will appear.

### *Accept every certificate*

This option allows the Panda Gatedefender Appliance to automatically accept all the certificates from the remote server, even those that are not valid or outdated.

To activate the HTTPS proxy, click on *Save* and wait a few seconds.

The lower part can be used to either upload a certificate that will be used by the Panda Gatedefender Appliance or to generate a new one, that will replace the one already present, if any.

### *Upload proxy certificate*

To use an existent certificate, click on *Browse...*, choose the certificate on the local hard disk, then click on *Upload* to copy the certificate to the Panda Gatedefender Appliance.

### *Create a new certificate*

To create a new certificate from scratch, click on this button. A confirmation dialog box appears, requiring a confirmation. Click on *OK* to proceed or on *Cancel* to close the dialog box and go back.

After the certificate has been uploaded or created, a new option in the form of a hyperlink will appear next to the *Upload proxy certificate* label:

### *Download*

Click this hyperlink to download the certificate, which will be needed by the the clients.

## POP3

This page contains configuration options for the spamassassin mail filter and how it should manage the e-mails recognised as spam.

## Global settings

On this page, by ticking the appropriate checkboxes, a few global configuration settings of the POP3 proxy can be enabled.

### *Enabled on Green, Enabled on Blue, Enabled on Orange*

Enable the POP3 e-mail scanner on the GREEN, BLUE, and ORANGE zone, respectively. They appear only if the corresponding zones are enabled.

### *Virus scanner*

Activate the virus scanner.

### *Spam filter*

Enable spam filtering on the e-mails.

### *Intercept SSL/TLS encrypted connections*

When the checkbox is ticked, also connections over SSL/TLS are scanned for virus.

### *Firewall logs outgoing connections*

Let all the outgoing connections be logged by the firewall.

## Spam filter

This page allows to configure how the POP3 proxy should proceed when it finds a spam e-mail.

### Note

Even when an email has been marked as spam, it will be delivered to the original recipient. Indeed, not delivering it would break [RFC 2821](#), which states that once an email is accepted, it must be delivered to the recipient.

### *Spam subject tag*

The prefix that will be added to the subject of the e-mail recognised as spam.

### *Add spam report to mail body*

Tick the checkbox to replace, in each spam e-mail, the body of the original e-mail with a report of the **spamassassin** daemon with the summary of its findings, i.e. with the reasons why the e-mail has been reported as spam.

### *Required hits*

The number of hits required for a message to be considered as spam.

### *Activate support for Japanese emails*

Tick this checkbox to activates support for Japanese character sets in e-mails to search for Japanese spam.

### *Enable message digest spam detection (pyzor)*

To detect spam e-mails using pyzor (in short: spam e-mails are converted to a unique digest message that can be used to identify further analogous spam e-mails).

### Warning

Activating this option might considerably slow down the POP3 proxy!

### *White list*

A list of e-mail addresses or whole domains, specified using wildcards, e.g., \*@example.com, one address per line. E-mails sent from these addresses and domains will **never** be checked for spam.

### *Black list*

A list of e-mail addresses or whole domains, specified using wildcards, e.g., \*@example.com, one address per line. E-mails sent from these addresses and domains will **always** be marked as spam.

The settings can be saved by clicking on the *Save* Button.

### Encrypted e-mails.

The Panda Gatedefender Appliance is unable to scan the e-mails sent through a POP3 SSL connection since it is an encrypted channel.

Therefore, to allow a client to use POP3 over SSL it is necessary to appropriately configuring it and to disable the encryption from the client to the Panda Gatedefender Appliance. Encryption should be disabled (i.e., do not use SSL), but the port for POP3 traffic in plain text changed from the default 110 to 995.

After setting this configuration, the connection from the client to the Panda Gatedefender Appliance will remain in plain text, but it will use port 995, making the Panda Gatedefender Appliance setup an encrypted POP3 over SSL connection from it to the POP3 server.

## FTP

The FTP proxy is available only as a transparent proxy in the zones that have been enabled and allows for scanning the files downloaded via FTP to search for viruses. The Panda Gatedefender Appliance employs frox as FTP proxy.

### Note

Only connections to the standard FTP port (21) are redirected to the proxy. This means that if a client is configured to use the HTTP proxy also for the FTP protocol, settings for the FTP proxy will be bypassed.

A few options can be configured in this page:

*Enabled on GREEN, Enabled on BLUE, Enabled on ORANGE*

Enable the FTP proxy on each zone. Only available on the activated zones.

#### *Firewall logs outgoing connections*

Log the outgoing connections in the firewall.

#### *Bypass the transparent Proxy from Source*

Allow the sources under the corresponding text area not to be subject to the FTP proxy scanning.

#### *Bypass the transparent Proxy to Destination*

Allow the destinations under the corresponding text area not to be subject to the FTP proxy scanning.

FTP proxy and FTP client's active and passive mode.

The Panda Gatedefender Appliance supports transparent FTP proxying with frox if and only if it is directly connected to the Internet.

Problems may also arise when the FTP transparent proxy is enabled and there is a NAT device between the Panda Gatedefender Appliance and the Internet. In this setup, any FTP connection to a remote FTP site will be blocked until it times out, and in the logs will appear messages like:

```
Mon Mar  2 11:32:02 2009 frox[18450] Connection timed out when
  trying to connect to <your ftp client ip>
Mon Mar  2 11:32:02 2009 frox[18450] Failed to contact client data port
```

To overcome this problems, the ftp *client* should be configured to use **passive mode (PASV)** as transfer mode, and a rule under Menubar › Firewall › System access must be created, that allow the traffic on ports 50000 to 50999 for the NAT device. For security reasons, though, these ports should be enabled only if necessary. To understand the motivation of this setup, here is the description in more details of how active and passive modes work and how they interact with the FTP proxy.

The active mode requires that the server (in our case, the FTP proxy) initiate the data connection to the client. However, a NAT device between the clients and the proxy causes the connection from the server to never reach the client. For this reason the client must use the passive mode.

With passive mode, the ftp client is required to initiate the connection to the server (again, the FTP proxy) using a dynamic port, which has been negotiated through the control connection. The ftp proxy listens to that port, but the system access firewall needs to allow traffic to that port.

Since multiple concurrent data connections can try to access the the ftp proxy, it is necessary to allow connections for a whole port range, Therefore all the ports reserved for passive data connections (i.e., 50000-50999) need to be allowed by the system access firewall.

## SMTP

The SMTP proxy can relay and filter e-mail traffic when it is sent from the clients to the mail servers.

The purpose of the SMTP proxy is to control and optimise the SMTP traffic and to protect the local networks from threats when using the SMTP protocol. SMTP is used whenever an e-mail is sent from a local e-mail client to a remote mail server, that is, for the outgoing e-mails. It will also be used if an mail server is running on the LAN (i.e., within the GREEN zone) or DMZ (ORANGE zone) and the e-mails can be sent from outside the local network (incoming requests) through t hat mail server, that is, when clients are allowed to send e-mails from the RED interface.

In order to download mail from a remote mailsrver to a local e-mail client, the POP3 or IMAP protocol are used. In order to protect that traffic too, enable the POP3 proxy in Menubar › Proxy › POP3.


#### Warning

Scanning of IMAP traffic is currently not supported.

With the e-mail proxy functionality, both incoming and outgoing e-mail traffic can be scanned for viruses, spam, and other threats. E-mails are blocked if necessary and in that case both the receiving user and the administrator are notified. With the possibility to scan incoming e-mails, the e-mail proxy can handle incoming connections from the RED interface and pass the e-mail to one or more internal mail servers. Hence, it is possible to run an own mail server behind the firewall without the need to define appropriate port forwarding rules.

The SMTP proxy configuration is split into six tabs, each one tailored to one aspects of the SMTP proxy.

## Configuration

This is the main configuration page for the SMTP proxy. The SMTP proxy can be enabled by clicking on the toggle switch . When enabled, for each active zone can be chosen whether the SMTP proxy should be active, inactive, or transparent:

#### *active*



The SMTP proxy is enabled for the zone and accepts requests on port 25.

#### *transparent mode*

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 the clients. This option is not available for the RED zone.

#### *inactive*

The SMTP proxy is not enabled for that zone.

Additional options are available, grouped in five panels. Each panel can be expanded by clicking on the  icon or hidden by clicking on the  icon.

### **Spam settings**

In this panel there is the possibility to configure the software applications used by Panda Gatedefender Appliance to recognise and filter out spam, configuring the following options:

#### *Filter mail for spam*

Enable the mail spam filter and allows the configuration of additional options that will appear below.

#### *Choose spam handling*

There are three actions that can be carried out on e-mails that have been recognised as spam:

- *move to default quarantine location*: The spam e-mails will be moved to the default location.
- *send to quarantine email address*: Spam e-mails are forwarded to a custom e-mail address that can be specified in the *Spam quarantine email address* textbox that will appear upon selecting this option.
- *mark as spam*: The e-mail is marked as spam before delivery.
- *drop email*: The spam e-mail is immediately deleted.

#### *Spam subject*

A prefix applied to the subject of all e-mails marked as spam.

#### *Email used for spam notifications (spam admin)*

The e-mail address that will receive a notification for each processed spam e-mail.

#### *Spam tag level*

If SpamAssassin's spam score is greater than this number, the *X-Spam-Status* and *X-Spam-Level* headers are added to the e-mail.

#### *Spam mark level*

If SpamAssassin's spam score is greater than this number, the *Spam subject* and *X-Spam-Flag* headers are added to the e-mail.

#### *Spam quarantine level*

Any e-mail that exceed this spam score will be moved to the quarantine location.

#### *Send notification only below level*

Send notification e-mails only if the spam score is below this number.

#### *Spam filtering*

Enable [spam greylisting](#) and show the next option.

#### *Delay for greylisting (sec)*

The greylisting delay in seconds can be a value between 30 and 3600.

#### *Spam report*

Tick the checkbox to add a report to the body of e-mails that are recognised as spam.

#### *Japanization*

Tick this box to activate the support for Japanese character sets in e-mails and filter Japanese spam e-mails.

## Note

While most simple and 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 personalised and stronger filter (bayes).

## Virus settings

In this panel a few options can be configured to manage any virus found.

### Scan mail for virus

Enable filtering of e-mails for viruses and to reveal the additional virus filter options.

### Choose virus handling

There are three or four available actions (depending on the type of Panda Gatedefender Appliance) that can be carried out on e-mails that have been recognised as spam. They are the same as in the *Spam settings* above:

- *move to default quarantine location*: any e-mail containing virus will be moved to the default location.
- *send to quarantine email address*: e-mails containing virus are forwarded to a custom e-mail address that can be specified in the *Virus quarantine email address* textbox that will appear upon selecting this option.
- *pass to recipient (regardless of bad contents)*: e-mail containing virus will be delivered normally.
- *drop email*: The e-mail containing virus is immediately deleted.

### Email used for virus notifications (virus admin)

The e-mail address that will receive a notification for each processed e-mail containing virus.

## File settings

This panel contains settings to block any files attached to an e-mail depending on their extension. Whenever those file extensions are found in any attachment, the selected action will be performed.

### Block files by extension

Activate the extensions-based filtering on files and reveal the additional virus filter options.

### Choose handling of blocked files

There are three or four available actions (depending on the type of Panda Gatedefender Appliance ) that can be carried out on e-mails that have blocked (They are the same as in the previous *Spam settings* and *Virus settings* boxes):

- *move to default quarantine location*: e-mails containing blocked files will be moved to the default location.
- *send to quarantine email address*: e-mails containing blocked files are forwarded to a custom e-mail address that can be specified in the *Email used for blocked file notifications* textbox that will appear upon selecting this option.
- *pass to recipient (regardless of blocked files)*: e-mails containing blocked files will be delivered normally

### Choose filetypes to block (by extension)

The file extensions to be blocked.

#### Hint

Hold down the **CTRL** key and click on the left mouse button to select multiple extensions.

### Email used for blocked file notifications (file admin)

The e-mail address that will receive a notification for each processed e-mail containing blocked attachments.

### Block files with double extension

Enable the blocking of any file with a double extension.

## Note

Files with double extensions are usually malicious files which may appear as inoffensive images or documents, but when they are clicked, an application is executed that has the purpose to harm a computer or steal personal data. A file with a double extensions is exactly like a normal file, but whose name (e.g., `image . jpg`) is followed by `.exe`, `.com`, `.vbs`, `.pif`, `.scr`, `.bat`, `.cmd` or `.dll` (e.g., `image . jpg . exe`).



It is necessary to configure the e-mail domains for which each local server should be responsible. The list of combinations domain-SMTP server can be defined under Menubar › Proxy › SMTP › Incoming domains.

### Quarantine settings

There is only one option in this panel:

#### *Quarantine retention time (in days)*

The number of days that the e-mail will be stored in the special quarantine location on the Panda Gatedefender Appliance before being deleted.

Hint

The e-mails stored in the quarantine can be managed in the Mail Quarantine, located at Menubar › Services › Mail Quarantine

### Bypass transparent proxy

In the last panel custom lists of domains can be defined for which the transparent proxy should be disabled.

#### *Bypass transparent proxy from SUBNET/IP/MAC*

E-mails sent from these sources are not subject to the transparent proxy.

#### *Bypass transparent proxy to SUBNET/IP*

E-Mails sent to these destinations are not subject to the transparent proxy.

## Black- & Whitelists

In this page there are four panels: Three allow the definition of several custom black- and whitelists, while the fourth allows to select and use existing RBL.

Examples for recipient/sender black- and whitelists:

Entire (sub-)domains can be white- or blacklisted as follows:

- A domain including subdomains: `example.com`
- Only the subdomains: `.example.com`
- A single address: `info@example.com, admin@example.com`

Examples for client black- and whitelists:

- A domain or IPs: `example.com, 10.10.121.101, 192.168.100.0/24`

### Accepted mail (Black- & Whitelists)

In the first panel any number of domains, sub-domains, or single e-mail addresses to be white- or blacklisted can be entered. For both of the lists any number of senders, recipients, and clients can be entered in the appropriate textareas, as follows:

#### *Whitelist sender*

All the e-mails sent from these addresses or domains will be accepted. This is the e-mail **From** field.

#### *Blacklist sender*

All the e-mails sent from these addresses or domains will be rejected. This is the e-mail **From** field.

#### *Whitelist recipient*

All the e-mails sent to these addresses or domains will be accepted. This is the e-mail **To** field.

#### *Blacklist recipient*

All the e-mails sent to these addresses or domains will be rejected. This is the e-mail **To** field.


#### *Whitelist client*

All the e-mails sent from these IP addresses or hosts will be accepted.

### Blacklist client

All the e-mails sent from these IP addresses or hosts will be rejected.

### Realtime Blacklist (RBL)

An often used method to block spam e-mails are so called RBL, whose use can be configured in the second panel. These lists are created, managed, and updated by different organisations with the purpose to identify as quickly as possible new SMTP server used to send spam and block them. If a domain or sender IP address appears in one of the blacklists, e-mails sent from there will be rejected without further notice. The use of RBL saves bandwidth, since the mails will not be accepted and then handled like legitimate e-mails, but rather dismissed as soon as the sender's IP address or domain is found in any blacklist. The Panda Gatedefender Appliance uses many different RBL, which are divided into IP-based and domain-based. The blacklist that belong on each category are shown by clicking on the small  icon, and can be enabled or disabled by clicking on the red or green arrow on top of the list, or individually. The homepage of the various organisations that compile the lists is reachable by clicking on the list's name.

### Warning

Sometimes it can happen that IP addresses or domains have been wrongly listed by an RBL operator. If this should happen, it may negatively impact communications, since even legitimate e-mails from those domains will be refused without the possibility to recover it. Since there is no possibility to directly influence the RBLs, it is necessary to take into account the policies applied from the organisations that manage the RBLs before using them. Panda is not responsible for any e-mail that might be lost using the RBLs.

Among the blacklist installed, there are:

#### *bl.spamcop.net*

A blacklist based on submissions from its users.

#### *zen.spamhaus.org*

This list replaces the old 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 (e.g., HTTP, socks, AnalogX, wingate etc.) that 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.

#### *[name].dnsbl.sorbs.net and rhsbl.dnsbl.sorbs.net*

Several blacklists are supplied from this organisation (replace [name] with safe, relays, etc), and can be activated individually or all together by enabling the *dsnbl.sorbs.net* blacklist.

#### *uceprotect.net*







Lists that hold domains of known spam sources for at most seven days. After this period, domains are delisted, but subsequent violations cause the application of more restrictive policies.

#### *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.

#### Note

The rfc-ignorant.org site has shut its service down on the 30th of November 2012 (see the [announcement](#)), but its content has been inherited by people at <http://www.rfc-ignorant.de/>. Their work, however, has not yet produced working RBLs as of today (November 2013).

The RBLs are grouped into two boxes. On the left-hand side there are IP-based RBLs, while on the right-hand side there are domain-based RBLs. To activate all the RBLs in one box, click on the  icon next to the box's title bar (the icon will become ) , while to enable only some of the RBLs, click on the  icon next to each RBL's name. In that case, the  or  icon on the title bar will be replaced by a  icon.

### Spam greylisting

In the third panel, greylisting whitelists can be created by adding entries for every recipient, IP address or network in the two textareas. To the items in the whitelist will not be applied any greylisting

### Whitelist recipient

All E-mail addresses or whole domains written in this textarea, e.g. test@example.com or example.com are considered "safe", i.e., the e-mail received from them will not be checked for spam.

#### *Whitelist client*

All the mailservers' address in this textarea are considered "safe", i.e., all the e-mails coming from this server's address will not be checked for spam.

#### Greylisting

Greylisting is a method used by a MTA to verify whether an e-mail is legitimate by rejecting it a first time and waiting for a second dispatch of the same e-mail. If the e-mail is not received anymore the sender is considered as a spam source. The idea behind greylisting is that any mass spam bot will not try to resend any rejected e-mail, so only valid e-mails would be resent.

#### **Spam (Black- & Whitelists)**

Finally, in the last panel, explicit black- and whitelists for the spam filter are defined.

#### *Whitelist sender*

E-mail addresses or whole domains can be whitelisted in this textarea (i.e., they will never be detected as spam), like e.g. test@example.com or the domain example.com.

#### *Blacklist sender*

E-mail addresses or whole domains can be blacklisted in this textarea (i.e., they will always be detected as spam), like e.g. test@example.com or the domain example.com.

## Incoming domains

When incoming mail has been enabled (i.e., clients outside the RED interface can send e-mails from a local SMTP server) and e-mails to be sent should be forwarded to an mail server behind the Panda Gatedefender Appliance - usually set up in the ORANGE zone - it is necessary to declare the domains to be accepted by the SMTP proxy and to which of the e-mail servers the incoming mail should be forwarded. It is possible to specify multiple mail servers behind the Panda Gatedefender Appliance for different domains.

The page presents a list of domains along with the mailservers responsible for each of them, if any has been defined. To add a new domain, click on the *Add a domain* button: A simple form will open, in which the combination domain-mailservers can be created.



#### *Domain*

The domain this mailservers is responsible for.

#### *Mailservers IP*

The IP address of the mailservers.

The new entry will be shown at the bottom of the list. The actions available for each domain are:



-  - modify the domain's property.
-  - remove the domain.

#### Warning

No confirmation is asked after clicking on the  icon: The domain will be removed immediately.

## Domain routing

The page shows a list of domains along with the smarthost responsible for the e-mails' delivery to or reception from those domains. The information shown by the list are the same that shall be provided when adding a new domain. Available actions are:

-  - modify the domain routing.
-  - remove the domain routing.

To add a new domain, click on the *Add new domain route* button: A simple form will open, in which the combination domain-mailservers can be created.

### Direction

Decide whether the rule will be applied to the domain associated with the sender or with the recipient.

### Domain

The domain this mailserv is responsible for.

### Outgoing address

The interface or IP address of the uplink through which the e-mails will be sent, among those available in the drop-down menu. If left blank, it will be left to the smarthost the choice of the uplink or IP address to be used.

### Smarthost



A tick on this checkbox will reveal more options to override the system's smarthost and configure an external one. The options are the same that are in the [Smarthost configuration](#) below.

### Rule's priority

Suppose you have set up two rules for domain routing: One with domain mydomain.com as the sender and uplink *main* as the route, and a second one with domain example.org as the receiver and uplink *secondary* as the route. What happens to an email that is sent from server foo.mydomain.com to a user on bar.example.org? The answer can be found in how the Panda Gatedefender Appliance's MTA, **postfix**, processes the e-mails' sending rules: It first reads all the rules involving the *sources*, then the rules involving the *recipient*. Thus, the e-mail that is sent from foo.mydomain.com to bar.example.org will be routed through through the *secondary* uplink.

## Mail Routing

This option allows to send a BCC of an e-mail to a given e-mail address and is applied to all the e-mails sent either to a specific recipient or from a specific sender address. The list show the direction, the address and the BCC address, if any, and the available actions:

-  - modify the mail routing.
-  - remove the mail routing.

To add a new mail route, click on the *Add a Mail Route* button. In the form that opens these options can be configured:

### Direction

Select from the drop-down menu whether the mail route should be defined for a sender or recipient of the e-mail.

### Mail address

Depending on the direction chosen, this will be the e-mail address of the recipient or sender to which the route should be applied.



### BCC address

The e-mail address which are the recipient of the copy of the e-mails.

### Warning

Neither the sender nor the recipient will be notified of the copy being sent to a third party. In most countries it is highly illegal to read other people's private messages, so please **do not** misuse **nor** abuse of this feature.

## Advanced

In this page of the SMTP proxy configuration there are advanced settings options available, grouped in four panels, that can be shown or hidden by clicking on the  or  icons on the left of the panel title.

### Smarthost configuration

In the first panel a smarthost can be activated and configured. If the SMTP server has a dynamic IP address, for example when using an ISDN or an ADSL dialup Internet connection, there can be some troubles sending e-mails to other mail servers, since that IP address might have been blacklisted in some RBL (see [Black- & Whitelists](#) above) and therefore the remote mailserv might refuse the e-mails. Hence, it becomes necessary to use a smarthost for sending e-mails.

