COMODO
Creating Trust Online®

COMODO DOME
FIREWALL

Comodo **Dome Firewall**

Software Version 2.3

Dome Firewall Virtual Appliance Administrator Guide

Guide Version 2.3.020618

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction to Comodo Dome Firewall - Virtual Appliance

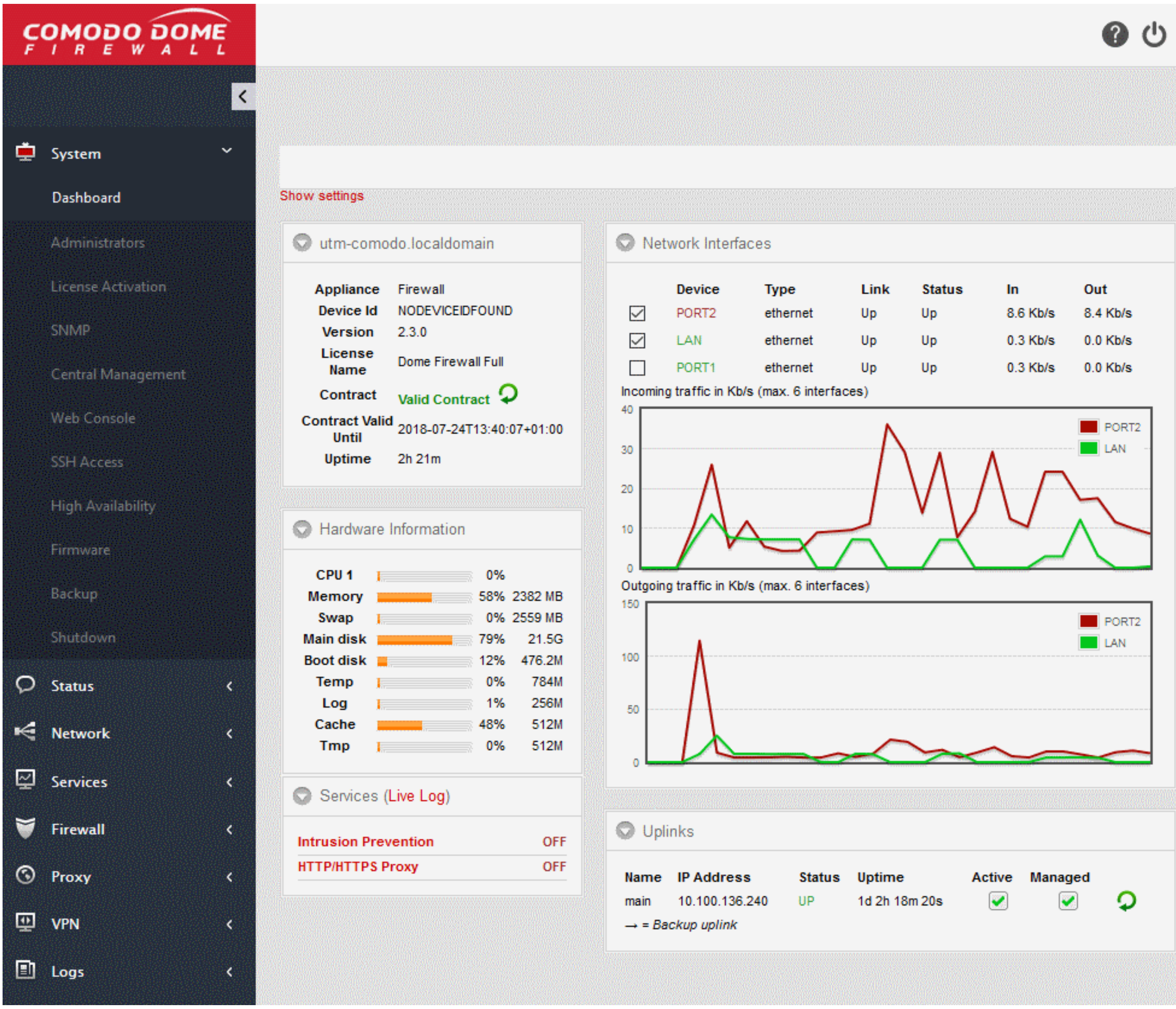
Comodo Dome Firewall (DFW) provides comprehensive security for enterprise networks and is available in two versions:

- Firewall SaaS
- Firewall software that can be installed on a system or a virtual machine

Dome Firewall simplifies the overall management of network security by delivering a single interface through which administrators can control firewall policy, antivirus, intrusion prevention, website filtering, traffic monitoring, VPN and proxy servers. Dome Firewall also features highly configurable notifications, in-depth reporting and an informative dashboard which offers a panoramic view of all major security settings and network events.

Key benefits:

- Fully integrated security - All DFW modules are designed to work in complete harmony with each other, avoiding interoperability issues and without leaving gaps in your protection
- Fast setup and configuration - Simply connect the Dome Firewall virtual appliance to your network and use a single interface to configure your entire network's security
- Slash costs - Dome Firewall costs a fraction of the purchase price of individual systems, consumes less power and means enterprises no longer need to pay for multiple service and support contracts
- Reduced technical requirements - With just one product to learn, technical personnel are released from the need to manage multiple systems and become more productive, effective and efficient
- Central Management - You can manage multiple Dome Firewall appliances remotely using Dome Firewall Central Manager. The central manager allows you to coordinate firewall security policy for multiple networks and customers from a single centralized console.



utm-comodo.localdomain

Appliance	Firewall
Device Id	NODEVICEIDFOUND
Version	2.3.0
License Name	Dome Firewall Full
Contract	Valid Contract
Contract Valid Until	2018-07-24T13:40:07+01:00
Uptime	2h 21m

Hardware Information

CPU 1	0%	
Memory	58%	2382 MB
Swap	0%	2559 MB
Main disk	79%	21.5G
Boot disk	12%	476.2M
Temp	0%	784M
Log	1%	256M
Cache	48%	512M
Tmp	0%	512M

Services (Live Log)

Intrusion Prevention	OFF
HTTP/HTTPS Proxy	OFF

Network Interfaces

	Device	Type	Link	Status	In	Out
☑	PORT2	ethernet	Up	Up	8.6 Kb/s	8.4 Kb/s
☑	LAN	ethernet	Up	Up	0.3 Kb/s	0.0 Kb/s
□	PORT1	ethernet	Up	Up	0.3 Kb/s	0.0 Kb/s

Incoming traffic in Kb/s (max. 6 interfaces)
40
30
20
10
0
PORT2
LAN
Outgoing traffic in Kb/s (max. 6 interfaces)
150
100
50
0
PORT2
LAN

Uplinks

Name	IP Address	Status	Uptime	Active	Managed
main	10.100.136.240	UP	1d 2h 18m 20s	☑	☑

→ = *Backup uplink*

Key features:

- Policy driven enterprise firewall
- Gateway antivirus
- Advanced Threat Protection
- Intrusion prevention system
- Website/URL filtering
- VPN and hotspot configuration
- Load balancing and traffic shaping
- Traffic monitoring and quality of service controls
- SSL and SSH inspection
- DNS and DHCP configuration
- Web proxy
- Full active directory integration
- Role Based Administrative Control for Administrators
- High Availability

Environmental Pre-requisites for Secure Operation:

To ensure secure operations, please ensure you deploy Dome Firewall in an acceptable environment:

- Dome Firewall administrators, should be properly trained in security operations and should fully understand how to configure the product. Passwords and authentication secrets should be adequately protected from unauthorized access.
- Please ensure no other products, virtual appliances or services are running which could conflict with Dome Firewall.
- Dome Firewall virtual appliance device and related peripheral units should be located in a physically protected area. Physical access to Dome Firewall should be provided only to required and authorized administrator(s).
- If the remote logging feature is to be used, it is recommended you run syslog server in protected zones.