### Smarthost for delivery

Tick this checkbox to enable a smarthost for delivering e-mails and to show additional options.

### Smarthost address

The IP address or hostname of the smarthost.

#### *Smarthost port*

The port on which the smarthost is listening, defaults to 25.

#### *Smarthost authentication*

Tick this checkbox if the smarthost requires authentication. The next three extra options are then shown.

#### *Smarthost username*

The username used for authentication on the smarthost.

#### *Smarthost password*

The password used for authentication on the smarthost.

#### *Choose authentication method*

The authentication methods required by the smarthost: *PLAIN*, *LOGIN*, *CRAM-MD5*, and *DIGEST-MD5* are supported. More methods can be chosen by holding the **CTRL** key pressed and clicking on each of the desired methods.

#### **Note**

In a few words, a smarthost is a mailserver used by the SMTP proxy as the outgoing SMTP server. The smarthost needs to accept the e-mails and relays them. Normally, the provider's own SMTP server is used as the smarthost, since it will accept to relay the e-mails, while other mailservers would not.

#### **IMAP Server for SMTP authentication**

This panel contains configuration options for the IMAP server that should be used for authentication when sending e-mails. These settings are especially important for SMTP incoming connections that are opened from the RED zone. The following settings can be configured:

#### *SMTP authentication*

Tick this checkbox to enable IMAP authentication and to show additional options.

#### *Choose number of authentication daemons*

How many concurrent logins are possible through the Panda Gatedefender Appliance.

#### *IMAP authentication server*

The IP address of the IMAP server.

#### *IMAP authentication port*

The port on which the IMAP server is listening, defaults to 143 for plain IMAP or 993 for IMAP over SSL.

#### **Mail server settings**

In this panel, additional parameters of the SMTP server can be defined.

#### *SMTP HELO*

When this checkbox is ticked, the connecting client must send a HELO (or EHLO) command at the beginning of an SMTP session.

#### *Invalid hostname*

Reject the connecting client when the client HELO or EHLO parameter supplies an invalid hostname.

#### *SMTP HELO name*

The hostname to send with the SMTP EHLO or HELO command. The default value is the REDIP, but a custom hostname in FQDN format can be supplied.

#### *Always BCC to address*

An e-mail address here that will receive a BCC of each message that goes through the SMTP proxy.

#### *Choose mailtemplate language*

The language in which error messages should be sent, among those available: English, German, Italian, and Japanese.

#### *Verify recipient address*

Enable the check for a valid recipients address before sending the message.

#### *Choose 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).

### *Choose maximal email contentsize*

The maximum size allowed for a single e-mail message. Several predefined values can be selected from the drop-down menu. Choosing the *custom email contentsize* option reveals the next option.

### *Custom maximum email contentsize (in KB)*

The maximum size in mega bytes of the e-mail that will be accepted by the SMTP server.

### *Enable DSN on zones*

Choose from the available zones those which will send a bounce message (i.e., a DSN message) to undeliverable e-mails or to e-mails that can not be correctly sent. In other words, it will be possible to receive delivery notification messages of emails only from zones that have been selected here.

### HELO/EHLO and hostname

Almost all mail servers require that clients connecting via SMTP announce themselves with a *valid hostname* along with the HELO/EHLO, or they drop the connection. However, the Panda Gatedefender Appliance uses its own hostname in order to announce to foreign e-mail servers, which is sometimes not publicly valid within the global DNS.

If that is the case, another custom hostname can be configured under Menubar › Proxy › SMTP › Advanced › Mail server settings › SMTP Helo Name, that can be understood by the remote mail server.

Instead of a custom hostname, even a numeric IP address within brackets (e.g., [192.192.192.192]) can be supplied, which should be the REDIP address.

### Spam prevention

Finally, in this last panel additional parameters for the spam filter can be defined, by ticking one or more of the four checkboxes.

#### *invalid recipient*

Reject the request when the *RCPT TO* address is not in FQDN form, as required by the [RFC 821](#).

#### *invalid sender*

Reject the connecting client if the hostname supplied with the HELO or EHLO command is not a FQDN as required by the [RFC 821](#).

#### *unknown recipient domain*

Reject the connection if the domain of the recipient e-mail address has no DNS *A* or *MX* record.

#### *unknown sender*

Reject the connection if the domain of the sender e-mail address has no DNS *A* or *MX* record.

### Troubleshooting STMP proxy.

When the message “**Mail for xxx loops back to myself**” appears in the log file, it is indicative of a misconfiguration in the custom SMTP HELO name on the appliance, that is the same as the hostname of the internal mailserver to which the incoming e-mail should be forwarded.

In that case the SMTP connection received from the internal mailserver will contain an hostname (the one in the HELO line from the SMTP Proxy setting), that is the same as the hostname of the internal mailserver, hence the internal mailserver believes to send **and** receive the same e-mail, producing the error message.

Possible solutions are:

- Change the hostname of the internal mailserver.
- Create a new publicly valid *A* Record within the DNS zone which also points to the Panda Gatedefender Appliance and use this hostname as the HELO line within the SMTP Proxy.
- Use the numeric IP Address of the uplink as the HELO line.

## Anti-Spam

This page includes configuration settings for the anti-spam engine. The following options can be configured:

### *Enable spamassassin shortcircuit*

Check this box to skip spamassassin whenever Cyren (former Commtouch) marks a message as spam.

#### *Ignore IPs/Networks*

Here IPs and networks which should not be checked by Cyren can be defined.

In the SPAM tag level section the following options can be configured. The valid values for each option are between -10 and 10 included.

#### *CONFIRMED*

Every e-mail with a tag level above this value will be recognised as spam.

#### *BULK*

Every e-mail with a tag level above this value will be identified as bulk mail.

#### *SUSPECTED*

Every e-mail with a tag level above this value will is suspected to contain spam.

#### *UNKNOWN*

E-mails with a tag level below this value will be classified as unknown.

#### *NONSPAM*

E-mails with a tag level below this value will be recognised as non-spam mails.

## DNS

The DNS proxy is a proxy server that intercepts DNS queries and answers them, without the need to contact a remote DNS server each time it is necessary to resolve an IP address or a hostname. When a same query is often repeated, caching its results locally may sensibly improve performances. The available settings for the DNS proxy are grouped into three tabs.

### DNS proxy

A few options for the DNS proxy can be configured in this page.

#### *Transparent on Green, Transparent on Blue, Transparent on Orange*

Enable the DNS proxy as transparent on the GREEN, BLUE, and ORANGE zone, respectively. They appear only if the corresponding zones are enabled.

Specific sources and destinations can be set up to bypass the proxy by filling in their values in the two text areas.

#### *Which sources may bypass the transparent Proxy*

Allow the sources under the corresponding text area not to be subject to the DNS scanning. The sources can be specified as IP addresses, networks, or MAC addresses.

#### *Destinations to which bypass the transparent Proxy*

Allow the destinations under the corresponding text area not to be subject to the DNS proxy scanning. The destinations can be specified as IP addresses or networks.

### DNS Routing

This page allows the management of custom domain - nameservers pairs. In a nutshell, whenever a sub-domain of a domain is queried, the corresponding nameserver in the list will be used to resolve the domain into the correct IP address.

A new domain - nameserver combination can be added by clicking on the *Add new custom nameserver for a domain* link. When adding an entry, a few values can be entered for the various options available:

#### *Domain*

The domain for which to use the custom nameserver.



#### *DNS Server*

The IP address of the nameserver.

#### *Remark*

An additional comment.

On each domain in the list, these actions can be carried out:

-  - edit the rule.
-  - delete the rule.

## Anti-spyware

This page presents configuration options about the reaction of the Panda Gatedefender Appliance when asked to resolve a domain name that is known to be either used to propagate spyware or that serves as phishing site. The options that can be set are:

### *Enabled*

The requests are redirected to localhost. In other words, the remote site will neither be contacted nor reachable.

### *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*

The update frequency of the spyware domain list. Possible choices are *Daily*, *Weekly*, and *Monthly*. By moving the mouse cursor over the respective question mark, the exact time of the update execution is shown.

### Hint

to download updated signatures, the system must be registered to Panda Perimetral Management Console.



# 8. The VPN Menu

---

A VPN allows two separated local networks to directly connect to each other over potentially unsafe networks such as the Internet. All the network traffic through the VPN connection is securely transmitted inside an encrypted tunnel, hidden from prying eyes. Such a configuration is called a *Gateway-to-Gateway VPN*, or *Gw2Gw VPN* for short. Similarly, a single remote computer somewhere on the Internet can use a VPN tunnel to connect to a local 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.

The Panda Gatedefender Appliance supports the creation of VPNs based either on the *IPsec* protocol, which is supported by most operating systems and network equipment, or on the *OpenVPN* service.

The Panda Gatedefender Appliance can be set up either as an OpenVPN server or as a client, and even play both roles at the same time, in order to create a network of OpenVPN-connected appliances. The menu items available in the sub-menu are the following:


- OpenVPN server - set up the OpenVPN server so that clients (both *roadwarriors* and other Panda Gatedefender Appliances in a Gateway-to-Gateway setup) can connect to one of the local zones.
- OpenVPN client (Gw2Gw) - set up the client-side of a Gateway-to-Gateway setup between two or more Panda Gatedefender Appliances
- IPsec/L2TP - set up IPsec-based VPN tunnels and L2TP connections
- Authentication - manage users of VPN connections.
- Certificates manage certificate that shall be used with VPN connections.

## OpenVPN server

When configured as an OpenVPN server, the Panda Gatedefender Appliance can accept remote connections from the uplink and allow a VPN client to be set up and work as if it were a local workstation or server.




Starting with version 5.50, the OpenVPN server deployed on the Panda Gatedefender Appliance allows the simultaneous presence of several instances. Each server will listen to one different port, accepting incoming connections on that port only. Moreover, when the hardware on which Panda Gatedefender Appliance is installed has multiple CPU cores, every instance may be assigned more than one core, thus resulting in an increase of the throughput and data processing of that instance. It is nevertheless also possible to have multiple instances of OpenVPN running on a device equipped with a single-core CPU, though this results in the CPU carrying the load of all instances.

## Server configuration

This page shows a switch *Enable OpenVPN server* 

that will start the OpenVPN server and all services related to it (like e.g., the [VPN firewall](#) if enabled) once clicked.

Below, there is one box, *OpenVPN settings*, that allows to set up some global settings. Right below, a link allows to define a new server instance while at the bottom of the page there's the list of the available OpenVPN servers running on the Panda Gatedefender Appliance, if any has already been defined. The list shows the following data about each OpenVPN server instance defined: The name, remark, and details about the configuration, namely: The port on which it is listening, the protocol, the type of device, and the type of network. Finally, the actions available are:

-  - the server is active or stopped.
-  - modify the server's configuration
-  - remove the configuration and the server.

Note

When starting the OpenVPN server for the first time, the root and host certificates are generated automatically.

### OpenVPN settings

The box on the top shows the current OpenVPN settings, which concern the authentication method, and are:

*Authentication type*

There are three available authentication methods to connect clients to the OpenVPN server running on the Panda Gatedefender Appliance:

- *PSK (username and password)*. Connection is established after providing correct username and password.
- *X.509 certificate*. A valid certificate only is needed to connect.
- *X.509 certificate & PSK (two factor)*. Besides a valid certificate, username and passwords are needed.

#### Warning

When employing certificate-only authentication, a client with a valid certificate will be granted access to the OpenVPN server even if it has no valid account!

Panda Gatedefender Appliance's default method is *PSK (username/password)*: The client authenticates using username and password. To use this method, no additional change is needed, while the other two methods are described below.

#### Certificate configuration

This drop-down menu is used to select the method of creation of a new certificate. The available options are:

- *Generate a new certificate*. Create a new certificate from scratch. This option is only available if no host certificate has already been generated. A form will open where to specify all options necessary to create a new certificate. These are the same found in the new certificates generation editor, with two slight changes: *Common name* becomes *System hostname* and *Organizational unit name* becomes *Department name*.
- *Use selected certificate*. Select one certificate from those available, shown on the right-hand side of the drop-down menu. It is possible to see the full details of this certificate by clicking on the *View details* hyperlink.

#### Hint

The name of the certificate selected appears right above the hyperlink.

- *Use an existing certificate*. A second drop-down menu on the left allows to select a certificate that has already been created and stored on the Panda Gatedefender Appliance.
- *Upload a certificate*. By clicking on the *Browse...* button that appears underneath the drop-down menu it will be possible to select from the workstation and to upload an existing certificate. The password for the certificate, if needed, can be provided in the textfield on the right-hand side.
- *Upload a certificate signing request*. The *Browse...* button that appears underneath the drop-down menu can be clicked to select from the workstation and upload an existing certificate signing request. The validity of the certificate in days can be provided in the textfield on the right-hand side.

#### OpenVPN server instances

The list of already defined OpenVPN instances is shown in this panel, above which is present the *Add new OpenVPN server instance* byperlink. A click on this link will open an editor in which to provide all the necessary configuration values for a new VPN instance.

#### Note

When the number of OpenVPN instances is greater than the cores, a yellow callout informs that the performances may degrade.

In the editor, the following configuration options are shown.

#### Name

The name given to the OpenVPN server instance.

#### Remark

A comment for this instance.

#### Bind only to

The IP address to which the instance should listen to.

#### Port

The port on which the instance waits for incoming connections.

#### Device type

The device used by the instance, chosen between TUN and TAP from the drop-down menu. TUN devices require that the traffic be routed, hence the option *Bridged* below is not available for TUN devices.

#### *Protocol*

The protocol used, chosen between TCP and UDP from the drop-down menu.

#### *Bridged*

Tick this option to run the OpenVPN server in bridged mode, i.e., within one of the existing zones.

#### *Note*

If the OpenVPN server is not bridged (i.e., it is routed), the clients will receive their IP addresses from a dedicated subnet. In this case, appropriate firewall rules in the [VPN firewall](#) should be created, to make sure the clients can access any zone or some server/resource (e.g., a source code repository). If the OpenVPN server is bridged, it inherits the firewall settings of the zone it is defined in.

#### *VPN subnet*

This option is the only available if bridged mode is disabled. It allows the OpenVPN server to run in its own, dedicated subnet, that can be specified in the text box and should be different from the subnets of the other zones.

#### *Bridge to*

The zone to which the OpenVPN server should be bridged. The drop-down menu shows only the available zones.

#### *Dynamic IP pool start address*

The first possible IP address in the network of the selected zone that should be used for the OpenVPN clients.

#### *Dynamic IP pool end address*

The last possible IP address in the network of the selected zone that should be used for the OpenVPN clients.

Routed and bridged OpenVPN server, static and dynamic.

When configuring a pool of IP addresses to be reserved for clients connecting via OpenVPN, it is necessary to keep in mind a few guidelines that help both the prevention of future malfunctioning and the cleaner and easier design and set up.

Before starting the configuration of the server, there is a golden rule to remember, concerning the implementation of the VPN multicore architecture: Regardless of the bridged or routed mode used for a multicore VPN server instance, the reservation of static IP addresses is neglected. In other words, a client connecting to this VPN server, will receive a dynamic IP address, even though in her configuration there is a static IP assignment.

The first choice is to define whether the OpenVPN server should act in routed or bridged mode. In the former case, it is necessary to define a suitable *VPN subnet* that will provide the IP addresses for the clients. The traffic directed to this subnet has to be filtered, if necessary, using the VPN firewall. In the latter case, the OpenVPN server is configured to consider the clients, upon connecting, as they were physically connected to that zone, i.e., the server *bridges* the client to one of the zones. In this case, a pool of IP addresses must be defined within that zone using the two option that appear right before this box. This pool must be entirely contained in the zone's subnet and smaller than that one. It is also important to make sure that this pool does **conflict** with other pools defined in that zone, like e.g., a DHCP server.

In a bridged OpenVPN server it is possible to assign to some (or even to all) user a static IP address. When planning this possibility, it is a good practice that these static IP addresses do not belong to any of the IP pools defined in that zone, to prevent any conflicts of address and wrong routing. Traffic to this particular client can then be filtered using the VPN (or IPsec) user as source or destination of traffic in the Firewall rules.

In the **Advanced options** box, additional options can be configured.

#### *Number of cores*

The drop-down menu allows to chose how many CPUs of the Panda Gatedefender Appliance can be used by the instance, hence the options in the drop-down menu may vary.

#### *Allow multiple connections from one account:*

Normally, one client is allowed to connect from one location at a time. Selecting this option permits multiple client logins, even from different locations. However, when the same client is connect twice or more, the VPN firewall rules do not apply anymore.

#### *Block DHCP responses coming from tunnel*

Tick this checkbox when receiving DHCP responses from the LAN at the other side of the VPN tunnel that conflict with the local DHCP server.

#### *Client to client connections*

Select from the drop-down menu the modalities of the communications between clients of the OpenVPN server:

- **Not allowed:** The clients can not communicate one to the other.
- **Allow direct connections:** The clients can connect. This option is only available on single-core CPUs.
- **Filter connections in the VPN firewall** The clients can communicate each other, but their traffic is governed by the VPN Firewall.

#### *Push these nameservers*

By ticking this checkbox, the nameserver specified in the textfield below are sent to the clients upon connection.

#### *Nameservers*

The nameservers specified in this textfield are sent to the connected clients, when the previous checkbox has been ticked.

#### *Push these networks*

By ticking this checkbox, the routes to the networks defined in the textfield below are sent to the connected clients.

#### *Networks*

The networks specified in this textfield are sent to the connected clients, when the previous checkbox has been ticked.

#### *Push this domain*

By ticking this checkbox, the search domain defined in the textfield on the right-hand side, is added to those of the connected clients.

#### *Domain*

The domain that will be used to identify the servers and network resources in the VPN network (i.e., the *search domain*).

#### **Note**

The options *Push these nameservers* and *Push domain* only work for clients running the Microsoft Windows operating system.

The first time the service is started a new, self-signed CA certificate for this OpenVPN server is generated, an operation that may take a long time. After the certificate has been generated, it can be downloaded by clicking on the *Download CA certificate* link. This certificate must be used by all the clients that want to connect to this OpenVPN server, otherwise they will not be able to access.

After the server has been set up, it is possible to create and configure accounts for clients that can connect to the Panda Gatedefender Appliance in the *Authentication* tab.

#### *Enabled*

Tick this checkbox to make sure the OpenVPN server is started.

#### Troubleshooting VPN connections.

While several problem with VPN connections can be easily spotted by looking at the configuration, one subtle source of connections hiccups is a wrong value of the MTU size. The Panda Gatedefender Appliance sets a limit of 1450 bytes to the size of the VPN's MTU, to prevent problems with the common MTU value used by the ISP, which is 1500. However, some ISP may use a MTU value lower than the commonly used value, making the Panda MTU value too large and causing therefore connection issues (the most visible one is probably the impossibility to download large files). This value can be modified by accessing the Panda Gatedefender Appliance from the CLI and following these guidelines:

1. Write down the MTU size used by the ISP (see link below).
2. Login to the CLI, either from a shell or from Menubar > System > Web Console.
3. Edit the OpenVPN template with an editor of choice: **nano /etc/openvpn/openvpn.conf.tmpl**.
4. Search for the string **mssfix 1450**.
5. Replace 1450 with a lower value, for example 1200.
6. Restart OpenVPN by calling: **jobcontrol restart openvpnjob**.

See also

More information about [the MTU size](#).

# Authentication

This page shows three tabs, which allow to manage local *Users*, local *Groups*, and *Settings* for remote authentication

## Users

In this page, all users that have an account on the Panda Gatedefender Appliance's VPN server are displayed in the table, and for each the following information are shown:

- Name. The name of the user.
- Remark. A comment.
- Authentication server. The server used for the user authentication, which is either *local* (the Panda Gatedefender Appliance itself) or *LDAP* (an external LDAP server, configurable in the [Settings](#) tab).
- Actions. The available operation that can be carried out on the account. For LDAP users they are *Enable/Disable* and *Edit*, for local users, there is also the possibility to *Delete*. Editing an LDAP user only allows to modify its local options, not of other data like username or password, which are entirely managed by the LDAP server.

Click on *Add new local user* above the table to add a new local account. In the form that will show up, the following options can be specified for each user.

### Add new local user

#### *Username*

The login name of the user

#### *Remark*

An additional comment.

#### *Password, Confirm password*

The password for the user, to be entered twice. The passwords are actually not shown: To see them, tick the two checkboxes on their right.

#### *Certificate configuration*

Select the mode to assign a certificate to the user. The available modes are selectable from the drop-down menu: *Generate a new certificate*, *Upload a certificate*, and *Upload a Certificate signing request*. Upon selection, below the drop-down menu appear the available options for each mode, which are described in the [Certificates](#) page.

#### *Organizational unit name*

The Organisation Unit to which the user belongs to, i.e., the company, enterprise, or institution department identified with the certificate.

#### *Organization name*

The organisation to which the user belongs to.

#### *City*

The city (L) in which the organisation is located.

#### *State or province*

The state or province (ST) in which the organisation is located.

#### *Country*

The Country (C) in which the organisation is located, chosen from those in the selection menu. By typing one or more letters, matching countries are searched for and displayed.

#### *Email address*

The e-mail address of the user.

#### *Group membership*

In this part of the panel it is possible to assign membership to one or more groups to the user. In the search widget it is possible to filter existing groups to find matching groups. Group membership is added by clicking on the + on the right of the group name. Groups to which the user belongs are show in the textfield below. There are also shortcuts to *Add all* and to *Remove all* groups memberships at once.

### *Override OpenVPN options*

Tick this checkbox to allow the OpenVPN protocol to be used. This option will reveal a box in which to specify custom option for the account, see below.

### *Override L2TP options*

Tick this checkbox to show a box in which to choose the L2TP tunnel to be used.

#### Note

This option can not be selected if no L2TP tunnel has yet been configured. In such a case, an informative message appears as a hyperlink: Upon clicking on it, the IPsec connection editor opens. Once done, it will be possible to allow a VPN user to connect using the L2TP Protocol.

#### Hint

The box for L2TP options will appear below the *OpenVPN options* box, if also OpenVPN option are to be overridden

### *Enabled*

Tick the checkbox to enable the user, i.e., to allow her to connect to the OpenVPN server on the Panda Gatedefender Appliance.