Guide Structure

1.1 Installing Dome Firewall and logging-in to the Administrative Console

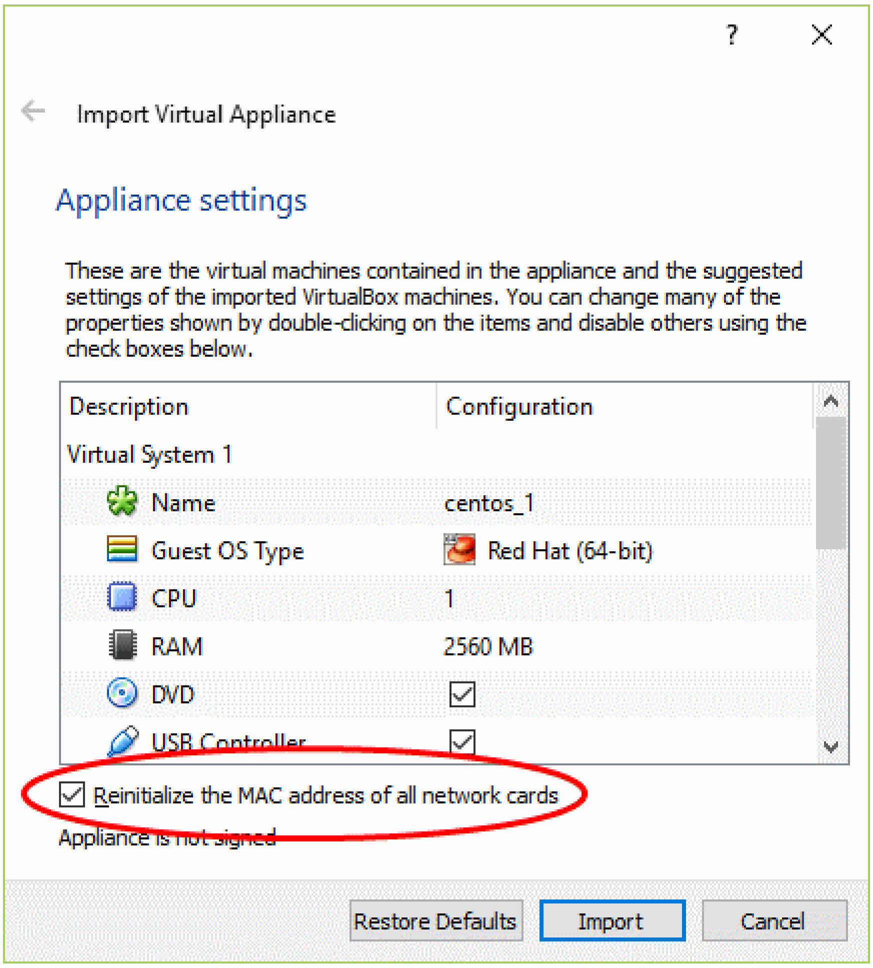
- How to Install the Virtual Appliance
- Initial Configuration

How to Install the Virtual Appliance

- Download the setup file, install the appliance and activate your license.
- The virtual appliance setup file is available in two formats:
  - .OVA File
  - .ISO File
- Please ensure your PC meets the following minimum requirements:
  - 1 x Intel or equivalent CPU
  - 2 GB RAM
  - 4 GB Storage
  - 2 x 1 GbE NIC

Install from OVA File

- Download the .ova file from **https://download.comodo.com/dome-repo/dome-fw-image/domefirewall.ova**.
- Import the virtual appliance into a virtual server such as Virtualbox or Vmware.
- **Important Note**: Select 'Reinitialize the MAC address of all network cards' when importing in order to avoid conflicts between the network adapters of the firewall device and the host machine.



Import Virtual Appliance

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Description	Configuration
Virtual System 1	
Name	centos_1
Guest OS Type	Red Hat (64-bit)
CPU	1
RAM	2560 MB
DVD	☑
USB Controller	☑

☑ Reinitialize the MAC address of all network cards

Appliance is not signed

Install from ISO File

- Download the .iso file from **https://download.comodo.com/dome-repo/dome-fw-image/domefirewall.iso**.
- Create a CentOS virtual machine on a virtual server such as Virtualbox or Vmware.
- Install the firewall virtual appliance from the .iso file

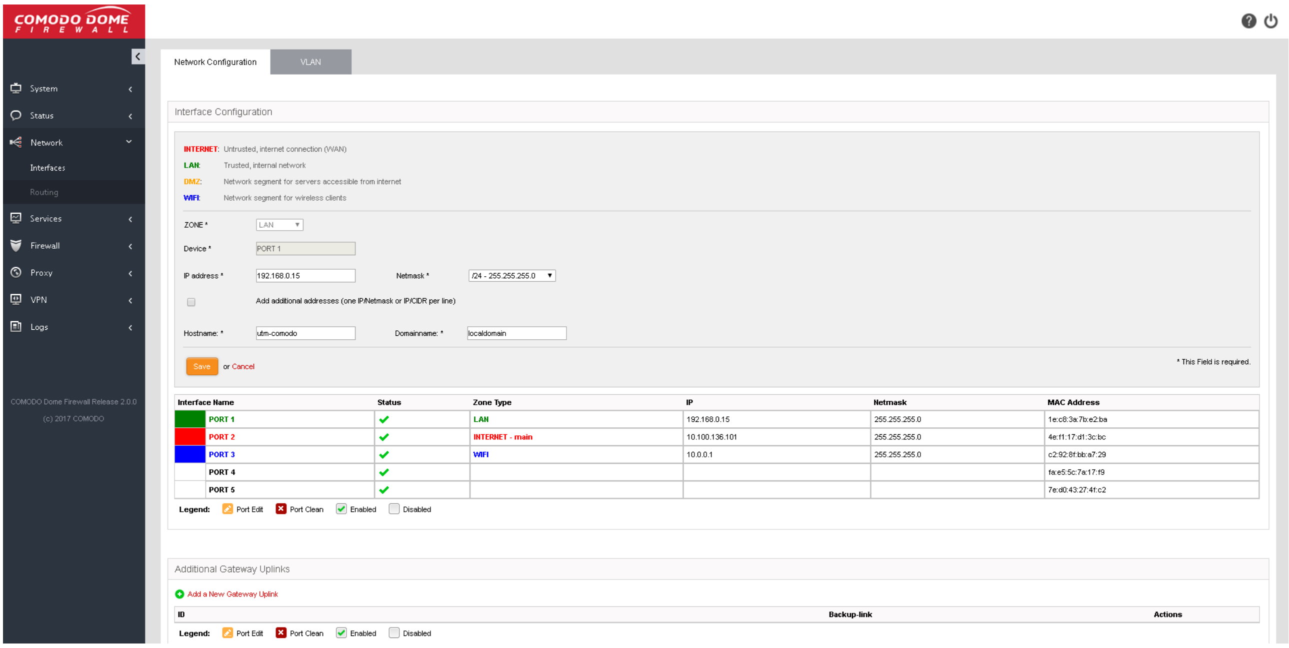
Initial Configuration

You can login to the management console at **https://192.168.0.15:10443**. The default credentials are: Username - admin and Password - comodo

The firewall requires you to change the default password after first login. Please choose a strong password that contains a mix of upper and lower case letters, numbers and special characters. We also recommend regularly changing your password as best security practice.

Once logged in, first configure the related ports for your network:

1. To setup network settings, click on 'Network' > 'Interfaces' in the menu on the left. You will find that port 1 is already configured with IP: 192.168.0.15 and Subnet mask : 255.255.255.0



Interface Configuration

INTERNET: Untrusted, internet connection (WAN)
LAN: Trusted, internal network
DMZ: Network segment for servers accessible from internet
WIFI: Network segment for wireless clients

ZONE * LAN
Device * PORT 1
IP address * 192.168.0.15 Netmask * /24 - 255.255.255.0
□ Add additional addresses (one IP/Netmask or IP/CIDR per line)
Hostname: * utm-comodo Domainname: * localdomain

Save or Cancel * This Field is required.