### **OpenVPN Options**

#### *direct all client traffic through the VPN server*

If this option is checked, all the traffic from the connecting client, regardless of the destination, is routed through the uplink of the Panda Gatedefender Appliance. The default is to route all the traffic whose destination is outside any of the internal zones (such as Internet hosts) through the client's uplink.

#### *Push only global options to this client*

For advanced users only. Normally, when a client connects, tunnelled routes to networks that are accessible via VPN are added to the client's routing table, to allow it to connect to the various local networks reachable from the Panda Gatedefender Appliance. This option should be enabled if this behaviour is not wanted, but the client's routing tables (especially those for the internal zones) should be modified manually.

#### *Push route to GREEN [BLUE, ORANGE] zone,*

When this option is active, the client will have access to the GREEN, BLUE, or ORANGE zone. These options have no effect if the corresponding zones are not enabled.

#### *Networks behind client*

This option is only needed if this account is used as a client in a Gateway-to-Gateway setup. In the box should be written the networks laying behind this client that should be pushed to the other clients. In other words, these networks will be available to the other clients.

#### *Static IP addresses*

Dynamic IP addresses are assigned to clients, but a static IP address provided here will be assigned to the client whenever it connects.

#### Note

If the client connects to a multicore VPN server running on the Panda Gatedefender Appliance, this assignment will not be taken into account.

#### *Push these nameservers*

Assign custom nameservers on a per-client basis here. This setting (and the next one) can be defined, but enabled or disabled at will.

#### *Push these domains*

Assign custom search domains on a per-client basis here.

#### Note

When planning to have two or more branch offices connected through a Gateway-to-Gateway VPN, it is good practice 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`. Using this solution, several possible sources for errors and conflicts will be avoided. Indeed, several advantages come for free, including: The automatic assignment of correct routes, without the need for pushing custom routes, no warning messages about possibly conflicting routes, correct local name resolution, and easier WAN network setup.

## L2TP Options

### *IPsec Tunnel*

This drop-down menu allows to choose the tunnel that will be employed by the user, among those already defined.

## Groups

In this page a table is displayed, which shows all the groups that are either defined on the Panda Gatedefender Appliance or on an external LDAP server. For each group the following information are shown:

- Groupname. The name of the group.
- Remark. A comment.
- Authentication server. The server used for the user authentication, which is either *local* (the Panda Gatedefender Appliance itself) or *LDAP* (an external LDAP server, configurable in the *vpnauthsettings* tab).
- Actions. The available operation that can be carried out on the account. For LDAP servers the only action is to *Edit* the local properties, while for local groups there is also the possibility to *Delete* the group.

Click on *Add new local groups* above the table to add a new local group. In the form that will show up, the following options can be specified for each group.

### *Group Name*

The name given to the group.

### *Remark*

A comment.

### *Users*

In this part of the panel it is possible to assign users to the group. In the search widget it is possible to filter existing local users to find matching users. Users are added to the group by clicking on the + on the right of the username. Users in the Group are shown in the textfield below. There are also shortcuts to *Add all* and to *Remove all* users to/from a group.

### *Override OpenVPN options*

Tick this checkbox to allow the OpenVPN protocol to be used. This option will reveal a box in which to specify custom options for the account, which are the same as those specified for the [local users](#).

### *Override L2TP options*

Tick this checkbox to show a box in which to choose the L2TP tunnel to be used from a drop-down menu.

### Note

This option can not be selected if no L2TP tunnel has yet been configured. In such a case, an informative message appears as a hyperlink: Upon clicking on it, the IPsec connection editor opens. Once created a new L2TP tunnel, it will be possible to associate it to a user.

### Hint

The box for L2TP options will appear below the *OpenVPN options* box, if also OpenVPN options are to be overridden

### *Enabled*

Tick the checkbox to enable the user, i.e., to allow her to connect to the OpenVPN server on the Panda Gatedefender Appliance.

### Warning

While the same user can be legally part of one or more groups, care must be taken that the groups the user belongs to do not define contrasting *override* options. As an example, consider a user member of two groups, one allowing access only to the GREEN zone, and one only to the BLUE. In this case, it is not easy to predict whether that user will be granted or not access to the BLUE or GREEN zone. The management of these issues is left to the manager of the OpenVPN server.



## Settings

This page contains the current configuration of the authentication servers on which the Panda Gatedefender Appliance relies and allows for their management. Currently, only local and LDAP / Active Directory are supported, though in future releases additional types of authentication server might be added, like e.g. Radius servers.

There are two tables in this page, one displaying information about *Authentication servers*, and one showing *Authentication server mappings*. In the former, those information is shown:

- Name. The name given to the server
- Type. Whether the server is a local or an external LDAP one.
- Service. Which authentication is available for that server.
- Actions. For local authentication, it is possible to *enable/disable* the server, to *edit* it, or to delete it. For LDAP servers there is also the ability to *refresh* the connection, for synchronising the users and groups.

The table at the bottom shows the correspondences between a service (IPsec XAuth, OpenVPN, and L2TP) and the type of authentication allowed. The only *Actions* for the mappings is to *Edit* them. By clicking on *Edit*, a form will appear, in which a selector allows to select which authentication backends will be used for that service.

A click on the *Add new authentication server* link above the tables opens a form in which to supply all data to set up a new authentication server.

This form replaces the tables displaying the already defined authentication servers and allows to configure a new one, by specifying appropriate values for the following configuration options.

### *Name*

The name given to the authentication server.

### *Enabled*

Tick the checkbox to enable the server.

### *Type*

Select from the drop-down menu whether the server shall be *LDAP / Active directory* or *local*. All the next options, except for the last one, are available only for the configuration of LDAP servers.

### *LDAP server URI*

The URI of the LDAP server.

### *LDAP server type*

This drop-down menu allows the choice of the type of the authentication server among *Generic*, *Active Directory*, *Novell eDirectory*, or *OpenLDAP*.

### *LDAP bind DN username*

The fully distinguished name of the bind DN user, which must have the permission to read user attributes

### *LDAP bind DN password*

The password of the bind DN user.




The following options depend on the server's setup and are used to identify which users and groups shall be granted access to Panda Gatedefender Appliance's OpenVPN server: *LDAP user base DN*, *LDAP user search filter*, *LDAP user unique ID attribute*, *LDAP group base DN*, *LDAP group unique ID attribute*, *LDAP group member attribute*, *LDAP group search filter*

### *Limit to specified groups*

This option allows to select which groups on the LDAP server are allowed to connect to the Panda Gatedefender Appliance's OpenVPN server.

## OpenVPN client (Gw2Gw)

In this page appears the list of the Panda Gatedefender Appliance's connections as OpenVPN clients, i.e., all tunnelled connections to remote OpenVPN servers. For every connection, the list reports the status, the name, any additional option, a remark, and the actions available:

-   - the server is active or stopped.
-  - modify the server's configuration
-  - remove the configuration and the server.

The status is *closed* when the connection is disabled, *established* when the connection is enabled, and *connecting...* while the connection is being established. Beside to enable and to disable a connection, the available actions are to edit or delete it. In the former case, a form will open, that is the same as the one that opens when adding a connection (see below) in which to see and modify the current settings, whereas in the latter case only deletion of that profile from the Panda Gatedefender Appliance is permitted.

The creation of a new OpenVPN client connections is straightforward and can be done in two ways: Either click on the *Add tunnel configuration* button and enter the necessary information about the OpenVPN server to which to connect (there can be more than one) or import the client settings from the OpenVPN Access Server by clicking on *Import profile from OpenVPN Access Server*.

### Add tunnel configuration

There are two types of settings that can be configured for each tunnel configuration: The basic one includes mandatory options for the tunnel to be established, while the advanced one is optional and normally should be changed only if the OpenVPN server has a non-standard setup. To access the advanced settings, click on the >> button next to the *Advanced tunnel configuration* label. The basic settings are:

#### Connection name

A label to identify the connection.

#### Connect to

The remote OpenVPN server's FQDN, port, and protocol in the form

`myvpn.example.com:port:protocol`. The port and protocol are optional and left on their default values which are *1194* and *udp* respectively when not specified. The protocol must be specified in lowercase letters.

#### Upload certificate

The server certificate needed for the tunnel connection. Browsing the local filesystem is admitted, to search for the file, of the path and filename can be entered. If the server is configured to use PSK authentication (password/username), the server's host certificate (i.e., the one downloaded from the *Download CA certificate* link in the server's Menubar › VPN › OpenVPN server section) must be uploaded to the Panda Gatedefender Appliance. Otherwise, to use certificate-based authentication, the server's PKCS#12 file (i.e., the one downloaded from the *Export CA as PKCS#12 file* link on the server's Menubar › VPN › OpenVPN server › Advanced section) must be uploaded.

#### PKCS#12 challenge password

Insert here the *Challenge password*, if one was supplied to the CA before or during the creation of the certificate. This is only needed when uploading a PKCS#12 certificate.

#### Username, Password

If the server is configured to use PSK authentication (password/username) or certificate plus password authentication, provide here the username and password of the account on the OpenVPN server.

#### Remark

A comment on the connection.

### Advanced tunnel configuration

In this box, that appears when clicking on the >> button in the previous box, additional options can be modified, though the values in this box should be modified only if the server side has not been configured with standard values.

#### Fallback VPN servers

One or more (one per line) fallback OpenVPN servers in the same format used for the primary server, i.e., `myvpn.example.com:port:protocol`. The port and protocol values default to *1194* and *udp* respectively when omitted. If the connection to the main server fails, one of these fallback servers will take over.

Hint

The protocol must be written in lowercase letters.

#### Device type

The device used by the server, which is either TAP or TUN.

### *Connection type*

This drop-down menu is not available if TUN has been selected as *Device type*, because in this case the connection type is always *routed*. Available options are *routed* (i.e., the client acts as a gateway to the remote LAN) or *bridged* (i.e., the client firewall appears as part of the remote LAN). Default is *routed*.

### *Bridge to*

This field is only available if TAP has been selected as *Device type* and the *connection type* is *bridged*. From this drop-down menu, select the zone to which this client connection should be bridged.

### *NAT*

This option is only available if the *Connection type* is *routed*. Tick this checkbox to hide the clients connected through this Panda Gatedefender Appliance behind the firewall's VPN IP address. This configuration will prevent incoming connections requests to the clients. In other words, incoming connections will not see the clients in the local network.

### *Block DHCP responses coming from tunnel*

Tick this checkbox to avoid receiving DHCP responses from the LAN at the other side of the VPN tunnel that conflict with a local DHCP server.

### *Use LZO compression*

Compress the traffic passing through the tunnel, enabled by default.

### *Protocol*

The protocol used by the server: UDP (default) or TCP. Set to TCP only if an HTTP proxy should be used: In this case, a form will show up to configure it.

If the Panda Gatedefender Appliance can access the Internet only through an upstream HTTP proxy, it can still be used as an OpenVPN client in a Gateway-to-Gateway setup, but the *TCP* protocol for OpenVPN must be selected on both sides. Moreover, the account information for the HTTP upstream proxy must be provided in the text fields:

### *HTTP proxy*

The HTTP proxy host, e.g., `proxy.example.com:port`, with the port defaulting to 8080 if not entered.

### *Proxy username, Proxy password*

The proxy account information: The username and the password.

### *Forge proxy user-agent*

A forged *user agent* string can be used in some cases to disguise the Panda Gatedefender Appliance as a regular web browser, i.e., to contact the proxy as a browser. This operation may prove useful if the proxy accepts connections only for some type of browsers.

Once the connection has been configured, a new box at the bottom of the page will appear, called *TLS authentication*, from which to upload a TLS key file to be used for the connection. These options are available:

### *TLS key file*

The key file to upload, searchable on the local workstation.

### *MD5*

The MD5 checksum of the uploaded file, which will appear as soon as the file has been stored on the Panda Gatedefender Appliance.

### *Direction*

This value is set to 0 on servers and to 1 on clients.

### **Import profile from OpenVPN Access Server**

The second possibility to add an account is to directly import the profile from an OpenVPN Access Server: In this case, the following information must be provided:

### *Connection name*

A custom name for the connection.

### *Access Server URL*

The URL of the OpenVPN Access Server.

#### Note

Note that the Panda Gatedefender Appliance only supports XML-RPC configuration of the OpenVPN Access Server, therefore a URL input here has the form: `https://<SERVERNAME>/RPC2`.

#### Username, Password

The username and password on the Access Server.

#### Verify SSL certificate

If this checkbox is ticked and the server is running on an SSL encrypted connection, then the SSL certificate will be checked for validity. Should the certificate not be valid then the connection will be immediately closed. This feature might be disabled when using a self-signed certificate.



#### Remark

A comment to recall the purpose of the connection.

## IPsec

The IPsec page contains two tabs (IPsec and L2TP), that allow to set up and configure the IPsec tunnels and to enable the L2TP support, respectively.

### IPsec

To enable L2TP on the Panda Gatedefender Appliance, the switch next to the *Enable L2TP* label should be green . If it is grey  click on it to start the service.

The IPsec tab contains two boxes: The first one is *IPsec settings*, which concerns the certificate choice and various options, also for debugging purposes. The second one is *Connections*, which shows all the connections and allows to manage them.

IPsec, L2TP, and XAuth in a nutshell.

IPsec is a generic standardised VPN solution, in which the encryption and the authentication tasks are carried out on the OSI layer 3 as an extension to the IP protocol. Therefore, IPsec must be implemented in the kernel's IP stack. Although IPsec is a standardised protocol and it is compatible to most vendors that implement IPsec solutions, the actual implementation may be very different from vendor to vendor, sometimes causing interoperability issues.

Moreover, the configuration and administration of IPsec may become quite difficult due to its complexity and design, while some particular situations might even be impossible to handle, for example when there is the necessity to cope with NAT.

Compared to IPsec, OpenVPN is easier to install, configure, and manage. However, mobile devices rely on IPsec, thus the Panda Gatedefender Appliance implements an easy-to-use administration interface for IPsec, that supports different authentication methods and also two-factor authentication when used together with L2TP or XAuth.

Indeed, IPsec is used to authenticate clients (i.e., tunnels) but not users, so one tunnel can be used by only one client at a time.

L2TP and XAuth add user authentication to IPsec, therefore many clients can connect to the server using the same encrypted tunnel and each client is authenticated by either L2TP or XAuth.

An additional option is available when using XAuth and is called *XAuth hybrid* mode, which only authenticates the user.

#### IPsec settings

In this box a few global IPsec options can be set, namely two for Dead peer detection, and quite a lot debugging options. Additionally, configuration of certificates used in IPsec tunnelled connections is also carried out here.

#### Roadwarriors virtual IP pool

The IP interval from which all roadwarrior connections receive their IP address.

#### Ping delay (in seconds)

The amount of seconds between two successive pings, used to detect whether the connection is still active.

#### Timeout interval (in seconds) - IKEv1 only

The maximum amount in seconds of the exchange interval for the IKEv1 protocol.

Hint

IKEv2 does not need a timeout interval, as it is capable of detecting when the other endpoint does not reply and which actions to take.

#### *Certificate configuration*






Certificate configuration and management is carried out exactly like in the case of OpenVPN server (in Menubar › VPN › OpenVPN server), in which all the various management modalities are explained.

#### **Debug options**

Debug options are rather advanced settings and usually not needed, as they only will increase the number of events and messages recorded in the log file.

#### **Connections**

In this table are shown all the already configured IPsec connection, with the following information:

- Name. The name given to the connection.
- Type. What kind of tunnel is used.
- Common Name. The name of the certificate used to authenticate the connection.
- Remark. A comment about the connection.
- Status. Whether the connection is either *Closed*, *Connecting* or *Established*.
- Actions. The possible operations that can be made on each tunnel:
  -  - the connection is active or not.
  -  - modify the connection's configuration
  -  - restart the connection.
  -  - display detailed information about the connection.
  -  - remove the connection.

Hint

When a connection is reset from the Panda Gatedefender Appliance, it is necessary for the client to reconnect in order to establish the connection.

Upon clicking on *Add new Connection*, a panel will appear, which contains all options needed to set up a new IPsec connection.

#### *Name*

The name of the connection.

#### *Remark*

A comment for the connection.

#### *Connection type*

There are four different connection modalities can be chosen for the IPsec tunnel:

- *Host-to-Net*. The client is connecting to the IPsec server on the Panda Gatedefender Appliance is a single remote workstation, server, or resource.
- *Net-to-Net*. The client is an entire subnet. In other words, the IPsec connection is established between remote subnets.
- *L2TP Host-to-Net*. The client is a single device, using also L2TP.
- *XAuth Host-to-Net*. The client is a single device and authentication is carried out by XAuth.

Hint

Linux users can read more about XAuth by reading the Xsecurity(7) manpage, also available [online](#) for everyone.

The options available for each of them are basically same, with only one more option available for Net-to-Net connections.

#### *Authentication Type*

The option selected from the drop-down menu determines how the client's authentication is carried out. Available values are:

- *Password (PSK).* The client shall supply the password specified in the *Use a pre-shared key* textfield situated on the right.
- *Peer is identified by either IPV4\_ADDR, FQDN, USER\_FQDN or DER\_ASN1\_DN string in remote ID field.* The client is authenticated by its IP Address, domain name, or by other unique information of the IPsec tunnel.
- *Use an existing certificate.* The certificate chosen from the drop-down menu on the right shall be used.
- *Generate a new certificate.* Additional options will be shown to create a new certificate.
- *Upload a certificate.* Select from the local workstation a certificate to use.
- *Upload a certificate request.* Select from the local workstation a certificate request to obtain a new certificate.
- *XAUTH hybrid.* Only available for *XAuth Host-to-Net* connections: The user will authenticate, while the encryption tunnel must not.

#### *Local ID*

A string that identifies the client within the local network.

#### *Interface*

The interface through which the host is connecting.

#### *Local subnets*

The local subnets that will be accessible from the client.

#### *Note*

Mobile devices running iOS can not properly connect via XAuth to the Panda Gatedefender Appliance if this value is not set, therefore the special subnet *0.0.0.0/0* is automatically added when the *Connection type* is set to XAuth.

#### *Hint*

Only when using IKEv2 it is possible to add more than one subnet, one per line, since IKEv1 only supports one subnet.

#### *Remote ID*

The ID that identifies the remote host of the connection.

#### *Remote subnet*

Only available for Net-to-Net connections, it specifies the remote subnet.

#### *Hint*

When using IKEv2 it is possible to add more than one subnet.

#### *Remote host/IP*

The IP or FQDN of the remote host.

#### *Note*

When a hostname is supplied in this option, it must match the *local ID* of the remote side.

#### *Roadwarrior virtual IP*

The IP Address specified in the textfield will be assigned to the remote client.

#### *Hint*

This IP Address must fall within the pool defined in the [IPsec settings](#) below.

#### *Note*

This option is available neither for L2TP Host-to-Net connections, as it is L2TP that takes charge of IP address assignment to clients, nor for Net-to-Net connections.

#### *Dead peer detection action*

The action to perform if a peer disconnects. Available choices from the drop-down menu are to *Clear*, to *Hold*, or to *Restart* the peer.

By clicking on the *Advanced* label, additional options are available, to choose and configure different types of encryption algorithm. For every option, many types of algorithm can be chosen.

#### *Note*

It is necessary to change algorithm only in case some remote client uses a given algorithm and can not change it.

### *IKE encryption*

The encryption methods that should be supported by IKE.

### *IKE integrity*

The algorithms that should be supported to verify the integrity of packets.

### *IKE group type*

The IKE group type.

### *IKE lifetime*

How many hours are the IKE packets valid.

### *ESP encryption*

The encryption methods that should be supported by the ESP.

### *ESP integrity*

The algorithms that should be supported to verify the integrity of packets.

### *ESP group type*

The ESP group type.

### *ESP lifetime*

How many hours should an ESP key be valid.

### *Negotiate payload compression*

Tick the checkbox to allow payload compression.

See also

IKE is defined in [RFC 5996](#), which also supersedes the older [RFC 2409](#) (IKEv1) and [RFC 4306](#) (IKEv2).

ESP is described in [RFC 4303](#) (ESP) and [RFC 4305](#) (encryption algorithms for ESP).

How to create a Net-To-Net VPN with IPsec using certificate authentication.

Scenario:

- Firewall CoreFW - REDIP: 100.100.100.100, GREENIP: 10.10.10.1/24
- Firewall LocalFW - REDIP: 200.200.200.200, GREENIP: 192.168.0.1/24

Problem: Connect LocalFW to CoreFW using IPsec.

Solution:

- The following steps have to be performed on CoreFW:
  1. Go to Menubar › VPN › IPsec, enable IPsec, and specify 100.100.100.100 as Local VPN hostname/IP.
  2. After saving, click on the *Generate host/root certificate* button, unless they have already been generated, and compile the form.
  3. Download the host certificate and save it as **fw\_a\_cert.pem**.
  4. In the *Connection status and control* box click on the *Add* button, then select *Net-to-Net*. In the page that opens, two box will appear.
  5. In *Connection configuration* enter 200.200.200.200 in the *Remote host/IP* field, 10.10.10.0/24 as *Local subnet* and 192.168.0.0/24 as *Remote subnet*.
  6. In the *Authentication* box select *Generate a certificate* and compile the form. Make sure to set a password.
  7. After saving, download the PKCS12 file and save it as **fw\_a.p12**.
- The following steps have to be performed on LocalFW:
  1. Go to Menubar › VPN › IPsec, enable IPsec, and specify 200.200.200.200 as Local VPN hostname/IP.
  2. After saving click on the *Generate host/root certificate* button. If they had already been generated, *Reset* the previous certificates.

3. In the *Generate host/root certificate*, **Do not** fill in any field in the first section! Instead, upload the **fw\_a.p12** file saved from CoreFW, enter the password, and click on the *Upload PKCS12 file*.
4. Click on *Add* in the *Connection status and control* box, then select *Net-to-Net*. In the page that opens, two box will appear.
5. In *Connection configuration* enter 100.100.100.100 in the *Remote host/IP* field, 192.168.0.0/24 as *Local subnet* and 10.10.10.0/24 as *Remote subnet*.
6. In the *Authentication* box select *Upload a certificate* and upload the **fw\_a\_cert.pem** that have created on MainFW.