	Interface Name	Status	Zone Type	IP	Netmask	MAC Address
🟩	PORT 1	✓	LAN	192.168.0.15	255.255.255.0	1e:c8:3a:7b:e2:ba
🟥	PORT 2	✓	INTERNET - main	10.100.136.101	255.255.255.0	4e:f1:17:d1:3c:bc
🟦	PORT 3	✓	WIFI	10.0.0.1	255.255.255.0	c2:92:8f:bb:a7:29
	PORT 4	✓				fa:e5:5c:7a:17:f9
	PORT 5	✓				7e:d0:43:27:4f:c2

Legend: Port Edit ☒ Port Clean ☑ Enabled □ Disabled

Additional Gateway Uplinks

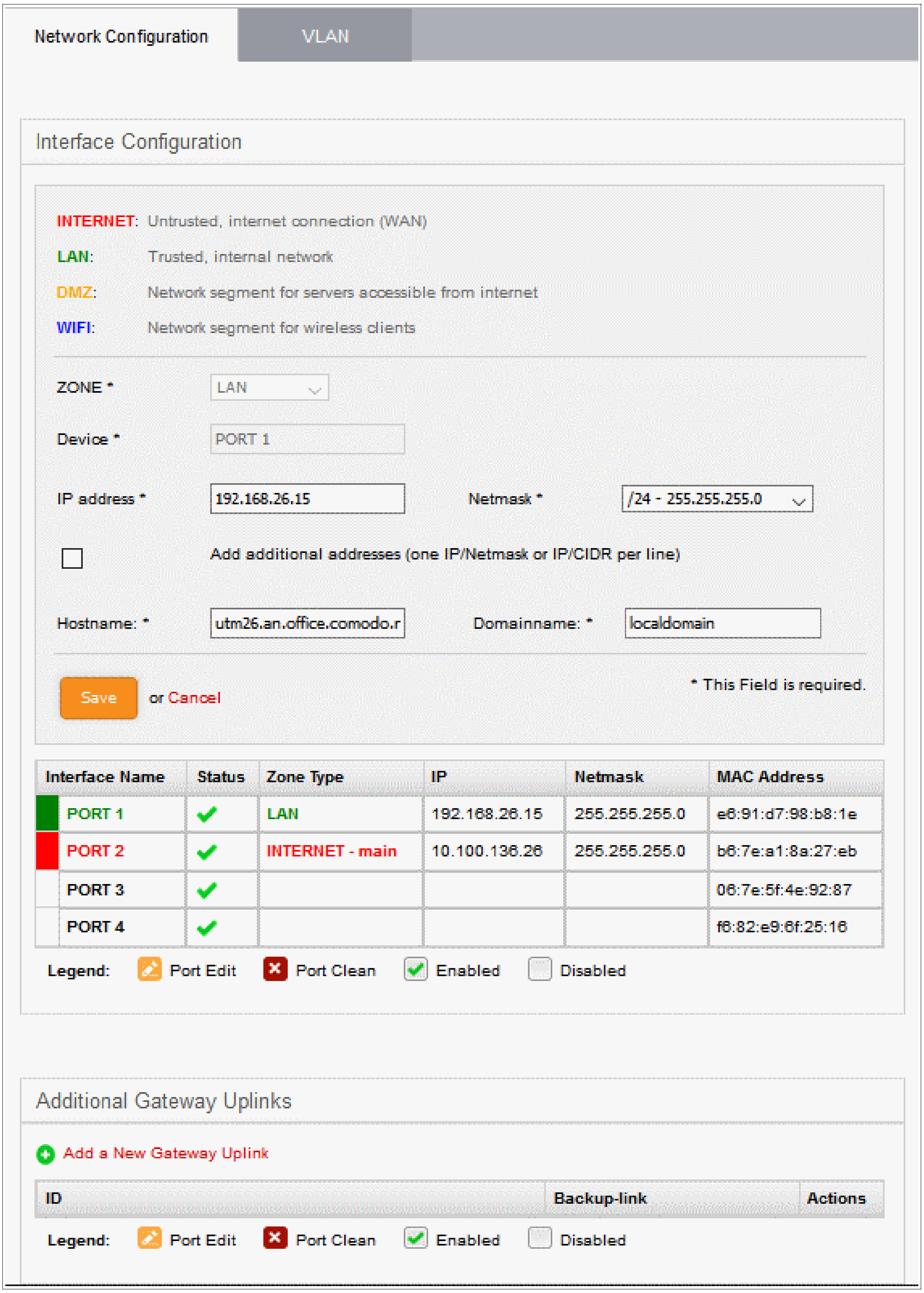
Add a New Gateway Uplink

ID	Backup-link	Actions

Legend: Port Edit ☒ Port Clean ☑ Enabled □ Disabled

2. For your INTERNET connection please use any port other than your LAN port (port 1) with your WAN IP and subnet configuration. Refer to the section **Network Configuration** for more details.