## L2TP

L2TP, the Layer 2 Tunnelling Protocol, is described in [RFC 2661](#).

To enable L2TP on the Panda Gatedefender Appliance, the switch next to the *Enable L2TP* label should be green. If it is grey, click on it to start the service.

The following options are available to configure L2TP.

### Zone

The zone to which the L2TP connections are directed. Only the activated zones can be chosen from the drop-down menu.

### L2TP IP pool start address, L2TP IP pool end address

The IP range from which L2TP users will receive an IP address when connecting to the Panda Gatedefender Appliance.

### Enable debug






Tick this checkbox to let L2TP produce more verbose logs.

## Certificates

The *Certificates* page allows the management of the certificates that are needed by the various OpenVPN server instances running on the Panda Gatedefender Appliance and is composed of three tabs: *Certificates*, *Certificate Authority*, and *Revoked Certificates*.

### Certificates

Here it is possible to manage all the certificates stored on the Panda Gatedefender Appliance. The table, initially empty, shows all certificates along with the following details, one per each column:

- *Serial*. A unique number identifying the certificate.
- *Name*. The name assigned to the certificate.
- *Subject*. the collection of information that identify the certificate. itself. See the options below.
- *Expiration Date*. The final date of validity of the certificate.
- *Actions*. What can be done with the certificate:
  -  - to show all its details.
  -  - to download it in PEM format.
  -  - to download it in PKCS12 format.
  -  - to delete the private key associated to it.
  -  - revoke the certificate.

Above the list, a link can be clicked to *Add new certificate*. Upon clicking, the page will be replaced by a form that allows to provide all data necessary to the generation of a new certificate.

At the bottom of the table, on the left-hand side there is a navigation widget, that allows to navigate among the various pages composing the table, if there are many certificates, whereas on the right-hand side there is a reload widget, used to refresh the list of certificates.

### Add new certificate

Three alternatives are available to store a new certificate on the Panda Gatedefender Appliance, selectable from this drop-down menu: *Generate a new certificate*, *Upload a certificate*, and *Upload a Certificate signing request*.



### **Generate a new certificate**

The first alternative allows to create a new certificate directly on the Panda Gatedefender Appliance, by providing the following information. The capital letters in parentheses show the field of the certificate that will be filled by the value supplied and form the *Subject* of the certificate.

#### Note

A Root Certificate Authority is needed to create certificates, so create the Root CA before creating certificates.

#### *Common name*

The common name (CN) of the certificate's owner, i.e., the name with which the owner will be identified.

#### *Email address*

The e-mail address of the certificate's owner.

#### *Organizational unit name*

The Organisation Unit (OU) to which the owner belongs to, i.e., the company, enterprise, or institution department identified with the certificate.

#### *Organization name*

The organisation (O) to which the owner belongs to.

#### *City*

The city (L) in which the organisation is located.

#### *State or province*

The state or province (ST) in which the organisation is located.

#### *Country*

The Country (C) in which the organisation is located, chosen from those in the selection menu. By typing one or more letters, matching countries are searched for and displayed.

#### *Subject alt name (subjectAltName=email:\*,URI:\*,DNS:\*,RID:\*)*

An alternate name for the subject, i.e., the certificate.

#### *Certificate type*

The type of the certificate, chosen between *Client* and *Server* from the drop-down menu.

#### *Validity (days)*

The number of days before the certificate expires.

#### *PKCS12 file password*

The password for the certificate, if needed.

#### *PKCS12 file password Confirmation*

Type once more the certificate's password for confirmation.

### **Upload a certificate**

The next alternative is to upload an existing certificate from the local workstation to the Panda Gatedefender Appliance.

#### *Certificate (PKCS12/PEM)*

By clicking on the *Browse* button or on the textfield, a file chooser will open, in which to supply the path to the certificate to be uploaded.

#### *PKCS12 file password*

The password for the certificate, if needed.

### **Upload a certificate signing request**

The third alternative is to upload a CSR from the local workstation to the Panda Gatedefender Appliance, i.e., an encrypted text file containing all necessary information to generate a new certificate, recognised by the server.

#### *Certificate Signing Request (CSR)*

By clicking on the *Browse* button or on the textfield, a file chooser will open, in which to supply the path to the CSR to be uploaded.




#### *Validity (days)*

How many days shall the certificate be valid.

## Certificate Authority

This page allows to manage the CA, which are necessary for the correct working of an OpenVPN encrypted connection. There are two ways to add a CA: Either by clicking on the link above the table of already existent certificates to generate a new certificate, or by uploading one using the widgets below the table.

The table, once populated, shows the same information as in the *Certificates* tab, with the only difference in the *Actions* available, which are:

-  - to show all CA details.
-  - to download it in PEM format.
-  - to delete the certificate.

To upload a certificate, supply the following information:

### *CA name*

The name of the Authority who created the certificate.

### *Certificate (PEM)*

By clicking on the *Browse* button or on the textfield, a file chooser will open, in which to supply the path to the certificate to be uploaded.

Clicking on the *Upload CA certificate* will start the upload process.

### **Generate new root/host certificates**

This procedure can be applied only once and will generate two certificates: A root certificate authority and a host certificate, with the latter that shall appear in the list shown in the *Certificates* tab. When clicking on the link, a form will replace the list, in which to supply the following data, that will be used in the new root and host certificates.

### Note

The only way to generate a new root certificate is to delete the existing one.

### *System hostname*

The name of the system, that will be used as the certificate's Common Name.

### *Email address*

The e-mail address of the system's owner or responsible.

### *Organizational unit name*

The Organisation Unit (OU) to which the system belongs to.

### *Organization name*

The organisation (O) to which the system belongs to.

### *City*

The city (L) in which the organisation is located.

### *State or province*

The state or province (ST) in which the organisation is located.

### *Country*

The Country (C) in which the organisation is located, chosen from those in the selection menu. By typing one or more letters, matching countries are searched for and displayed.

### *Subject alt name (subjectAltName=email:\*,URI:\*,DNS:\*,RID:\*)*

An alternate name for the subject, i.e., the certificate.

### *Validity (days)*

The number of days before the certificate expires.

## Revoked Certificates

The certificates that have been revoked are listed in the table, that show the serial number and the subject of the certificate.



*Download the Certificate Revocation List*

A click on this link will allow to download the on a local workstation the Certificate Revocation List.

## Certificate Revocation List

In this page can be managed all the Certificate Revocation lists that have been uploaded.

The table shows all the Certificate Revocation Lists that have been uploaded and for each item in the table are show the name of the certificate, the issuer, and the issued date. Available actions are:

-  - display the certificate details
-  - download the certificate on the local workstation.

# 9. The Hotspot Menu

---

The hotspot shipped with the Panda Gatedefender Appliance is a highly flexible and customisable solution to provide secure and reliable wireless connection as well as for wired LAN connections. The key features implemented in the hotspot include:

- three roles for the hotspot: it can work as a standalone hotspot, in a master-satellite configuration, or relying on an external RADIUS server
- three types of users: hotspot administrators (full administration access), account-editors (some user management), and normal users (only Internet navigation)
- different types of tickets: time-based vs. data-based, pre-paid vs. post-paid access
- three different access portals for users: normal mode, no-JavaScript, and mobile
- the option to add a customised background page seen by all users
- a SmartConnect™ option to allow a user to buy access with credit card
- user creation and activation via SMS.
- option to allow certain web sites to be accessed even without tickets.

In the Panda Gatedefender Appliance, the BLUE zone is dedicated to the wireless devices, therefore the hotspot does not work if the BLUE zone is disabled. The connections from the BLUE zone to the RED one (uplink, i.e., the Internet) are governed by the [outgoing firewall](#), hence to selectively allow access to the Internet, appropriate rules shall be defined there.

Upon entering the Hotspot, a page will open that contains three items in the left-hand side sub-menu, an *Enable hotspot* switch, and the first configuration option: The operating role of the hotspot.

The left-hand side menu items give access to various configuration and management options for the Hotspot Settings, Administration Interface, and Hotspot User respectively :



Hotspot Settings is the starting hotspot's page, e.g., the you are currently in, and allows to choose the modality of the hotspot.

Administration Interface is the main part of the hotspot, where all the administrative tasks can be accomplished.

Hotspot User allows the management of the hotspot's superusers

Moreover, Client Access to the Hotspot is a guide that drives clients through the process of accessing the hotspot and then to connect to the Internet.

## Hotspot Settings

The hotspot can be enabled or disabled by clicking on the main switch  at the top of the page. When enabled (i.e., the switch is green , one of three roles can be selected:

### 1. Master/Standalone hotspot or Standalone hotspot

When the hotspot is used as a Master all the configuration data, even those of the satellites, e.g., user database, portal configuration, setting, logs, and so on, are stored locally and the management tasks are performed on this hotspot.

For the *Master* role, one setting is available and also the available VPN accounts are shown that can be assigned to the satellites.

#### *Hotspot password*

This is the *Master Hotspot's password*. Remote satellite systems need to use it to connect to the master hotspot. If this field is left blank, a new random password will be generated.

#### *Hotspot satellites*

The list of available OpenVPN tunnels for use in connecting a remote satellite system. One or more systems can be selected from this list.

### 2. Satellite hotspot

A satellite hotspot does not store any configuration, but relies on the Master to verify user data, ticket availability, and all the settings. When selecting this option, the IP address and the password of the Master hotspot must be specified, along with the VPN tunnel name (see [below](#)). In detail, these are the available options:

#### *Master hotspot IP address*

Specify in this field the IP address of the master hotspot, which is usually the first IP address available in the special OpenVPN subnet (see [The zones](#)) defined in the OpenVPN server settings (under Menubar › VPN › OpenVPN server › Server configuration) of the Master hotspot.

#### *Master hotspot password*

The Master hotspot password. This is typically auto-generated on the Master. Click on the *Show* checkbox to reveal the password mask.

#### *Hotspot VPN tunnel*

From this drop-down menu, select the OpenVPN tunnel used to reach the Master hotspot.

### **3. External RADIUS server**

In this configuration, the hotspot relies on an external RADIUS server, like [FreeRadius](#) for its activities: It connects and ask for authentication to the RADIUS server, which stores all the data about accounting, settings, ticketing and connections. Several information about the RADIUS server are required for its correct functioning: the IP address, password, and ports, the IP address of the fallback server. Additionally, the external portal can be used.

#### *RADIUS Server IP address*

The IP address of the external RADIUS Server.

#### *Fallback RADIUS Server IP address*

The IP address of the fallback external RADIUS Server.

#### *RADIUS Server password*

The password for the RADIUS Server. Click on the *Show* checkbox to reveal the password.

#### *RADIUS Server AUTH port*

The RADIUS Server AUTH (Authentication) port number.

#### *RADIUS Server ACCT port*

The RADIUS Server ACCT (Accounting) port number.

#### *RADIUS Server COA port*

The RADIUS Server COA (Change of Authorisation) port number.

#### Hint

The default values for the RADIUS port are: 1812 (AUTH), 1813 (ACCT), and 3799 (COA)

#### *Use external Portal*

When this option is chosen, an external portal can be configured as the login interface that the users see when they want to connect through the hotspot. The external portal must be compatible and communicate with chilli. The following options should be configured to activate the external portal.

#### *External Portal URL*

The location on which the portal is located.

#### *NAS ID*

The Network Access Server Identifier of the RADIUS server that identifies the portal.

#### *UAM Secret*

The UAM shared secret from the external RADIUS server. While it is possible to not define a value for this option, it is suggested to define it, since it improves security.

#### *Allowed Sites / Access*

A list of websites accessible even without registering to the hotspot.

#### *Enable AnyIP*

Allows clients without an active DHCP client to connect to the hotspot.

#### Note

The setup of a RADIUS server is not discussed here since it is outside the scope and duties of Panda, who does not provide assistance in this task.

Master/Satellite roles and VPN.

The Master/Satellite roles can prove useful when wide areas should be covered and one hotspot does not suffice. When such an architecture is employed, all the management tasks for users and tickets are carried out on the master only. On the satellite systems only the *Reports* section (under the hotspot administration Interface) will be available.

The connection between the Master and its satellites is set up by creating OpenVPN accounts on the Master, using one for each Satellite, and creating a VPN tunnel between each Master-Satellite pair. Many tasks have to be completed before setting up this configuration, both on the Master and the Satellite systems, that are grouped in two parts, each encompassing operations to be carried out on either the Master, in which case they are labelled with **M#**, or on the Satellite, labelled with **S#**.

When a Master and one (or more) Satellite hotspots have already configured, an additional Satellite only requires that only tasks M3, M4, and M5 on the Master be carried out, but all tasks on the Satellite.

M0. Set the hotspot as *standalone* (This is optional).

M1. On the The VPN Menu section (VPN › OpenVPN server), set up the hotspot as OpenVPN server with a routed connection type and an ad-hoc network range (say *xxx.yyy.zzz.0/24*) that must be different from the subnets of the other Panda Gatedefender Appliance zones.

M2. A new virtual interface is created that routes the traffic from the OpenVPN tunnels. The Master acquires the IP *xxx.yyy.zzz.1* (i.e., the first available IP address in the network range) and acts as the gateway for all the OpenVPN tunnels.

M3. Create one unique OpenVPN account for each remote satellite system (from under Menubar › VPN › OpenVPN server › Accounts) The OpenVPN account must be configured with a static IP address. The IP addresses assigned to the satellites must fall within the subnet defined in step M1. Within that subnet, IP addresses ending with 0, 255, and the first IP of the subnet range are not available to Satellites.

Hint

Good practices suggest to assign to each new Satellite the lowest IP available, so that they remain in order.

Once all the necessary client accounts have been created and before activating the Master/Satellite configuration, it is necessary to verify that the OpenVPN connection be setup correctly. Hence, on the Satellite side two steps are needed:

S1. Create the OpenVPN client account (VPN › OpenVPN client (Gw2Gw)), using one of the accounts created at step M3.

S2. Connect to the Master and verify that the connection is established and the traffic can flow.

Now it is possible to activate the Master and complete the setup:

M4. Open the Hotspot settings page and enable the necessary VPN account in the list of hotspot satellite systems.

M5. Click on *Save* and then on *Apply* to activate the changes.

The set up of the master is now finished, so proceed to complete the Satellite setup:

S3. Enter the hotspot menu, choose the *Satellite hotspot*, enter the first IP address available in the OpenVPN subnet of the Master and the Master hotspot password, and select the Hotspot VPN tunnel from the drop-down menu.

S4. Click on *Save* and then on *Apply* to activate the changes.

To verify that the satellite system is properly connected, open the satellite system's Hotspot Administration interface: Only a limited interface shows up, containing the *Reports* section and nothing else: all the management's task are delegated to the Master.

The setup is now complete: both the Master and the Satellite systems are correctly working.

### Use External Authentication

When the role of the Hotspot is *Master / Standalone hotspot*, it has now the ability to rely on an external resource only for the purpose of authenticating the users, while keeping accounting, logging, user database, and all other settings locally on the Panda Gatedefender Appliance. In other words, the data of a user are copied locally from the external server, either a RADIUS or a LDAP server, allowing her to provide her credentials of the remote server and immediately use the hotspot, without the need to create a new account.

To allow the Hotspot to connect to the remote server and retrieve the data, there is an option available:

#### *Use External Authentication*

By ticking this checkbox, the two possible remote authentication modalities are shown, together with all the necessary options to configure them.

#### *Server Type*

This drop-down menu allows to choose one of the two supported servers, either *LDAP* or *RADIUS* and changes the configuration options displayed accordingly.

Note

The additional configuration options that will appear are very similar to those that appear in Menubar › Proxy › HTTP › Authentication.

Example HS1 - External Authentication with LDAP.

The settings for the LDAP server may be filled in as follows, using standard Active Directory's format, in which:

- DC is the domain controller
- OU is the organisational unit, a group of objects within the DC
- CN is the common name of the user in the OU

Hence, to authorise the users in the `Staff` organisation unit in the domain `ACME` of the LDAP server located at `ldap.example.org` to use the hotspot, the following settings are needed:

1. *LDAP server* `ldap://ldap.example.com`
2. *Bind DN settings* `ou=Staff,dc=ACME`
3. *Bind DN username* `cn=admin,dc=ACME`
4. *Bind DN password* -remote password of user admin-
5. *User search filter* `(&(uid=%(u)s))`

For the *LDAP server*, the following configuration options are available:

#### *LDAP server*

The IP address or hostname of the LDAP server, in LDAP format.

Hint

The port specification, if needed, can be written after the URL, like e.g., `ldap://192.168.0.20:389/`. The standard port, 389, can safely be omitted.

#### *Bind DN settings*

This settings define the Distinguished Name of the LDAP server, i.e., the top level node of the LDAP's tree structure.

#### *Bind DN username*

The username to be used for querying the DN. It is necessary to retrieve and authenticate the credentials of the Hotspot's users.

#### *Bind DN password*

The password for the user specified in the previous option. A click on the checkbox on the right shows or hides the characters.

#### *User search filter*

The string that shall be used to query the remote LDAP server.

#### *LDAP backup server*

The IP address or hostname of the LDAP fallback server, in LDAP format, that shall be used when the primary server is not reachable.

#### *Default rate*

The rate that shall be associated to each users that authenticate through this method.

For the *RADIUS server*, the following configuration options are available:

#### *RADIUS server*

The IP address or URL of the RADIUS server.

#### *Port of RADIUS server*

The port on which the RADIUS server is listening.

#### *Identifier*

An additional identifier.

#### *Shared secret*



The password to be used.

#### *RADIUS backup server*

The IP address or URL of the fallback RADIUS server, used when the primary server is not reachable.

#### *Default rate*

The rate that shall be associated to each users that authenticate through this method.

## Administration Interface

The Hotspot Administration Menubar

This section describes the core component of the hotspot and includes sub-pages that explain how to manage accounts, tickets and ticket rates, to create reports, and to configure the general settings. Although this graphic interface shares the design with the other modules, it contains an entirely new menu structure: Its complexity and the countless configuration options it offers require that a different layout be employed. The choice was to consider the hotspot as an independant module of the Panda Gatedefender Appliance and therefore to replace the standard menubar, common to all other main sections of the Panda Gatedefender Appliance, with a new one that consist of two parts, as shown in the figure above. The upper part does not change across the various parts of the Administration Interface and contains the 'proper' menu, while the lower part is a sub menu, which changes depending on which section of the Administration Interface is chosen.

Each of the four main sections allows the management of one hotspot's component:

[Accounts](#) - Create, manage, import, and export user accounts.

Tickets - Define ticket rates and generate tickets.

Reports - Consult the various balance, connection, and transaction logs.

Settings - Change the appearance of the web interface, set up SmartConnect™, enable the API, and configure all the functionalities.

On the far right, the *Main Menu* link will always be there to go back to the initial Dashboard and menubar.

## Accounts

This section of the Hotspot's Administration Interface contains four sub-menu items, *List*, *Import from CSV*, *Export as CSV*, and *Account Generator*, that allow to create, delete, and manage the clients of the hotspot.

### List

This page shows by default a list of the available user accounts with some information, namely *Username/MAC Address*, *Name* (The user's full name), *Enabled* (the status of the account), *Creation Date*, and *Valid until*. A few options help customise the view:

#### *Sort by*

Users can be sorted by any of the fields mentioned above, except by their status.

#### *Reverse order*

Sort the list in ascending or descending order.

#### *Hide disabled accounts*

Hide from the list the disabled users, i.e., users that exists but that can not access the hotspot.

#### *Search*

Searching for accounts is also possible, with pagination available for huge result sets.

### Note

Users mentioned in this section are intended as user of the hotspot as clients who can access and browse the Internet. There are, however, two other types of users, namely Administrators and Account Editors, whose abilities and duties are described in section [Hotspot User](#).

Several *Actions* are available on each account and are shown along each account on the right-hand side of the table:

#### *Edit / Add ticket*

An account can be edited or deleted, while tickets can be assigned to it

#### *Balance*

Show the balance of the account

#### *Connections*

Show detailed information about the account.

#### *Delete*

Delete the user account from the hotspot.

#### *Print*

Print an informative message with the credentials for that account.

#### *Hint*

Messages for MAC-based accounts can not be print as they do not foresee username and password defined.

The actions of showing the balance and connection, along with options for their management, are described under the Reports section, while the accounts' administration (i.e., user and ticket management) composes the remainder of this section.

A new account can be created in two alternative manners: Either by specifying a username and a password, or by providing a MAC address. Both actions can be carried out by clicking on the appropriate link above the accounts' table. The data associated with each account is divided in three types: *Login information*, *Account information*, and *Tickets*. [Login information](#) slightly differ in the two types of account, depending on the type of account, while [account information](#) are exactly the same. Finally, tickets can be associated to an account, depending on the types of tickets already defined and available in the hotspot. See the Tickets section for a description of tickets types and settings.

#### *Add Account*

The creation of a new account requires that a username and a password be specified that will identify the user connecting to the hotspot. Additional settings can be modified from their default values, defined in Settings, which are: Expiry date (*'valid until'*), whether the account is active, the language, and the bandwidth limit in kb/s. The Language can be chosen among those activated in Hotspot › Admin interface › Settings › language

#### *Add MAC-based Account*

The only difference is that for this type of accounts the username and password are not needed. Instead, the MAC-Address of a computer's network interface should be provided, that will be used to identify the account. The remaining settings are the same as before, but MAC-based addresses can also be given a static IP address.

To each account, the following data can be associated:

#### **Login information**

This box contains the information related to the newly created account and necessary to access and use the hotspot.

#### *Username*

The username associated to the account. If the field is left blank, then a random username is generated.

#### *Password*

The password for the new account, that can conveniently be autogenerated by the system by leaving the field blank. The password will only appear when printing the message that will be handed to the user with her credentials to access the hotspot.

#### *MAC Address*

The MAC address that shall be used to identify the account. Available for MAC-based accounts only.