3. For your DMZ connection please use any port other than INTERNET and LAN ports with necessary IP and subnet information. You can find an example configuration below.



Interface Configuration

INTERNET: Untrusted, internet connection (WAN)

LAN: Trusted, internal network

DMZ: Network segment for servers accessible from internet

WIFI: Network segment for wireless clients

ZONE *	LAN		
Device *	PORT 1		
IP address *	192.168.26.15	Netmask *	/24 - 255.255.255.0
□	Add additional addresses (one IP/Netmask or IP/CIDR per line)		
Hostname: *	utm26.an.office.comodo.r	Domainname: *	localdomain

* This Field is required.

	Interface Name	Status	Zone Type	IP	Netmask	MAC Address
🟩	PORT 1	✓	LAN	192.168.26.15	255.255.255.0	e6:91:d7:98:b8:1e
🟥	PORT 2	✓	INTERNET - main	10.100.136.26	255.255.255.0	b6:7e:a1:8a:27:eb
	PORT 3	✓				06:7e:5f:4e:92:87
	PORT 4	✓				f6:82:e9:6f:25:16

Legend: Port Edit ☒ Port Clean ☑ Enabled □ Disabled

Additional Gateway Uplinks

ID	Backup-link	Actions

Legend: Port Edit ☒ Port Clean ☑ Enabled □ Disabled

4. After configuring INTERNET and DMZ interfaces, you just have to configure your LAN interface so that it will include your own LAN subnet IP and mask.

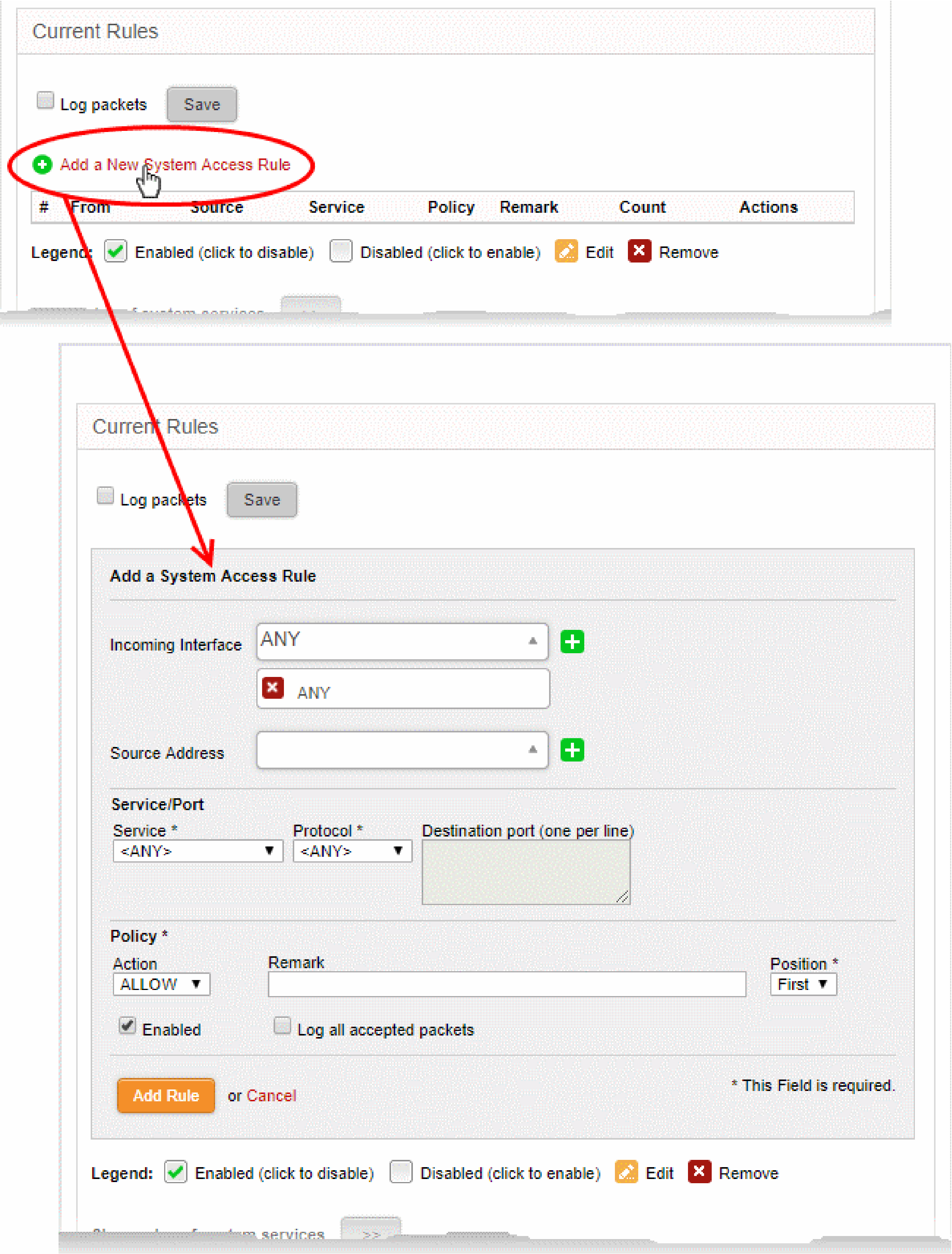
5. You need to create a 'System Access' rule so hosts in your network zones can access basic firewall services.
   - Dome Firewall Virtual Appliance ships with a set of pre-configured rules that allow hosts in different zones to access basic services like DNS (port 53), the firewall admin interface (port 10443); and DHCP (port 67).
   - You need to create a system access rule to ensure that hosts in the network zones can initially