#### *Valid until*

The date when the account expires. The default value of one year, or 365 days, can be changed under Settings. To change the value for the current account, either provide the new date in the form DD.MM.YYYY or click on the ... button and select the new date from the calendar pop-up.

#### *Active?*

This checkbox specifies if the account is enabled or not. If ticked, the account is active.

#### *Language*

The language in which the user will see all the hotspot's messages, chosen among the available ones from a drop-down menu.

#### *Bandwidth limiting*

The upper bandwidth limits in both upload and download for the account in kb/s. An empty field means no limit, i.e., the user can use up to the whole bandwidth. Custom limits are activated by ticking the checkboxes.

*Static IP address*

This option is only available for MAC-based accounts, which can be associated to a static IP address, specified here.

**Warning**

Bear in mind that changing some of the account's existing [login information](#) like the username, will cause a **new** account to be created.

**Account information**

This box contains all the personal information related to the owner of the account.

*Title*

The person's title (e.g. Mrs., Dr.)

*Firstname*

The user's first name.

*Lastname*

The user's last name.

*Street*

The street in which the user lives.

*ZIP*

The ZIP code of the user's hometown.

*City*

The city or town the user comes from.

*Country*

The country the user comes from, that shall be chosen from the drop-down menu.

*E-mail address*

The E-mail address that will be associated with the account. E-mail addresses can be changed in the account editor with no limitation, except that an e-mail address that is already in use can not be used to register a SmartConnect™ account.

*Phone number*

The phone number associated with the account. The country code can be chosen from the drop-down menu on the left-hand side and the number shall be written in the textbox on the right-hand side..

*Birthdate*

The user's birthday.

*City of birth*

The city or town in which the user was born.

*Document Type*

The type of document that has been used to identify the user. Four types of documents are available from the drop-down menu: Birth Certificate, Identity Card, Passport, and Drivers License

*Document ID*

The ID of the document that has been used to identify the user. Note that in some Countries, collecting Documents may be mandatory to access public hotspots.

*Document issued by*

The issuer of the document (e.g., the City of New York)

*Description*

An additional description for the account.

**Tickets**

This box allows to see and manage the tickets associated with the current account and shows the following options:

*Add new ticket*

The drop-down menu shows the available ticket rates and if they are time- of traffic based. It is not possible to mix time- and traffic based tickets, hence if a user has already one or more time based ticket, no traffic based ticket can be added, and vice-versa.

#### *Validity*

Once chosen one available ticket rate, this option will appear and allows to customise the ticket validity. The available values are the same defined during the Ticket rates creation and will override the ticket's default value (shown by the textbox and the drop down-menu underneath).

#### *Add*

Once the ticket has been chosen, it can be associated to the current account by clicking this button.

#### *Note*

When editing an existing account it is also possible to print a welcome message containing also the credentials by clicking on the *Print* button: This is the same action that can be carried out from the list of the accounts.

At the bottom of the box, a small table shows all the tickets associated with the account with a couple of information for each of them. If a ticket is still valid, it can be deleted, but if it has expired, it remains there as it is already stored in the accounting for the account (see Reports for more info about balance and accounting).

If the Panda Gatedefender Appliance has already support for cyclic tickets (introduced with release 2.5-20130516, after choosing a cyclic ticket from the drop-down menu, a small form is displayed instead of the *Validity* drop-down menu, with the following options.

#### *Start date*

The day on which the first cycle of the ticket starts. If the ticket period is *Monthly*, it can only be chosen the first month of validity. For tickets with *monthly* cycle, indeed the start of the period is the first day of the month, while the end is the last day of the month.

#### *End date*

The day on which the first cycle of the ticket ends. If the ticket period is *Monthly*, it can only be chosen the last month of validity.

Below these options, a variable message shows the total number of cycles of the tickets, the price per cycle, and calculates the total price of the ticket. Like in the case of the normal tickets, a table maintains the list of the cyclic tickets associated with the account. For the sake of clarity, this table is kept separated from the other one.

## **Import from CSV**

When importing the account names from a CSV file, the filename is not important (exported files have peculiar names, see next section), but it needs a fixed format of the fields. The follow options are available:

#### *Choose a File*

Click on this button to select the CSV file that shall be uploaded. The file shall be in plain text, i.e, ZIP archives, GPG encrypted files and the like are not accepted.

#### *Delimiter*

The character that shall be used as delimiter, which is usually a comma ',' or a semicolon ';'. If not provided, the Panda Gatedefender Appliance will try to guess which is the correct character.

#### *Hint*

The Panda Gatedefender Appliance uses commas to separate the fields.

#### *The first line of the CSV file holds the column titles*

Tick the checkbox to let the Panda Gatedefender Appliance know that the first line of the CSV file contains the header of the columns and ignore it when importing it.

#### *Note*

Files that the Panda Gatedefender Appliance fails to recognise as CSV files will be rejected with the message *The given file does not seem to be in CSV format.*

#### *Import accounts*

Click on this button to import the CSV file.

After the account have been imported, the page will be replaced by a new one, containing some columns (depending on how many accounts have been found in the file). The first column contains all the available fields, while the second all the fields that have been recognised in the CSV file.

#### Hint

If in the first column all the labels have a red background, and those in the second column all have a green background, the data have been correctly imported.

The remaining columns show the content of the file and how will the data in the file be interpreted. All fields that have not been recognized are depicted in yellow: They can be associated with the available fields by dragging the red labels from the left-most column onto the yellow fields in the second columns.

#### Note

The data in these columns can not be modified, so if there's something wrong with them, go back to the previous page to break the import process and modify the CSV file before trying again to import it.

Below the table appears the following options:

#### *Do you want to see which accounts are imported?*

By ticking the checkbox, before the new accounts are actually imported and stored, a summary of the accounts will be shown, divided into two parts: At the top of the page the new accounts are displayed, while on the bottom there are the accounts to be updated.

#### *Store Accounts*

A click on this button starts the storage of the accounts in the Panda Gatedefender Appliance and concludes the import process.

#### Hint

If the checkbox above is ticked, click again on this button after the summary has been show to complete the import process.

#### Warning

Recall that modifying one of the user's login information causes a new account to be created. This is true also when importing accounts that only slightly differ in some login information from existing ones. Make sure to examine them prior importing them, in order to avoid potential issues later.

## Export from CSV

A list of existing accounts can be exported and saved in CSV format. When exporting the list, the fields that will appear in the exported file are fixed, so it is only possible to decide whether to open (view) the file or under which directory to save it. For convenience, the filename will be saved as `accounts_YYYYMMDD_HHMM`, where `YYYYMMDD` represents the year, month, and day, and `HHMM` represents the hour and minutes when the list has been exported. This choice allows the exported files to be listed in lexicographic order in the directory in which they are saved. The filenames can however be modified at will. The exported files can be used as backups and imported later.

#### Warning

Remember that the exported list contains also the passwords of the users in **plain text**, so remember to keep the list in a safe place.

## Account Generator

The use of the account generator can prove particularly useful when there is a necessity to create a bulk of new accounts with a default ticket already assigned and can therefore be handed in to e.g., a group of users. As an example, consider the registration phase at the beginning of events like conferences or conventions, during which large groups of people need to access the hotspot and receive their credentials in a small interval of time. The account generator allows to create at once a specific number of accounts by providing only some common options, grouped in three parts: Username, Password, and Settings, described below. This page is divided in four boxes: the first three compose the Account Generator, while the fourth one is the list of generated bulks of accounts, shown on the bottom of the page after at least some bulk has already been created.

Example HS2 - Generation of multiple accounts.

This example shows the differences between the the sequential and the random generator in the output of 5 accounts using the same common settings:

- Username prefix: `USEI` (4 characters).
- Username length: `8` characters (hence there are 4 more characters to fill).

- Password length: 8 characters.
- Character sets: `a1l`.

Using the *Sequential* username generator, with the *Sequence start* option is set to `10`. The resulting output (username / password) is:

```
user0010 / hLFE.+6C
user0011 / u_4w3.N_
user0012 / h7R7p7sK
user0013 / p6lGRc3T
user0014 / KqUDmWiI
```

Since there are two more characters needed to reach the length of 8 characters required for the usernames, `0`s are added to between the prefix and the sequence.

Using the *Random* username generator, with all the *Character set* except for *Extra*, the resulting output (username / password) is something like:

```
userLI4u / p0Dch_fA
userWNDS / Qhbovf7
userrq7K / dQTlmA-u
userSYE0 / BuWHuKfZ
userAHEQ / -GxlyMta
Username
```

There are 2 different types of username generators: *Sequential* and *Random*, both of which share two common option:

#### *Prefix*

The starting part of the username, shared by all accounts in the bulk. An empty prefix is also accepted.

#### *Length*

The total length of the username.

The length shall be longer than the prefix's length, otherwise an error message will be shown.

The complete usernames will be filled up differently for the two generators, and for both generators there will be displayed a peculiar option. In the case of the sequential generator, increasing numbers are used, defined by the option:

#### *Sequence Start*

The digit or number from which the sequence starts.

#### Hint

If more characters are needed, besides the prefix length and the sequence, to reach the required length, `0`s will be added. (see [Example HS2](#)).

In the case of the random generator, characters are used, defined by the different *Character sets* selected:

```
* Uppercase Letters (A-Z)
* Lowercase Letters (a-z)
* Numbers (0-9)
* Extra characters (._-+)
```

#### **Password**

The length of the password and which character sets should be used to generate the random passwords can be defined here. The strength of the password depends on its length and on how many character sets are used among the available four: Uppercase and lowercase letters, numbers, and extra characters. As a rule of thumb, choosing a 8 character long password and all character sets will generate 48-bit passwords, which should suffice for most uses.

#### **Settings**

Additional option about the generated accounts: The number of accounts to generate, whether they should immediately be enabled, if they have a default ticket associated, and finally how many days will the account last.

To generate users with the specified settings, click on the *Generate accounts* button: A sample of the first 5 username - password combinations will appear. The whole bulk will be generated only after clicking on *Confirm*, otherwise a click on *Cancel* will delete even the 5 samples shown.

After the first creation of a bulk of accounts, the page will reload with a confirmation message and, beneath the account generator, a new table will show up, that contains information about the accounts created. In particular, the following columns are shown in the table:

### Date

The date on which the accounts have been generated.

### Generated Users

The number of users that have been generated.

### Actions

There are three available actions on each bulk:

*Load settings*, to load the setting used to create those accounts and reuse them to generate a new bulk.

*Delete users*, to remove all the users created in that generation. This action will only delete users who have not yet connected or who do not have credit left: In other words, users which have already connected to the hotspot or have credit left will not be deleted.

*Export as CSV* to export the username / password combination in CSV format. This proves useful to print the data on prepaid cards.

## Tickets

In this section server the purpose to manage every option related to tickets: which type of tickets are available and whether they are time-based or traffic-based, their rate -i.e., how much the user pays per unit of time or data-, and the creation of expendable tickets. The options are grouped in three categories, shown in the *Tickets* submenu: Rates, Quick Ticket, and Ticket Generator.

New in version 2.5-20130516: Cyclic tickets

### Rates

The Panda Gatedefender Appliance gives the possibility to define several ticket rates in the *Add Rates* page, by selecting different combinations of the payment (post-paid vs. prepaid) and measuring (traffic-based vs. time-based) options from the appropriate drop-down menu. Depending on the combination chosen, the price for unit of use or for the whole ticket can be set. In particular, postpaid payment allow to define the price per one hour (time-based) or per 10 MB (traffic-based). The prepaid payment, instead, allows the definition of a more precise price and even the unit. In this case, indeed, even the amount of time (in minutes, hours, or days) or traffic (in Mb or Gb) and either the ticket price or the unit price can be supplied.

#### Note

When entering the ticket price, the price per unit is automatically calculated, and vice versa. This proves useful when offering different prepaid types of tickets and verify, for example, that the cost of four prepaid, 15 minutes duration tickets are more expensive than one prepaid, one hour duration ticket.

#### Cyclic tickets

New in version 2.5-20130516.

Cyclic tickets are a new type of tickets that can be offered to Hotspot users. The idea behind the introduction is to assign to a user the same amount of traffic within a period (*cycle*), that can be repeated an arbitrary number of times (*cycle duration*). Every user can be assigned one cyclic ticket at a time.

More in details, a cyclic ticket consist of three parts:

1. a *rate*, which is the cost per amount of time or of MB of traffic, exactly like other rates
2. a *cycle duration*, which is a period of either one day, one week, one month, or one year, during which the traffic must be consumed
3. a *number of cycles*, that shows how many consecutive times the ticket can be used. This number is decided by the hotspot's administrator and is by default 1.

Although all types of ticket can be purchased at any moment and being used immediately, there is one exception: Cyclic tickets whose *cycle duration* is **Monthly** always start a cycle on the *first day of the month* and expire on the *last day of the month*. As an example, consider a monthly cyclic ticket purchased on the 20th of June. While it is possible to start using it immediately, the first cycle will finish on the 30th of June. It is therefore suggested to start the validity of this ticket on the 1st of July, so the first cycle will expire on the 31st of July.

Cyclic ticket can only be prepaid, i.e., they must be purchased in advance. Residual traffic within a cycle is **not** added to the next one, i.e., it must be used before the end of the cycle or is lost. Cyclic rates can not be used for quick tickets, smartconnect tickets, ticket generator, and account generator: They must be explicitly assigned to an existent user or during the creation of a new user.

The tickets offered can even be made available for SmartConnect™ transactions (see below).

The available types of tickets are shown when opening the *Ticket* page in a table composed by several columns, which correspond to the options that can be defined in the *Add Rates* page. The tuples can be ordered by rate name, payment, or measuring mode. The ordering criteria can be reversed if the *Reverse Order* checkbox is ticked. To search for a particular rate name or to filter among them, fill in the input form located on top of the table with at least one character and press **Enter**. The columns of the table carry the following information:

#### *Rate Name*

The name given to the ticket rate.



#### *Ticket Code*

The ASA code for the ticket rate. Although used only for the ASA hotel management system, this field is mandatory. In case there is no ASA management system, fill it with any character or string.



Hint

When not using ASA, use the same string for the rate name and for the asa ticket code.

#### *SmartConnect?*

This column shows whether this rate is available for SmartConnect™ transactions, in which case a  icon will appear in the list, otherwise a  is displayed. A click on the icon toggles the status of the rate.

#### *Quick Ticket?*

Similarly to the previous, this shows whether this rate can be used for the creation of new quick tickets: In this case a  icon will appear in the list, otherwise a  is displayed. A click on the icon toggles the status of the rate.

New in version 2.5-20130516.

#### *Payment*

This column appears if the rate requires prepaid or Postpaid payment.

#### *Measuring Mode*

This column shows whether the rate uses the time-based or traffic-based measuring mode.

#### *Cycle*

The length of each cycle of the ticket.

#### *Amount*

This is the amount of time or traffic available when a single ticket is created with this rate. In the Rate editor this option appears right below the *measuring mode*. A drop down menu allows the choice between time-based and traffic-based ticket. In the former case, the number of minutes, hours, or days of validity can be chosen, while in the latter the amount of megabytes or gigabytes.

#### *Price*

This shows the hourly or per-10MB price and the ticket price specified for this rate. In the rates editor, two textboxes appear that quickly convert the price for unity (10Mb or one hour) into the price for ticket, which proves useful to control the average price per unit of the various rates defined.

#### *Actions*

Choose whether to edit or delete a ticket rate.

When the choice of the *Rate type* is *Cyclic*, the rates editor changes slightly, displaying the following configuration options, instead of *Price*:

#### *Duration of the cycle*

The duration of one cycle of the rate, that can be either *one day*, *one week*, *one month*, or *one year*.

#### *Price per cycle*

The cost of each cycle.

#### *Default number of cycles*

The default number of cycles for the validity of the ticket. If it is not specified, the value **1** will be applied.



### Total price examples

As soon as the price per cycle has been entered, this table calculates the total price for the cyclic ticket for some relevant number of cycle (e.g., 7 or 14 Days, 3 or 6 months and so on).

In the rates editor, one additional setting can be specified for the ticket:

### Validity

This option defines the expiry dates for the single tickets created out of this type and appears only in the rate editor. The four possible values, chosen from the drop-down menu are:

- *Always, unlimited validity*
- *From ticket creation* allows to specify the length of validity of the ticket, measured in either minutes, hours, days, weeks, or months from its creation.
- *From ticket first use* like the previous one, but the validity starts when the ticket is first used to access the hotspot.
- *Until the end of the day*, the ticket shall be used within the current day.

These values will be the default for the new tickets that will be created, though they can be overridden on a user basis when associated to a user under Accounts › List › Edit / Add ticket › Add ticket.

### Warning

After one ticket rate has been saved, only the rate name, the rate code, or the availability for SmartConnect™ transactions are changeable. Indeed, changing anything else would lead to have inconsistent accounting data. Hence, in order to modify a price for a rate, rename the existing rate and create a new rate with the original name. Suppose for example that there is a rate called *hourly* whose cost should be modified. First, rename that rate to something like *OLD-hourly*, then create a new rate with the original name "hourly".

## Quick Ticket

This page is used to create a new, single user account, whose username and password are automatically generated. To do so, optionally supply the first and last name of the user, then click on the desired rate among those displayed.

### Hint

Only rates available for SmartConnect™ are available for quick tickets.

After clicking on the rate button, the username, password, and rate are shown on the screen: At this point the selection of the language for the user is possible. These accounting data can be printed by clicking on the *Print information* button. The new account inherits all the default settings -defined in Hotspot › Settings- and is listed in the Accounts page. It is a normal account on which all actions can be carried out.

## Ticket Generator

With the ticket generator it is possible to create a specific number of tickets which share common settings, including a predefined ticket rate. This option proves useful when there is the need to create a large set of prepaid ticket codes for customers that can directly use it on SmartConnect™ to access the hotspot, or even to use them as demo or evaluation codes. To be able to use a ticket, however, the customer must be registered: If she is not, she will be required to create a new account, an operation that can be easily carried out by the customer herself without the necessity of interaction of the hotspot's administrator.

The Ticket Generator page is split into two boxes: On the upper side the input forms can be filled in to quickly create new tickets, while the lower side contains a table listing the already generated bulks of tickets. After at least bulk of tickets has been produced, a link will appear between the two sides, *Show generated tickets*, that can be clicked to show all the tickets available (see below).

There are two groups of options available in the generator to create new tickets:

### Ticket Code

Define the prefix text (string) to use when creating the bulk of tickets, the length of the tickets' name, and which character sets should be used to generate the random tickets.

### Settings

The number of tickets to generate and the assigned rate that should be assigned to the tickets, among those already present in [Rates](#).

To generate the bulk of tickets with the specified settings, click on the *Generate tickets* button: A sample of the first 5 ticket - code combinations will appear. The whole bulk will be generated only after clicking on *Confirm*, otherwise a click on *Cancel* will delete even the 5 samples shown.

Beneath the ticket generator options, all previously generated bulk of tickets are listed in a table whose columns are:

#### *Date*

The date and time on which the tickets have been generated.

#### *Generated Tickets*

The number of tickets that have been generated.

#### *Actions*

There are three available actions on each bulk:

*Load Settings*, to load the setting used to create those tickets and reuse them to generate a new bulk.

*Delete tickets*, to remove all the tickets created in that generation. This action will only delete tickets that have not yet been consumed.

*Export as CSV*, to export the list of tickets combination in CSV format.

Clicking on the *Show generated tickets* link leads to the page showing a table with all the generated tickets, that can be (reverse) sorted by either the ticket's code or creation date, with the option to hide unused or expired tickets. Specific codes can also be searched for using the input form next to the *Code:* label.

The table shows the ticket code, which user has used or has been assigned a ticket -if any, the ticket rate, the ticket creation date, and an optional link to either delete a single unused ticket code or to expire a ticket code in use. When the table contains a large number of tickets, pagination is available to split the list.

## Reports

The Reports section contains several pages with information and statistics about the activities, users, tickets, traffic, connections, and accounting data related to the hotspot. Few actions are available in this section, whose purpose is to provide a detailed view of the users' statistics and connections and of the use of the hotspot.

#### Note

On the satellite hotspots, *Reports* is the only available menu item in the entire hotspot administration interface.

## Connections

The default view when opening the *Reports* pages is to show the table reporting all the currently active connections to the hotspot, including those on satellites - if any. For each connection, the following information are displayed:

#### *Satellite*

The name (i.e., the OpenVPN account's name) of the remote hotspot satellite system, if this Panda Gatedefender Appliance is a Master in a Master/Satellite configuration (more on that in the roles of an hotspot section) and the user is connected to a satellite.

#### *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 total time since the connection has been established.

#### *IDLE Time*

The amount of time since no traffic has been detected between the account and the hotspot.

#### *IP Address*

The IP address of the client connected to the hotspot.

#### *MAC Address*

The MAC address of the client's connected interface.

#### *Action*

Every active connection can be closed by clicking on the *Logout* link in this column.

### **Balance**

This page contains a list of accounts with information about their connections, followed by a global summary at the bottom of the page. Two alternative views are available to show users' balances, called *Filter Period* and *Open Accounting Items*, with the former being the default view. They can mutually be accessed by clicking on the link available on the far right of the page. The actual data shown in the two views are different, but they report quite the same type of information, which are the following:

#### *Username*

The username or MAC address of the account. When clicking on the username, the Account Balance page of that user will open. (see [below](#)).

#### *Amount used*

The amount of money that has been used by this account.

#### *Paid*

The money already paid by the user.

#### *Duration*

The time this user has been connected to the hotspot.

#### *Traffic*

The traffic that has been generated by this account.

At the top of the table, a start and an end date can be written into the *From* and *Until* fields respectively: By clicking on the *Filter* button on the right, the page will be reloaded with statistics limited to the interval between these two dates only. To show a calendar to ease the search for a date, click on the ... buttons on the right of the textfield. Pagination is available to split any long lists.

#### Hint

The format of the date is DD.MM.YYYY, like e.g., 03.06.2013 (third of June 2013)

The alternate view, *Accounting Items*, displays the same, aforementioned data, but with one additional column:

#### *Amount to pay*

The amount of money that has not been yet paid by that account.

On either view, clicking on a username or MAC address opens the Account Balance page for that account, that reports detailed statistics about the user's tickets and billing, grouped in four parts. Note that this page can be reached also from Accounts › [ User list ] › [ Actions ] › Balance.

### **User Information**

All the user's login information, i.e. name, username, city of birth and birth date, Document ID, and the party issuing the document.

### **Account Balance**

Detailed information about the account balance, with all the time-based related statistics followed by the traffic-based statistics. In both cases, the total pre- and post-paid tickets assigned to the user, and the total used and available time or traffic are shown.

### **Postpaid payment**

In this column, two boxes show the amount of money that the user has already been paid, and that she still has to pay, displayed in the currency configured on the Settings page. The lower box has a green background if everything has already been paid, red otherwise. Credit can be added to the user (either to solve a debit or simply to allow her to buy more traffic), inserting any amount in the input field below the two boxes and clicking on *Add credit*.

### **Accounting Entries**

This table lies at the bottom of the page, and contains a list of the tickets associated with the user. For each ticket, a number of information is displayed:

#### *Ticket name*

The name of the ticket's rate.

#### *Amount*

The credit (with green background) or debit (red background) associated with this account.

Any cyclic ticket purchased by the user is shown in this column multiple times: Once when it has been created with the ticket name *Cyclic [name]*, then at the beginning of each cycle, a new ticket named *[named]* with amount 0.00 EUR (or in the currency used in the hotspot) is added to the accounting.

#### *Date / Time*

The timestamp of the tickets' creation.

#### *Duration*

How much time has the ticket been used

#### *Traffic*

The traffic consumed by the ticket.

#### *Processed*

Whether or not the ticket has been used.

#### *Retries*

This option is used by the ASA interface and shows how many times the system tried to account these entries.

#### *Message*

A custom message.

For each entry that is a cyclic ticket, the message contains the following information:

- *Period ID* is a progressive number that uniquely identifies the ticket.
- *Cycle:* and *Number of cycles* refer to the ticket and refer to the ticket's period length and to the number of cycles purchased.
- *Start date* and *End date* show the first and last day of the ticket's validity.

After filling the *Start date* and *End Date* fields above the user information (or clicking on the ... buttons to chose the dates from a pop-up calendar) and clicking on the *Filter* button, only the statistics within that period will be show.

The currently shown statistics can be printed by clicking on the >>> *Print* button.

## Connection Logs

This page contains a table showing several information about the current and past connections. The items can be (reverse) ordered by any of the columns and even filtered, to show only the connections established within two dates. The information shown are:

#### *Username*

The username making the connection.

#### *IP Address*

The IP address of the connected client.

#### *MAC Address*

The MAC address of the connected client's 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.

## Export Connection Logs as CSV

The connection logs, which contains detailed, relevant information, can be downloaded to be viewed or stored in CSV format by clicking on the *Export Connection Logs as CSV* link in the sub-menu. The default filename for the log file is *hotspot-YYYYMMDD-FULL.csv*, where YYYYMMDD is the date on which the file was created and FULL means that the file contains details about all connections.

Warning

Remember that the exported list contains also the passwords of the users in **plain text**, so remember to keep them in a safe place.

## SmartConnect Transactions

This page reports the list of all SmartConnect™ connections and transactions, that can be (reverse) sorted by either the transaction ID or the order time. Specific transactions can be searched by providing some character in the input form near the *Search:* label. The information provided in the table are:

### *Transaction ID*

The transaction identification string, mostly useful for accountability or in case of troubles with registration of clients and tickets. Any transactions can be looked up here.

### *Order Time*

The date and time of the transaction.

### *Payment*

The status of the payment, if it was successfully completed (free tickets will always show as *Completed*) or not.

### *User*

The username of the account created, which is the phone number in case of SMS-based SmartConnect™ transactions.

### *Phonenumber*

The phone number provided during account creation.

### *SMS*

The SMS with the account credentials are sent from the hotspot via the Panda Perimetral Management Console. If for any reason the message has not been sent or if the client never received it, this field shows *Failed*, otherwise it shows *Success*.

### *SMS Time*

The date and time when the SMS was processed.

### *Name*

The name provided at the account creation.

### *Info*

The address, zip code, and country information provided at the account creation.

[Pagination](#) is available for tables with many entries.

See also

SmartConnect

Hotspot › Settings › SmartConnect

## Settings

This section sorts out all the available options to configure the Hotspot in four main groups: Main, SmartConnect™, API, and Language.

### Main

This page contains all the System settings, divided in four parts: In the first one, *Portal*, it is possible to define default values for the portal appearance; in the second one, *Global Settings* allows to specify some option used by the various parts of the Hotspot; in the third one, *Accounts*, common options for the account are defined; and in the fourth, the *Character set for generated passwords* used in Quick Ticket are chosen.

## Warning

Some change in the settings in the *Portal* and *Global Settings* will cause all connect users to be forcibly logged off. Those settings are marked with a red asterisk in the GUI.

## Portal

The first box encompasses the following option that can be customised:

### *Homepage after successful login*

The URL of a web page that will be shown to the user after a successful login.

### *Portal Background Homepage*

The URL used as the background image for the Hotspot login portal.

### *Show login form*

Choose from a drop-down menu how the Hotspot login form is displayed:

- *immediately* will display the login form immediately over the background homepage.
- *manually* will display the background homepage with a top navigation bar allowing the user to access the registration page at any time, with the home site being browsable without any user registration: This proves useful to promote an own Web site or to provide some information. Access to all other sites will still require registration, although sites listed in *Allowed sites* (see below) can always be accessed.
- *after x seconds* will display the login form after a user-specified period of seconds over the background homepage (user is notified of impending registration time on the navigation bar).

### *Use mini portal for mobile devices*

This option governs which types of portal are served by the Hotspot. Besides the standard portal there are two more available: One without Javascripts and one tailored for mobile devices. When this option is checked, all the three types of portal are served, whereas if it not, then only the standard portal is offered to the users.

### *Allowed Sites*

The sites or IP addresses accessible even without being authenticated, i.e., those sites that can be visited by anyone. One site per line is allowed, in the form of either a normal domain name or a string of the format *protocol:IP[/mask]:port*, e.g. *pandasecurity.com* or *tcp:192.168.20.0/24:443*. Take into account that if the pages incorporate some widgets, javascripts, or other components from sites outside this list, they could not be loaded correctly.

## Global Settings

### *Hotspot name*

A name given to identify the hotspot.

### *Items per page*

The [pagination](#) value, i.e., the maximum number of items of a list or table per page that are displayed.

### *Currency*

The currency used in all the calculations of payments in the Hotspot.

#### Note

Some currency is not supported by PayPal, therefore it can not be used for SmartConnect tickets.

### *Popular Countries*

Popular countries are listed first in the list of Countries presented to the users when they register, in order to reduce the time needed for the whole registration process.

### *Enable AnyIP*

This option enables the AnyIP feature, which should assist clients not using DHCP and allow them to access the Hotspot even with a static IP that does not fall within the Hotspot's (BLUE zone) IP subnet.

### *Bandwidth limiting*

The default upload and download limits per user in Kilobyte/s. If these fields are left empty, then no limit is applied.

#### Note

Remember that in one KB there are 8 kilobit, so make sure to enter appropriate values in the fields.

#### *DHCP dynamic range*

When this option is enabled by ticking the checkbox, dynamic IP addresses are assigned to the devices connected to the hotspot.

#### *Dynamic IPs range*

This option appears when the previous one is active and allows to specify a custom range of IP addresses within the BLUE zone to be dynamically assigned to the hotspot's client.

### **Accounts**

#### *Require user authentication*

Tick the checkbox if you want that clients accessing the Hotspot need a valid, registered account.

#### *Require users to accept the 'Terms of Service' on login*

When this option is selected, the user is asked to accept the Terms of Service right before the login.

#### *Password recovery*

Allow a user that has lost or forgotten her credentials to be able to reset them. Three options can be chosen:

- *Disabled:* No password recovery is allowed
- *Using SmartConnect settings:* The credentials are sent via the same means used in SmartConnect™
- *Using custom settings:* Personalised settings can be defined.

#### **Note**

It is possible to allow anonymous login (i.e., without user authentication), but requiring all the users to agree with and accept the Terms of Service. To do so, it is first necessary to create a ticket of type *post-paid*, then to disable option *Require user authentication* and enable *Require users to accept the 'Terms of Service' on login*. If the post-paid ticket has been created with a given validity, after that period the user will again be required to accept the Terms of Service.

#### *Timeout for idle users*

The time of inactivity after which a user logged out (default is 15 minutes, i.e., after 15 minutes of inactivity a user is automatically logged out), so that the user does not waste too much of the ticket's validity.

#### *Default account lifetime (days)*

The number of days an account is valid (default is 365 days). After that number of days have passed, the user automatically becomes inactive.

#### *Allow deletion of used accounts*

This options allows the deletion of accounts that have already used parts of their tickets. If selected, the next option appears.

#### *Avoid deleting users who bought tickets with SmartConnect*

This checkbox appears when the previous option has been selected. By default it is enabled, suggesting that users who already bought tickets by credit card with SmartConnect not be deleted from the system.

#### *Delete disabled accounts on a daily basis*

Enable the automatic deletion of disabled user accounts on a daily basis.

### **Character set for Generated Passwords**

The second part of the main settings allows the choice of the default values for the passwords that are automatically generated, for example when creating bulk of tickets. The following values for the passwords can be customised: The length, whether to use uppercase and lowercase letters, numbers, or additional special characters. By default, passwords will be 6 character long and composed only by digits.

#### **Password recovery custom settings.**

When choosing to allow password recovery with custom setting, several configuration options appear, that are needed for a successful recovery process. The first one is the modalities by which recovery is done:

#### *Password recovery is done*

There are three choices for this option: via SMS, via e-mail, or both. Depending on the choice, different options appear, to configure how to send the SMS or the e-mail. Note that all options appear if both e-mail and SMS password recovery are enabled.

For the SMS recovery mode, there is only one additional option:

#### *Allowed country codes for password recovery*

It is possible to allow the sending of SMS only to those cell phones that belong to the selected countries. To add a new country code, start writing the country's name or code in the [Multiselect box](#) above the countries' list until the country's name appears in the box underneath, select it, and finally click on the + on the right of the country's name. Allowed countries appear in the right-hand side box and can be disallowed by clicking on the - on their right.

For the e-mail recovery mode, two options are available.

#### *Mail server*

The SMTP server used to send the recovery email. It is possible to choose among three option from the drop-down menu.

1. System SMTP server. To be able to choose this option, the Menubar › Proxy › SMTP must be activated.
2. Custom SMTP server. In this case, the name of the mail server can be specified in the textbox.

#### *Sender email address*

A custom e-mail address that will be used as the custom sender of the recovery e-mail.

An additional option is also available for both recovery modes:

#### *Limit password recovery to*

The interval of time that must pass before trying to recover the password another time. Only one out of four options can be selected from the drop-down menu: once every 10 minutes, once every 30 minutes, once every hour, and once every day.

## SmartConnect

On this page it is possible to configure the SmartConnect™ (self-service) and SmartLogin functionalities of the Hotspot. The SmartConnect™ system fully supports paid self-service ticket creation or the use of free tickets with no customer payment, while SmartLogin offers to the user the possibility to avoid the need of re-authenticate to the Hotspot closing and opening the browser. When not yet enabled, the first time this page is open, there is only one option available:

### **SmartConnect**

#### *Enable SmartConnect*

The SmartConnect™ feature is activated only if this checkbox is ticked.

As soon as SmartConnect™ is enabled, additional options will show up, to allow more control over this functionality:

#### *Self-Service user registration*

This drop-down menu allows to select the modality to notify the user of the successful account registration. Three mutually exclusive (i.e., only one can be selected at a time) options are available: via SMS, via E-mail, and no notification at all (disabled). Depending on the choice, additional options become available.

- Disabled: no additional options available. No new user can be created via SmartConnect™, though existing SmartConnect™ users are allowed to navigate and buy tickets.
- SMS. The activation of this option requires the availability of SMS bundles, used to send the confirmation to the user, that can verified under System › Event Notifications › SMS Notifications. Additional SMS bundles can be purchased from the Panda Perimetral Management Console. These additional options are available:

#### *Do not require phone number confirmation*

Disable the request to write twice the cellphone number to which to send the confirmation. Useful when compiling the request on a smartphone.

#### *Allowed Country Codes*

Only the cellphones that belong to the selected countries are allowed to register for SmartConnect™ access. To add a new country, start writing the country's name or code in the [Multiselect box](#) above the countries' list until the country's name appears in the box underneath, select it, and finally click on the + on the right of the country's name. Allowed countries appear in the right-hand side box and can be disallowed by clicking on the - on their right.

- E-mail. An e-mail with the access credentials is sent to the e-mail address provided during the registration process. A confirmation link is also included, that should be clicked for the user to successfully complete the process and activate the account. This option requires a smarhost or SMTP server.



#### *Do not require email address confirmation*

Disable the request to write twice the email address to which to send the confirmation. Useful when compiling the request on a smartphone.

#### *Ticket rate for email address verification*

This drop-down menu allows the selection of one among the available rates to allow a user to connect for a short time for her to read and receive the confirmation email.

#### Hint

The rates that can be selected here need to be defined as *time-based* and *pre-paid*, *from ticket creation* validity, and not enabled for SmartConnect™.

#### *Mail server*

This drop down menu allows the choice of the smarthost that will send the email with the access credentials. The available options are: *Custom mail server*, in which the URL of a customised mail server can be provided, *System smarthost*, and *System SMTP proxy*. The latter options are available only if a smarthost and a SMTP proxy have been configured and are running on the appliance.

#### *Sender email address*

A custom e-mail address that will appear as the sender of the confirmation e-mail.

### *Fields for user registration*

In this multiselect box it is possible to define which are the compulsory account's attributes to be provided during the registration process. The attributes that are presented to the user appear in the right-hand side column, along with the *required* or *optional* mark. The total number of optional or required attributes is shown at the top of the left-hand side.

#### Note

Depending on the User Registration type, some field are mandatory and cannot be disabled. When *registration by email* is enabled, *Username*, *Password*, and *Email address* are required, while when *registration by sms* is active, only the *Phone number* is required and will act as the username.

### *Limit free tickets per account*

The amount of free tickets that can be used by every account. The default option is "no limit", meaning that new tickets can be purchased at every moment, but there's the option "time limit" that allow users to purchase one new free ticket only every that given amount of minutes.

### *Enable Paid Tickets*

This option allows users to pay for Hotspot tickets by using Paypal or a credit card. When enabled, this feature allows to configure a PayPal account on which the payments will be collected.

#### Warning

If this option is activated while users are connected to the Hotspot, they will all be forcibly disconnected.

#### *Enable Paypal Sandbox*

This box enables or disables the PayPal sandbox for testing/demo purposes only: Using the sandbox permits to verify that the Paypal API integration works, without actually running live transactions with real money.

#### *Paypal API Username*

The PayPal API username.

#### *Paypal API Password*

The PayPal API password.

#### *Paypal API Signature*

The PayPal API signature.

#### Note

In order to properly setup the SmartConnect™ functionality of the Panda Hotspot and receive customer payments, it is necessary to sign up and create a PayPal account.

### **SmartLogin**

The SmartLogin functionality provides the Hotspot's users a convenient means to avoid a new authentication when reconnecting to the hotspot. In other words, when a user closes the browser, she later needs only to restart the same browser for an immediate access to the Internet, with no necessity to authenticate again. The SmartLogin functionality can be enabled globally for all Hotspot's users or individually for each user. In the latter case, SmartLogin works for those users even if it has not been activated globally, and can be enabled in the Login information section of the Accounts Editor.

The following options are available:

#### *Enable SmartLogin*

Tick the checkbox to enable SmartLogin for every user.

#### *SmartLogin cookie lifetime*

The time in days within the user has the possibility to use the SmartLogin functionality.

#### *Allow users to override SmartLogin cookie removal on logout*

When this option is enabled, in the user's [login portal](#) appears a new option (*Disable automatic login*) that gives her the choice to use or not the SmartLogin functionality.

Rates for email verification.

In order to allow the user to read the confirmation email, she should be allowed a quick free access to the Internet and to her mail account to read the credentials of the newly created account. Hence, a suitable rate with precise characteristics must be linked to the SmartConnect™ user registration process. In case no rates is yet available, a message describes the required options for this ticket, which can be created under Ticket › Rates. The ticket rates needs to be pre-paid, free, time-based, and not available for SmartConnect™. Moreover, they must also be defined with a 'From ticket creation' validity value. It is suggested that this value be limited to a few minutes, to give the user only the possibility to retrieve her credentials.

For help with the ticket rates creation, see also the online help.

## API

This section controls the settings of the Panda Hotspot's API, that allows the integration of the Hotspot of Panda Gatedefender Appliance into an already running system. Depending on the chosen *Mode*, different parameters can be set.

#### *Mode*

Version 2.5 of the Panda Gatedefender Appliance provides three different API modes: Panda's *generic API/JSON*, the *ASA jHotel*, and the *pcs phoenix* interfaces. The ASA jHotel and the pcs phoenix interfaces are only needed by hotels that use the ASA jHotel or the pcs phoenix hotel management software, respectively, whereas the generic API can be exploited to interact with other software systems. The three available modes are mutually exclusive, i.e., they can be activated one at a time. If there is one of the three interfaces enabled, and a different one is enabled, then only the latter is active, while the former is automatically disabled.

The other configuration options depend on the selected *Mode*. The following are the option to specify for the ASA jHotel mode.

#### *ASA jHotel Interface enabled*

By ticking this checkbox the ASA jHotel interface is enabled.

#### *ASA jHotel URL*

The URL of the ASA jHotel management interface. Its correctness can be tested by clicking on the *Test* button on the right of the input box.

Hint

In the sample URL provided, replace the *IP\_ADDRESS* of the ASA installation and the *COMPANY* name.

#### *Allow guest registration (Guest Login / SmartConnect)*

Allow a guest to self register by ticking this checkbox.

#### *Guest registration default rate*

Select the default rate that will be applied to new accounts from this drop-down menu. The available rates should already have been defined in Ticket › Rates.

#### *Allow non-free post paid tickets for guests that are not checked in.*

Tick the checkbox to allow non checked-in hotel guests to buy post paid tickets.

Hotspot access with the ASA jHotel management software.

Any user that already has an account in the ASA management software can quickly access the Hotspot without the need to create an account, provided that the Hotspot is correctly configured. The steps needed on the Hotspot are:

1. Tick the *ASA jHotel Interface enabled* checkbox and verify the the Hotspot can access the URL of the ASA jHotel interface.
2. Under Ticket › Rates, create a new *postpaid* rate, with *Ticket Code* the id used by ASA and give it a unique name (e.g., "my-ASA").

3. Go back to Settings › API, and choose the *ASA jHotel* mode and choose as *Guest registration default rate* the rate name created in the previous step ("my-ASA").

For the Generic API/JSON or the pcs phoenix interface, there are three options available:

#### *API enabled*

Tick the checkbox to enable the API.

#### *Accounting URL*

The Hotspot will send accounting information to this URL, to verify the data supplied by the user. Leave this field empty if the Hotspot should not accounting.

#### *Accounting URL requires HTTP Authentication*

If the URL provided in the previous option requires HTTP authentication, tick this checkbox. Two new text fields will appear to supply the username and password, respectively.

Finally, the API can be tested on the special page <https://GREENIP:10443/admin/api/>, in case the Generic API/JSON interface has been chosen.

## Language

The Language section allows to set all the language-dependent options and customise all the string shown in the various languages and the portal templates. The page is organised in two boxes: *Supported Languages*, *Edit Languages*, with a third one showing up depending on the *Edit* choice made in the second box.

### **Supported Languages**

In the first box it is possible to choose which languages are supported in the Hotspot and made available to the users. The languages must be selected in the multi-select box and then saved by clicking on the *Store* button. Only languages selected here will be available to the users during the registration process and when they connect to the portal.

### **Edit Languages**

In the second box it is possible to modify either one of the four portal templates or the user interface strings, for every language activated in the previous box. To personalise the templates and the strings, there are several variables that can be used. When a message shall be sent to a user -for example, she lost her account's password- each variable is replaced by an actual values, taken from the data stored in the Hotspot.

#### *Language*

The language for which to modify or add the translations. The available options from the drop-down menu depend on the activated languages.

#### *Edit*

The object(s) to modify. They can be either the *Portal Templates* or the *Portal Strings*. If the choice was to modify the *Portal Strings*, the editor is replaced by a list of the English words and sentences, used across the Hotspot's GUI and portal, each with an input box in which to write the translation in the chosen language. For the *Portal Templates* choice, one of the templates can be edited in the box that opens: *Welcome Page*, *Account Print*, *Terms of Service*, *Help*, *Email body*, and *Lost password email body*.

To learn more details on how to customise the portal, skip to [Hotspot customisation](#) below.

The content of each template can be changed and personalised with the help of a fully featured WYSIWYG editor.

#### Hotspot customisation

The portal presented to the users when they first connect to the Hotspot can be customised in several ways: the Language used in the portal, the text contained in the various pages, the CSS, the logo of the company running the Hotspot, and the portal's name. The last setting can be configured only from the CLI, while all other can be carried out from the Hotspot's administration interface, in the *Languages* section (Hotspot › Administration Interface › Settings › Languages)

#### Available languages.

There are six languages that are active by default: en (English, also used as default), de (German), it (Italian), ja (Japanese), es (Spanish), pt (Portuguese). A user connecting to the portal can select to customise each of the language. Additional languages can be served by the hotspot, by choosing them from the multi-select box the desired languages

#### Templates.

These are the templates that can be modified:

#### *Welcome Page*

The page presented to the user before logging in.

#### *Account Print*

A welcome message printed and handed out to the users after their registration along with their username and password. These are the variables that can be used: *\$title*, *\$firstname*, *\$lastname*, *\$username*, *\$password*.

#### *Terms of Service*

They are presented to the user when clicking the link next to the checkbox asking them to accept the Terms of Service before being able to login.

#### *Help*

The content of this page will be shown to the user as an help message.

#### *Email body*

The text to be included in the e-mail sent with the user's credentials upon registering, used when *registration by email* is active. These are the variables that can be used: *\$hotspot\_name*, *\$activation\_link*, *\$rate\_name*, *\$username*, *\$password*, *\$amount*, *\$price*, *\$currency*, *\$txn\_id*.

#### *Lost password email body*


The text to be included in the e-mail sent with the user's credentials , used when the user lost them and the *password recovery by email* option is selected. These are the variables that can be used: *\$username*, *\$password*

Each of the template can be edited for every language available on the hotspot and can make use of the pre-defined variables.

Text and images.

The content of the portal, be it images or text, can be modified from the editor, from which it is also possible to upload custom images, CSS and other files. To use the editor, go to the *Edit Languages* section, choose *Portal Templates* from the drop-down menu next to the *Edit:* label, then select the template from the drop-down menu below -labeled with *Template-* among those available:

- *Welcome Page*: The page that all the user see before connecting.
- *Account print*: The document to be printed and handed in to the user with her credentials.
- *Terms of Service*: The rules that user shall follow during the use of the Hotspot.
- *Help*: The page containing help and troubleshooting for the user.
- *Email body*: The text of the e-mail sent to the user as confirmation for the successful account creation.
- *Lost password email body*: The text of the e-mail sent to the user as a reminder of her credential to access the Hotspot.


In the editor at the bottom of the page it is possible to create documents with text and images. Adding images and custom files is indeed very simple: Put the cursor on the point in which to insert an image, then click on the  button to open a pop-up window called *Image Properties*. Here, in the *Image Info* tab, there are two alternatives to insert an image:

1. Provide an hyperlink to an image on the web in the *URL* textfield
2. Click on the *Browse Server* button to open a file browser and either choose an existing image on the server, or click on the *Choose File* button on the bottom of the page, to select an image from the local workstation, then click on the *Upload* button..

Hint

The uploaded files will be stored on the Panda Gatedefender Appliance into the `/home/httpd/html/userfiles/` directory. Custom files can be also directly uploaded e.g., via SSH in that location.

CSS.

Custom CSS files can also be used: Upload them to the Panda Gatedefender Appliance, placing them in the `/home/httpd/html/userfiles` directory. Like image files, they can be uploaded using the  button or via SSH.

The file shall be named:

- **hotspotcustom.css**, the CSS used for the administration interface
- **portalcustom.css**, the CSS used for the the Hotspot portal

- **miniportalcustom.css**, the CSS used for the Hotspot mini portal, i.e., the one with javascript disabled, tailored for mobile devices.

Hint

The original of these files can be found in the `/home/httpd/html/include` directory, and are named `hotspot.css`, `portal.css` and `miniportal.css`, respectively. They can be used as a basis for the custom ones.

Logo.

The logo that appears to the users on the portal can be replaced by using custom CSS `portalcustom.css` or `miniportalcustom.css` files. Upload the logo in the `/home/httpd/html/userfiles` directory (which shall be around 80x20 pixels in size), then modify the CSS files like:

```
div.logo img { display: none; }
div.logo { background-image: url('images/your-logo.png'); }
Hotspot name.
```

The operation of changing the domain name to the portal must be done manually from the CLI. The CLI access to the Panda Gatedefender Appliance can be enabled under Menubar › System › SSH access (see Section [Accessing the Panda Gatedefender Appliance](#) for directions).

Warning

Editing and modifying by hand any configuration file from the CLI file requires some acquaintance with the Panda Gatedefender Appliance internals, since a wrong edit to a file may cause a service to stop. It is recommended to be careful and it is suggested to save a backup copy of any file before editing it.

To change the Hotspot hostname and domain name, edit as root the file `/var/efw/hotspot/settings`, using e.g., the installed **nano** editor, and look for the lines, which are actually variable definitions (the values shown here are only examples):

```
HOTSPOT_HOSTNAME=hotspot
HOTSPOT_DOMAINNAME=example.com
```

Replace the values on the right-hand side (*hotspot* and *example.com*) with custom ones.

Moreover, since the connection to the captive portal is encrypted, a valid SSL configuration is also required, which amounts to create:

- a valid certificate (i.e., no **self signed** one)
- a private key file, not encrypted, and
- a file containing the SSL key chain for the certificate.

These files can be created in any directory, although the suggested best practice is to copy these files under `/var/efw/hotspot/` as well, to ensure that they are part of every configuration backup. Once all the certificates have been created, it is necessary also to make the Hotspot engine aware of their existence and to overwrite the default certificate settings, again editing the file `/var/efw/hotspot/settings` and add the following variables:

```
HOTSPOT_CERT=/<CUSTOM_PATH>/hotspot.example.com-cert.pem
HOTSPOT_KEY=/<CUSTOM_PATH>/hotspot.example.com-key.pem
HOTSPOT_CHAIN=/<CUSTOM_PATH>/hotspot.example.com-cabundle.pem
Remember to replace <CUSTOM_PATH> with the full path to the three certificates.
```

Finally, if an SSL key chain file is not needed, an empty value can be assigned to the last variable of the above configuration, like:

```
HOTSPOT_CHAIN=
Meaning of variables.
```

This is a complete reference for the variables that can be used when customising the Hotspot's portal templates and portal strings. They prove useful to compose messages tailored to each user: Whenever one of these variables appears in a template, it will be replaced by the corresponding value defined for that account. The variables are grouped together in three tables: [Table 1](#) contains variables that can be used in all portal templates, [Table 2](#) contains variables that can be used in the Print account template **only**, and [Table 3](#) contains variable used in the portal strings.

Table 1: Variables for all Portal Templates.

Variable	Replaced by
\$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
\$rate_name	The name of the Hotspot ticket rate
\$amount	The amount of traffic or time available
\$price	The cost of the ticket
\$currency	The currency in which the ticket was paid.
\$txn_id	The ID of the transaction.

The variables in the next table will be replaced in the printed account information by the values supplied in the corresponding fields of the account editor.

Table 2: Variables for the *Account Print* Portal Template.

Variable	Replaced by
\$language	The language of the user
\$birth_city	The city or town of the user's birth
\$birth_date	The date of the user's birth.
\$document_type	The document that identifies the user
\$document_party	
\$document_id	The ID of the document
\$street	The street in which the user lives
\$country	The country the user lives in
\$city	The city or town where the user lives
\$zip	The ZIP code of the user's city
\$description	The account's description
\$static_ip	
\$external_id	
\$phonenumber	The phonenumber supplied by the user
\$areacode	
\$email	The e-mail of the user

Variables for the Portal Strings.

Variable	Replaced by [string #]
<code>%(recovery_freq)s</code>	How frequently can a new password can be recovered [4]
<code>%(phonenumbers)s</code>	The user's phone number [9 42]
<code>%(transaction_id)s</code>	The transaction ID [9 11 28 31 37 42 44 105 121]
<code>%(email)s</code>	The user's e-mail address [11 44 121]
<code>%(grant_ticket_duration)s</code>	The minutes of the free Internet access [44, 121]
<code>%(seconds)s</code>	The number of seconds an user has to wait [55 113]
<code>%(home)s</code>	The link to the Hotspot's home page. [107]

Only a few of the portal strings (14 on 123) contain variables. For those 14 strings, it is required that every variable contained in the original string (e.g., string #4 *You are limited to one request every %(recovery\_freq)s.*) be contained also in the translated string.

The strings that contain some variables (and which) are the following:

4 `%(recovery_freq)s`

9, 42 `%(phonenumbers)s` and `%(transaction_id)s`

11 `%(email)s` and `%(transaction_id)s`

28, 31, 37, 105, `%(transaction_id)s`

44, 121 `%(grant_ticket_duration)s`, `%(email)s`, and `%(transaction_id)s`

55, 113 `%(seconds)s`

107 `%(home)s`

## Hotspot User

This section presents a list of the hotspot's (super)users, i.e., those who can perform different administrative tasks and are divided into two groups: A *Hotspot Administrator* can fully manage the hotspot interface but cannot access the Panda Gatedefender Appliance Main Menu, while a *Hotspot Account Editor* is allowed to only edit and enable or disable hotspot user accounts, by providing an existing username. Hence, an administrator has also the abilities of an Account Editor, but not vice-versa.

In this page, there is a list of users that shows their name, the group they belong to, and the actions available on the accounts. There is a default, protected administrator account, "hotspot", that can never be deleted. Available actions are to edit and to delete the user account: Deleting it will erase the user from the list, while edit will open the user editor (see below). When editing the `HOTSPOT` user, only its password can be changed, but neither its name nor its group can be modified.

An *Administrator* has access to the page <https://GREENIP:10443/admin/> and all the sections contained in it, which have been described in the whole Hotspot section of this guide. On the contrary, an *Account Editor* is granted access to the limited information editor page located at <https://GREENIP:10443/admin/infoedit/>, which is a simple web interface. Here, the Account Editor can insert an existing username, whose associated account information can be modified.

To add a user, simply click on the *Add user* link above the list. The *User editor* box will open, in which all the data necessary to the creation of a new user can be entered:

### *Username*

The username of the new account.

### *Group*

The group to which the new user belongs to. The drop-down menu allows to choose between the two available groups, *Hotspot Account editor* and *Hotspot Administrator*.

### *Password, Password (confirm)*

The password for the user that must be inserted twice as confirmation,

## Client Access to the Hotspot

This section describes the Hotspot user interface, the one seen by the clients when they connect via wireless to the hotspot. The portal appearance and settings can be customised by the hotspot administrator under [Menubar > Hotspot > Administration interface > Settings](#)

Before being able to surf the Internet, a user is required to access and log in to the hotspot. For this purpose, no software installation is necessary, since it suffices to run a browser and try to open any web page: The browser will be redirect to the hotspot's portal in which the user can login, register a new hotspot account or directly login and surf the Internet. The hotspot can serve to the client different type of portals, hence the client will see, depending on the device used, the portal for mobile devices, the one for browsers without JavaScript, or a generic one for all other types of device.

### Note

Since version 2.5, the user is not required to authenticate, if the hotspot is configured in user-less mode.

The login page is composed of two sections: On the left it is possible to choose the language of the interface from a drop-down menu and read an informative message. The section on the right is the login form, in which the user can proceed to login, register a new account, or buy a new ticket.

There are two versions for the login form: One for guest access, and one for registered user access. The former only works when ASA is running on the hotspot and encompasses the following options:

#### *Not a guest*

By clicking on this button, the login form for the registered user is shown, whose options are shown far below.

#### *Last name*

The last name of the guest

#### *First name*

The first name of the guest.

#### *Date of birth*

The guest's date of birth, in the form DD.MM.YYYY. (Example: 5th of February 1980 becomes 05.02.1980).

#### *Login*

After providing the required information, a click on this button will allow the access to the hotspot.

The login form for the registered users shows the following options.

#### *Username*

The username of the user.

#### *Passwords*

The password of the user.

#### *Register new account*

Non-registered users can create a new account to surf the Internet. This is only allowed when SmartConnect™ is running on the hotspot. The procedure for the new account setup can be found [below](#).

#### *Add ticket*

The user can buy a ticket, which is a mandatory requirement for accessing the hotspot. This option is also available when SmartConnect™ is activated.

#### *Login*

After providing the login credentials, a click on this button will allow the access to the hotspot.

When the hotspot is configured to accept the Terms of Service, after clicking on the *Login* button on either case, a window will open, with one button on the window's underside:

#### *I accept the terms of service*

By clicking on this link, a window will open that shows the terms of service.

### **Register new account**

Upon clicking on the new *Register new account* button, a four steps wizard will open, in which to set up and activate a new hotspot account. In the first step the user account is created, for whose successful creation the following mandatory data are required:

#### *First name, Last Name*

The name and surname of the user.



#### *Street, Postal code, City, Country*

The address, ZIP code, city, and Country where the user lives in.

#### *Phonenumber to receive the username and password*

The country code of the user's phone number, chosen among those available in the drop-down menu, followed by the user's actual phone number.

#### *Confirm Phonenumber*

Re-enter the phone number as confirmation.

It is also necessary to tick the checkbox next to the *I accept the terms of service* link for the account to be created. Clicking on the link will open a window with the terms of service, that can be read before accepting.

When all the data have been supplied, a click on the *Register* button on the bottom right of the form will lead to the second step. After registering, a SMS with the username and password will be sent, that will authorise the login to the hotspot.

In step two a ticket can be selected from a drop-down menu that will be associated to the account, and will grant the use of the hotspot to access the Internet. Depending on the hotspot setup, the choice can be only among free tickets or also among prepaid or postpaid tickets. For each available ticket, its name, duration, and cost are displayed. For this option to work, SmartConnect™ must be activated on the hotspot, and payments via PayPal should be set up.

After the selection of a ticket, click on the *Continue* button to proceed to step three.

#### **Note**

While there is no limit in the purchase of prepaid and postpaid tickets, it is not allowed to have time-based and traffic-based ticket at the same time. In other words, a client possessing one or more valid time-based ticket, cannot buy any traffic-based ticket until all the valid time-based tickets associated with the account have been consumed or expired. The same applies to traffic-based tickets: All of them must be used or expired before being allowed to purchase a time-based ticket.

In step three, choosing a ticket which requires payment, will redirect to the PayPal website where to provide the necessary data for the transaction and complete the purchase of the ticket using a credit card or an own PayPal account. Otherwise, if a free ticket has been selected, this step will be simply skipped and the process continues to step four.

In step four appears a message that informs of the successful registration or, if some part of the registration process were not successful, an error message will be displayed. In any case, also the **transaction ID** string will be reported. The transaction ID should be written down for future references or used in case of any problem has arisen during the registration process or if some issue will happen during the connection. In the former case, quickly contact an hotspot administrator to complete the registration and obtain the login credentials.

#### **Login**

When logging in after providing username and password, an informative panel on the page will display various details about the connection status. This page must remain open: If closed, the session will be immediately ended and a new log in to access the hotspot must be made. The following information are shown on the page:

#### *Remaining time*

The total time still to consume. The *unlimited* string appears when using a traffic-based ticket.

#### *Session time*

The duration of the current session.

#### *Remaining traffic*

The amount in Mb of Gb of the traffic available for the current ticket. The *unlimited* string appears when using a time-based ticket.

#### *Session traffic*

How much data have been exchanged while browsing. A total amount is given, as well as the amounts of downloaded and uploaded data within bracket.

#### *Idle timeout*

A countdown that shows the device's idle time, i.e., the time since the last activity between the device and the hotspot. When the countdown reaches 0, the device will automatically be disconnected.

#### *Session start time*

The timestamp of the session's starting time.

#### *Disable automatic login*

When the checkbox is ticked, the user will need to authenticate upon reconnection, regardless of the Smartlogin settings. Otherwise, when the checkbox is not ticked, there is no need for the user to authenticate upon reconnecting to the hotspot.

#### Note

This option only appears if the SmartLogin functionality has been enabled by the Hotspot administrator.

On the bottom of the panel two buttons appear.

#### *Start browsing*

By clicking on this button, located on the left-hand side, a new tab will open in the browser, that leads to the hotspot's home page.

#### *Logout*

Clicking on this button immediately logs out from the hotspot.

#### **Add ticket**

Before accessing the hotspot and the Internet, the user must own a valid ticket. The procedure to purchase a ticket is the same as the one described in step two and step three of the registration process.

# 10. The Logs and Reports Menu

---

In the logs section of the Panda Gatedefender Appliance the logs can be extensively viewed and their management can be done.

The sub-menu on the left-hand side of the screen contains the following items:

- Dashboard - the brand new reporting module
- Live Logs - get quick, live view of the latest log entries as they are being generated
- Summary - get daily summaries of all logs
- System - system logs (`/var/log/messages`) filtered by source and date
- Service - logs from the intrusion detection system (IDS), OpenVPN, and antivirus
- Firewall - logs from iptables rules
- Proxy - logs from the HTTP, SMTP, and content filter proxies
- Settings - customise all the log options
- Trusted Timestamping - securely time stamp the log files to verify they have not been altered.

In a nutshell, there are two modalities to access the log from the GUI: Live and "by-service": In the live mode the log files are visualised as soon as they are created, while in the "by-service" mode only the logs produced by one daemon or service are displayed.

## Dashboard

The reporting GUI is a new module, introduced in version 5.50, whose purpose is to graphically show the occurrence of various types of event on the system.

In a nutshell, the reporting module shows events happened on the Panda Gatedefender Appliance using different widgets and graphs. All events occurring on the system and the information concerning them recorded by the syslog daemon are parsed and used to populate a sqlite3 database. From here, data are gathered according to the options and filters applied in the GUI and are displayed by the widgets.

Note

This module is loosely coupled with the *Event notifications* located in Menubar › System › Event notifications. All events recorded there, and for which email or SMS alerts are sent, appear also here, but the vice-versa is not true.

This page is divided into six tabs: *Summary*, *System*, *Web*, *Spam*, *Attacks*, and *Virus*. Except for the first tab, which shows an overview of all events, each of them is dedicated to a precise service running on the Panda Gatedefender Appliance.

## Common elements

All the tabs share the same design: Below the tabs, on the left-hand side there are a date selector on the the left-hand side and a *Print* button on the right-hand side. Then, a line chart at with an horizontal slider right below, atop one informative boxes (*Summary Grid*) and a pie-chart. At the bottom, there are one or more tables, depending on the tab and the data shown. The table that is always present is the one displaying the syslog messages related to the events shown.

More in detail, here is a description of all the widget present in the reporting module.

### *Date selector*

At the top left-hand side of the GUI there is an hyperlink that shows the interval within which occurred those events that have been considered for the charts. By clicking on it, a small panel gives access to other choices of intervals. There are two types of choices, the first one concerns events that took place in the *last ... days*, namely events from the last day, week month, quarter, or year; the second one selects all the events occurred in one of the last 12 months. Upon selecting a new time span, the other widgets are also updated. There is also the possibility to not change the interval shown, by clicking on *Cancel*.

### *Print*

A click on this button shows a print preview of the current page, in which the *Back* button replaces *Print*, and open a pop up window in which to choose the printing device.

### Line Chart and Time Slider.

The line chart shows the event happened on the Panda Gatedefender Appliance during the selected time span in a two dimensional graph, in which the x-axis shows the time interval and the y-axis shows the number of occurrences. A coloured line connects events of the same type.

## Hint

Different types of event are denoted with different colours.

The time slider is located underneath the chart and allows, within the selected time span, a more fine-grained view of the events, depicted here as histograms. Indeed, the two grey handles on the left and right limits of the slider can be clicked and dragged to reduce the time span shown in the line chart. When reduced, the slider can also be moved by clicking in its middle and dragging it to the left or the right.

## Summary Grid

The summary grid has a twofold purpose: On the one hand to show the number of occurrences of the various types of events that took place on the Panda Gatedefender Appliance in the selected period, whereas on the other end to filter which type of events are shown in the line chart. Its content changes according to the tabs it is located, i.e., to the types of events logged. The summary grid is not present in the *Mail*, *Attacks*, and *Virus* tabs, in which is replaced by a number of tables with details about the events.

## Pie Chart

The pie chart diagram shows graphically the number of event that took place in the selected time span. When in the *Summary* tab, each slice can be clicked, to open the tab corresponding to the type of event and show a more detailed representation.

## Syslog table

A table that shows the syslog messages extracted from the log files and related to the events shown in the charts. When the table carries lot of messages, these are divided into many pages and can be browsed using the buttons and number at its left bottom. At the right bottom there is an icon that allows to refresh the table's content.

## Summary

The *Summary* tab gives an overview of all categories of events recorded on the Panda Gatedefender Appliance. The summary grid allows to filter the following types of events:

- System (Green). Number of Log ins and other events connected with system administration tasks (e.g., uplinks change of status, start and stop of logging, and so on) .
- Mail (Dark Grey). Number of spam e-mail received.
- Web (Blue). Number of pages blocked by the content filter.
- Virus (Red). Number of viruses found.
- Intrusion attempts (Yellow). Events recorded by the IPS.

Each category can be shown separately, with more information and a higher level of details in the other tabs of the page, see further on.

## System

The *System* tab displays all events that are related to the system efficiency and to system administration. These are all the events shown:

- Uplink (Red). The times the uplink(s) went online or offline.
- Status (Dark Grey). Changes in the state of the Panda Gatedefender Appliance
- Login (Blue). The number of logins, both successful and not.
- Disk (Yellow). Events involving disk I/O.
- Upgrade (Green). Events involving upgrade of system or of packages.
- Support (Light Grey). Number of accesses and operations donw by the Support Team.

A click on the small icon on the left-hand side of each event category causes the other categories to not be shown, while the current is further detailed and the pie chart is updated.

## Web

The *Web* tab displays the number of pages that have been blocked by the URL filter engine. The summary grid is composed by two tabs: *Access report* and *Filter report*. The former shows the blocked URL divided by *Source IP Address*, *URL*, and *Users* that have been blocked, and the total count for ever item, each in a table.

The latter tab shows in the first table, the following categories, that are those found in the Web filter (See Menubar › Proxy › HTTP › Web Filter).

- General Use (Green).
- Parental Control (Yellow).
- Productivity (Blue).
- Security (Red).
- Uncategorized Sites (Dark Grey).

Like in the case of the *System* tab, a click on the small icon on the left-hand side of each event category causes the other categories to not be shown, while the current is further detailed and the pie chart is updated.

The other tables at the bottom show the counts of each the blocked objects: The *Source IP Addresses*, the *URLs*, and the *Users*.

## Mail

The *Mail* tab displays all e-mails blocked as spam.

There is no summary grid in this tab, replaced by three tables, displaying counts for:

- From. The sender(s) of spam e-mails.
- To. The recipient(s) of spam e-mails.
- Source IP Address. The IP address from where spam e-mail have been sent.

## Intrusion attempts

The *Intrusion attempts* tab displays all tentative intrusions detected by the IPS (See Menubar › Services › Intrusion Prevention).

The tables at the bottom show counts of the following information:

- Intrusion attempts: The categories under which falls each attempt.
- Source IP Address. The IP address from where the attack originated.
- Destination IP Address. The IP Address to which the attach was launched.

## Viruses

The *Viruses* tab displays all viruses intercepted by the anti-virus engine (See Menubar › Services › Antivirus Engine).

The tables at the bottom show counts of the following information:

- Virus Name. The name of the virus found.
- Source IP Address. The IP address where the virus originally was located.
- Destination IP Address. The IP Address to which the virus was propagated.

## Connections

The *Connections* tab displays the average number of connections started by the users of the Panda Gatedefender Appliance, grouped into:

- Local connections. Accesses via SSH or console.
- Hotspot users. Users accessing the Hotspot.
- IPsec users. Clients connected via IPsec.
- OpenVPN users. clients connected using VPN.

## Traffic Monitoring

The ntopng software is the successor of the ntop network traffic analyser, which adds a more intuitive interface and more graphical representations of the traffic that flows through the Panda Gatedefender Appliance.

The management interface of ntopng provides now more usability and can be accessed easily accessed from any browser, and therefore has been integrated more tightly with the Panda Gatedefender Appliance interface than in previous versions.

In few words, the abilities of ntopng can be summarised as follows:

- Real time monitoring of every network interface of the Panda Gatedefender Appliance.
- Web-accessible management interface.
- Less resource needed compared to ntop.
- Integration of nDPI (Application firewall).
- Traffic analysis according to different parameters (protocol, source/destination).
- Export of reports in JSON format
- Storage of traffic statistics on disk.

The ntopng GUI is organised into four tabs: *Dashboard*, *Flows*, *Hosts*, and *Interfaces*. Moreover, there is also a search box to quickly display information about a given host.

In the footer of each tab, a couple of information are shown: Besides a copyright notice and a link to the ntop home page, there is a chart showing the network traffic over the last 20 seconds, updated in real time, and some numerical data about the current bandwidth used, the number of hosts and flows and the Panda Gatedefender Appliance's uptime.

## Dashboard

The dashboard shows all connections that interest the Panda Gatedefender Appliance, that is, all established *Flows* in which the Panda Gatedefender Appliance is involved.

The page is divided into several diagrams, with the first one -a so-called [Sankey diagram](#) showing all flows moving on the Panda Gatedefender Appliance, updated in real time. The horizontal flows show the traffic between two hosts, while the vertical width of each flows is proportional to the bandwidth used by that flows, i.e., to the amount of data flowing. The connections -and therefore the direction of the data sent- are shown left to right: Hosts on the left hand-side of the diagram send data to hosts on the right-hand side and are identified by either their IP address or hostname. A click on one host leads to the *Overview* page in the [Hosts](#) tab, which shows several information about that host.

Below the Sankey diagram, four informative-only pie charts show in percentage the items that that generate the most traffic, divided into: Total by host (top left); application protocols (top right), ASNs (bottom left), and live flow senders (bottom right).

## Flows

The active flows tab contains a big table with a number of information about the active flows:

- *Info*. A click on the icon opens a new page in which more detailed information about that flow is shown.
- *Application*. The application causing the flow. nDPI is used to recognise the application, therefore it might be necessary to wait for a couple of packets to see the correct application displayed: In this case, the (*Too Early*) message appears instead of the application name.
- *L4 Proto*. The network protocol used by the flow, which is usually TCP or UDP.
- *Client*. The hostname and port used by the flow on the client side. Clicking on either the hostname or port, more information will be shown in a new page about the network traffic flowing that host or port.
- *Server*. The hostname and port used by the flow on the server side. Like for the *Client* above, more information is shown when clicking on the hostname or port.

Hint

By clicking on the hostname or port, the table shows detailed information about it, opening a sub-tab in the [Hosts](#) tab.

- *Duration*. The length of the connection.
- *Breakdown*. The percentage of traffic generated by the client and by the server.
- *Throughput*. The amount of data currently exchanged between the client (on the left, in black) and server (on the right, in green).
- *Total Bytes*. The total data exchanged since the connection was first established.

At the bottom of the table, on the left-hand side it is shown the total number of rows shown, while on the right-hand side it is possible to browse the various pages in which the table is split, when the number of rows is higher than the pagination.

A click on the *Info* icon will give detailed information about that particular flow. Besides those already described above, these additional data are displayed.

- *First Seen*. The timestamp when the connection was established, along with the time passed since.
- *Last Seen*. The timestamp in which the connection was last active and the time passed since that moment.
- *Client to Server Traffic*. The number of packets and bytes sent from the client to the server.
- *Server to Client Traffic*. The number of packets and bytes sent from the server to the client.
- *TCP Flags*. The TCP states of the current flow.

It is possible to go back to the list of flows by clicking on the *Flows* hyperlink on the left, right above the table.

## Hosts

The *Hosts* tab allows to view several details about the involved parties of a flow: Host, port, application, flows and their duration, data exchanged, and so on.

Two representations are available: *Host List* and *Top Hosts (Local)*

The *Hosts List* representation shows information about all the hosts involved in some flow with the Panda Gatedefender Appliance and the following data about them:

- *IP Address*. The IP address or MAC Address of the host. The latter is shown if the DHCP lease for that host has expired.
- *Location*. Whether the host is in the local or in a remote network.
- *Symbolic Name*. If available, it is the hostname of the host.
- *Seen Since*. The timestamp of the first established connection.
- *ASN*.
- *Breakdown*. The trade-off between sent and received traffic.
- *Traffic*. The amount of data exchanged by the host.

A click on the IP address opens an overview of the host, showing several information about it, besides those listed above:



- *Last Seen*. The timestamp in which the connection was last active and the time passed since that moment.
- *Sent vs Received Traffic Breakdown*. The traffic generated or received by the host.
- *Traffic Sent*. The number of packets and bytes sent from the client to the server.
- *Traffic Received*. The number of packets and bytes sent from the server to the client.
- *JSON*. Download information about the host in JSON format.
- *Activity map*. How many flows have seen the host involved at a given timestamp. Each square shows a minute and the darker the colour, the more flows have taken place in that minute.

From here it is also possible to open additional informative tabs about that host. Each tabs contains one or more pie charts (except for the *Contacts* and *Historical* tabs) above a textual summary of the data displayed.

- *Traffic*. The network protocol used by the host. (TCP, UDP and ICMP being the most common).
- *Packets*. The length in packets of each flow. (note: just my guess)
- *Protocols*. The application protocol used by the host.
- *Flows*. The table with all the network flows from the hosts.
- *Talkers*. The Sankey diagram of the connections, very similar to the one shown in the Dashboard, which however shows only the most active flows.
- *Contacts*. This tab is slight different from the others. It shows on top an interaction maps and on the bottom a list of connection that have the host as client or receiver.
- *Historical*. An interactive graph that shows the history of the traffic flown from and to the host in a given timespan (up to one year), that can be selected above the graph.

The *Top Hosts (Local)* representation shows a real-time graphic of the hosts that have active connections to the host. It displays the last 30 minutes.

## Interfaces

The *Interfaces* tab allow to select the network interface, among the active ones, whose traffic should be displayed.

Note

It is currently not possible to select flows and/or hosts from different interfaces

## Live

When entering in the *Logs* section, or clicking on the *Live* entry on the sub-menu, the *Live log viewer* is shown, a box showing the list of all the log files available for real time viewing. Any number of logs to see can be chosen by ticking the corresponding checkboxes, that are displayed in a new window upon clicking on the *Show selected logs* button. To watch all the log files at once, simply tick the *Select all* checkbox right above the *Show selected logs* button and then click on the latter button. Otherwise, to view only one log file, simply click on the *Show this log only* link.

The window that opens contains two boxes, *Settings* at the top and *Live logs* at the bottom.

Warning

The list of log entries can become nearly unreadable if many logs are showed, due to the possible high number of log entries produced (especially by the firewall or proxy log, which can generate several log entries per second in case of heavy traffic). In this cases, the logs to be displayed can be configured in the *Settings* box.

### Settings

This box allows to modify the settings of the log viewer, including which of the log files to show, their colour and options to highlight or find specific keywords.

On the right-hand side of the box appears the list of the logs that are currently displayed, and the colour with which they are highlighted, while on the left-hand side some additional control elements are shown, that help limit the output:

*Filter*

Only the log entries that contain the expression in this field are shown.

### *Additional filter*

Like the filter above, but applied to the output of the first filter. In other words, only log entries containing both expressions are shown in the log.

### *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, quickly scrolling the old ones.

### *Highlight*

All the log entries that contain this expression will be highlighted in the chosen colour. The difference with the filtering option is that all the content is still displayed and the log entries containing the expression will be highlighted with a coloured background.

### *Highlight color*

Clicking on the coloured square gives the choice to select the colour that will be used for highlighting.

### *Autoscroll*

This option is only available if the *Sort in reverse chronological order* option in the Menubar › Logs › Settings section is turned off. This causes all the new entries to be shown at the bottom of the page: If this option is enabled, the list is scrolled upwards to show the latest entries at the bottom of the page, otherwise only the older entries are shown and the scrollbar on the right should be used to see the new ones.

To add or remove some log from the display, click on the *Show more* link right below the list of the log files on the top right. The controls will be replaced by a table from which the desired log files can be selected by ticking or unticking their respective checkboxes. To change the colour of a log file, click on the colour palette of that log type and then choose a new colour. To show the controls again, click on one of the Close links below the table or below the list of the displayed log files.

## **Live logs**

The logs chosen for viewing are shown in this box, which consists of a table divided in three columns.

### *Left column*

This column contains the log name, that is, the daemon or service producing the log entry.


### *Middle column*

The time stamp (date and time) of the event that has been recorded.

### *Right Column*

The actual message generated by the service or daemon and recorded in the log files.

### *Note*

Some log messages -especially Firewall entries- span more than one line, denoted by the  button at the right of the message. To show the whole message, click on it or on the button.

Finally, there is also the chance to increase or decrease the window size by clicking on the *Increase height* or *Decrease height* buttons, respectively, which are situated on the heading of the box.

## **Common actions**

The sub-menu entries *System*, *Service*, *Firewall*, and *Proxy* show log files for different services and daemons, grouped by similar characteristics. Several controls are available to search within the log, or view only some entries of the log, many of which are the same in all the services and daemons, with only the *System* menu item and the *HTTP report* tab under *Proxy* that have some additional control. These sub-menu entries have also a common structure of their pages, organised in two boxes: *Settings* at the top and *Log* at the bottom.

### *Filter*

Only the lines that contain the entered expression are shown.

### *Jump to Date*

Directly show log entries from this date.

### *Jump to Page*

Directly show log entries from this page in the result set. The number of entries shown per page can be modified on the Menubar › Logs › Settings page.

#### Update

After changing any of the settings above, a click on this button refreshes the page content. The page is not refreshed automatically.

#### Export

When clicking on this button the log entries are exported to a text file.

#### Sign log

When clicking on this link, the current log is signed. This button is only available if [Trusted Timestamping](#) is enabled.

#### Older, Newer

These two buttons are present in the *Log* box and show up whenever the number of entries grows too much and are divided into two or more parts. They allow to browse older or newer entries of the search results by clicking on them.

#### Note

A message at the top of the page informs if on a given date there are no logs available: This can happen either if the daemon or service were not running, or if they did not produce any message.

In the remainder of this section, all the services and their peculiar settings are presented.

## Summary

This page presents summaries for the logs produced by the Panda Gatedefender Appliance, separated by days and generated by the **logwatch** log monitoring software. Unlike the other parts of the log section, it has its own settings to control the level of details shown. The following control elements are available in the first box at the top of the page.

#### Month

Select from this drop-down menu the month in which the log messages were generated.

#### Day

The second drop-down menu allows to pick the day in which the log messages were generated.

#### <<, >>

Browse the history, moving from one day (or part of it when too many messages have been generated) to another. The content of the page will be automatically refreshed.

#### Update

Immediately refresh the content of the page when the month/day combination has been changed.

#### Export

When clicking on this button, a text version of the summary is shown and can be saved on a local filesystem.

Below the *Settings* box, a variable number of boxes appears, depending on the running services that have log entries. The *Disk Space* box should at least be visible, showing the available disk space on the chosen date, while other boxes that can show up include *Postfix* (mail queue) and *Firewall* (accepted and dropped packets)

Note that the summaries are not available for the current day, as they are generated every night from the log files generated the day before.

## System

In this section appears the log viewer for the various system log files. The upper box, *Settings*, defines the criteria to display the entries in the lower box. Besides the [common actions](#), one additional control is available:

#### Section

The type of logs that should be displayed, either *All* or only those related to a given service or daemon. Among others, they include kernel messages, SSH access, NTP, and so on.

Following the choice of the section, click on the *Update* button to refresh the logs displayed in the *Log* box at the bottom of the page, in which the *Older* and *Newer* buttons allow to browse the pages.

## Service

In this section appear the log entries for three of the most important services provided by the Panda Gatedefender Appliance: IDS, OpenVPN, and the Panda anti-virus, each in its own tab. Only the [common actions](#) are available.

## Firewall

The firewall log viewer contains the messages that record the firewall's activities. Only the [common actions](#) are available.

Information shown in the table are:

### *Time*

The timestamp at which the message was generated.

### *Chain*

The chain through which the packet has passed.

### *Iface*

The interface through which the packet has passed.

### *Proto*

The prototype of the packet.

### *Source, Src port*

The IP address and port from which the packet has arrived.

### *MAC address*

The MAC address of the source interface.

### *Destination, Dst port*

The IP address and port to which the packet had to arrive.

## Proxy

The proxy log viewer shows the logs for the four daemons that use the proxy. Each of them has its own tab: squid (*HTTP*), icap (*Content filter*), sarg (*HTTP report*), and smtpd (*SMTP*, email proxy).

## HTTP and Content filter

In addition to the [common actions](#), the log viewer for the HTTP proxy and content filter allow these values to be specified:

### *Source IP*

Show only the log entries containing the selected source IP Address, chosen from a drop-down menu.

### *Ignore filter*

A regular expression that filters out all the log entries that contain it.

### *Enable ignore filter*

Tick this checkbox to temporarily disable the ignore filter.

### *Restore defaults*

Clicking on this button will restore the default search parameters.

## HTTP Report

The *HTTP report* tab has only one option: To enable or not the proxy analysis report generator, by ticking the *Enable* checkbox and clicking on the *Save* button afterwards. Once the report generator is activated, a click on the *Daily report*, *Weekly report*, and *Monthly report* links shows detailed HTTP reports.

## SMTP

Only the [common actions](#) are available in the tab of the postfix daemon.

## Settings

This page contains all the global configuration items for the Panda Gatedefender Appliance's logging facilities, organised into four boxes: *Log viewing options*, *Log summaries*, *Remote logging*, and *Firewall logging*

### Log viewing options

#### *Number of lines to display*

The pagination value, i.e., how many lines are displayed per log-page.

#### *Sort in reverse chronological order*

If this checkbox is ticked, then the newest log entries will be displayed first.

### Log summaries

#### *Keep summaries for \_\_ days*

How long should the log summaries be stored on disk before deletion.

#### *Detail level*

The detail level for the log summary: the higher the level, the more log entries are saved and showed. The drop-down menu allows three levels of detail: Low, Medium, and High.

### Remote logging

#### *Enabled (Remote Logging)*

Ticking this box allows to enable remote logging. The next option allows to enter the hostname of the syslog server.

#### *Syslog server*

The hostname of the remote server, to which the logs will be sent. The server must support the latest [IETF](#) syslog protocol standards.

### Firewall logging

#### *Log packets with BAD constellation of TCP flags*

If this option 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*

With this option enabled, all new TCP connections without SYN flag will be logged.

#### *Log accepted outgoing connections*

To log all the accepted outgoing connections this checkbox must be ticked.

#### *Log refused packets*

All the refused packets will be logged by the firewall, if this option is enabled.

## Trusted Timestamping

Trusted timestamping is a process that log files (but in general any document) undergo in order to track and certify their origin and compliance to the original. In other words, trusted timestamping allows to certify and verify that a log file has not been modified in any way by anyone, not even the original author. In the case of log files, trusted timestamping proves useful for example, to verify the accesses to the system or the connections from the VPN users, even in cases of independent audits.

Trusted timestamping is not enabled by default, but its activation only requires a click on the grey switch. When it turns green, some configuration options will show up.

#### *Timestamp server URL*

The URL of the timestamp server (also called TSA) is mandatory, since it will be this server that signs the log files.

#### Note

A valid URL of a valid TSA is needed to be able to use trusted timestamping. Several Companies can supply this kind of service.

#### *HTTP authentication*

If the timestamp server requires to authenticate, tick the box below the *HTTP authentication* label.

#### *Username*

The username used to authenticate on the timestamp server.

#### *Password.*

The password used to authenticate on the timestamp server.

#### *Public key of the timestamping server*

To ease and to make the communication with the server more secure, the server's public key can be imported. the certificate file can be searched on the local computer by clicking on the *Browse...* button, and then uploaded to the Panda Gatedefender Appliance by clicking on the *Upload* button. After the certificate has been stored, next to the *Public key of the timestamping server* label, a *Download* link will appear, that can be clicked to retrieve the certificate, for example if it should be installed on another Panda Gatedefender Appliance.

After clicking on the *Save* button, the settings are stored and, on the next day, a new button will appear in the *Logs* section, on the right-hand side of the *Settings* box:

#### *Verify log signature*

When clicked it will show a message in a yellow callout to inform about the status of the log.

#### See also

The official [OpenSSL timestamping documentation](#) and [RFC 3161](#), the original definition of the Time Stamp Protocol.

# 11. Glossary

---

## Box

A box is an element of the page of a service, that contains several configuration option.

## Client

is a user connecting to the hotspot. It is sometimes called hotspot user

## GREEN IP

is the IP Address of the GREEN zone, i.e., of the LAN in which the Panda Gatedefender Appliance is located.

## Module

By module it is intended each of the items displayed in the Main Navigation bar (*System, Status, Logs* and so on), which groups together a set of functionalities.

## Multiselect box

A special box which displays a list of available items on the right-hand side, a list of 'active' or selected items on the left-hand side, and a search textbox on top. Some also allow to specify, for each allowed item, a characteristic (e.g., that the item is required or optional).

## Pagination

Pagination allows table containing lot of entries to be split into two or more parts when the number of entries exceeds the pagination value, showing only one part at a time. Currently available only for the hotspot and the logs, this value can be defined under Hotspot › Settings and Menubar › Logs › Settings. It is possible to browse through the pages by clicking on the *First, Previous, Next, and Last* links above the table.

## Plugin

Plugins are the boxes present in the dashboard.

## Smarthost

An SMTP relay server that instead of delivering an e-mail directly to the recipient, sends it to an intermediate server that will carry out the final delivery. Smarthosts usually require authentication, as opposed to *open relay server*, who do not.

## Tab

Tabs are sub-pages of a main service that are used to split and keep organised all the configuration option of that service.

## The Zones

Each of the 4 subnets managed by the Panda Gatedefender Appliance: GREEN, RED, BLUE, and ORANGE.

## User

is someone who uses the Panda Gatedefender Appliance.

## User agent

The *user agent* of a web browser is the string that every browser sends as identification when requesting a web page. It contains several information about the browser and the system. For example:

```
Mozilla/5.0 (X11; U; Linux i586; it; rv:5.0) Gecko/20100101 Firefox/5.0
```

A complete list of user agent strings can be found on the <http://www.useragentstring.com/> website.

## Widget

An element of a GUI that displays information and can sometimes be interactive, i.e., a user can interact with it to change the information present within it.



# APPENDIX A. Quicksheet - Where Can I...?

## Hotspot

- **Administer the hotspot:** Menubar › Hotspot › Administration interface or <https://GREENIP:10443/admin/> (remember trailing '/!').
- **Edit hotspot user account:** <https://GREENIP:10443/admin/infoedit/> (remember trailing '/!').
- **Add hotspot user account:** Menubar › Hotspot › Accounts › Add new account.
- **Enable SmartConnect and SmartLogin:** Menubar › Hotspot › Administration Interface › Settings › SmartConnect.

## Network

- **Enable/Disable BLUE/ORANGE zone:** Menubar › System › Network configuration, Step 2.
- **Change hostname and domainname:** Menubar › System › Network configuration, Step 3.
- **Change domainname by zone:** Menubar › Services › DHCP server.
- **Add uplink:** Menubar › Network › Interfaces.
- **Limit bandwidth per interface:** Menubar › Services › Quality of Service.
- **Add/Configure VLAN** Menubar › Network › Interfaces › VLANs.
- **Configure anti-spyware and anti-malware:** Menubar › Proxy › POP3 › Spam filter, Menubar › Proxy › DNS › Anti-spyware.
- **Configure anti-spam:** Menubar › Proxy › SMTP › Spam settings, Menubar › Services › Spam Training.
- **Configure anti-virus:** Menubar › Services › Antivirus Engine, Menubar › Proxy › [HTTP/POP3/FTP/SMTP].

## Miscellaneous

- **Modify default e-mail address:** Menubar › System › Network configuration, Step 6.
- **Open a support ticket:** Menubar › System › Support.
- **Change GUI language:** Menubar › GUI settings.
- **Visualise the license:** Menubar › System › License agreement.
- **Configure Trusted timestamping:** Menubar › Logs › Trusted Timestamping.
- **Reset to factory defaults:** Menubar › System › Backup.

# APPENDIX B. 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.

### 1. 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:

1. 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.
2. 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.
3. State on the Title page the name of the publisher of the Modified Version, as the publisher.
4. Preserve all the copyright notices of the Document.

5. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
6. 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.
7. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
8. Include an unaltered copy of this License.
9. 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.
10. 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.
11. 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.
12. 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.
13. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
14. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
15. 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.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright (c) YEAR YOUR NAME. 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".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.



Panda Gatedefender v.5.50  
2015-11-30

© Panda Security 2015. All rights reserved.

Neither the documents nor the programs that you may access may be copied, reproduced, translated or transferred to any electronic or readable media without prior written permission from Panda Security, C/ Gran Vía Don Diego Lopez de Haro 4, 48001 Bilbao (Bizkaia) SPAIN.

Registered trademarks.

Windows Vista and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other product names may be registered trademarks of their respective owners.