access firewall services.

- You can edit the rule to restrict access from specific hosts in and services at anytime.

To add a system Access' rule to allow traffic from all network zones

- Click 'Firewall' on the left and select 'System Access'
- Click the 'Add a New System Access Rule' link in the 'Current Rules' pane



Current Rules

□ Log packets [Save]

Add a New System Access Rule

#	From	Source	Service	Policy	Remark	Count	Actions

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) Edit ☒ Remove

Current Rules

□ Log packets [Save]

Add a System Access Rule

Incoming Interface: ANY
☒ ANY

Source Address:

Service/Port

Service *: <ANY>

Protocol *: <ANY>

Destination port (one per line):

Policy *

Action: ALLOW

Remark:

Position *: First

☑ Enabled □ Log all accepted packets

[Add Rule] or Cancel

* This Field is required.

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) Edit ☒ Remove

- Enter the parameters for the new rule as shown below:
  - **Incoming Interface** - Select 'Any' from the drop-down to allow access from hosts from all network zones connected to the firewall through different ports
  - **Source Address** - Leave the field blank
  - **Service/Port** - Select the type or the service hosted by the source, the protocol and the port used by the service.
  - **Service** - Choose 'Any' to allow traffic pertaining to all services
  - **Protocol** - Choose 'Any' from the drop-down
  - **Destination port** - Leave the field blank
  - **Policy** - Choose 'Allow' from the drop-down, to pass the packets from the all sources to their destined ports of the firewall device.
  - **Enabled** - Leave enabled to activate the rule after saving.
  - **Remark** - Enter a short description of the rule.
  - **Position** - Set the priority for the rule to 'First' in the list of 'System Access' rules list. The rules in the iptables are processed in the order they appear on the list.
  - **Log all accepted packets** - Select if you want packets allowed by the rule to be logged. See **View Logs** for more details on configuring storage of logs and viewing the logs.
- Click 'Add Rule'.

The new rule will be added and applied.

You can edit this rule at a later time to restrict access from hosts in selected network zones to selected services as required.

6. After configuring the Interfaces and the system access rule, you have to allow any traffic from LAN zone to INTERNET zone so that you will be able to reach internet sources before applying any complex or specific firewall policies.

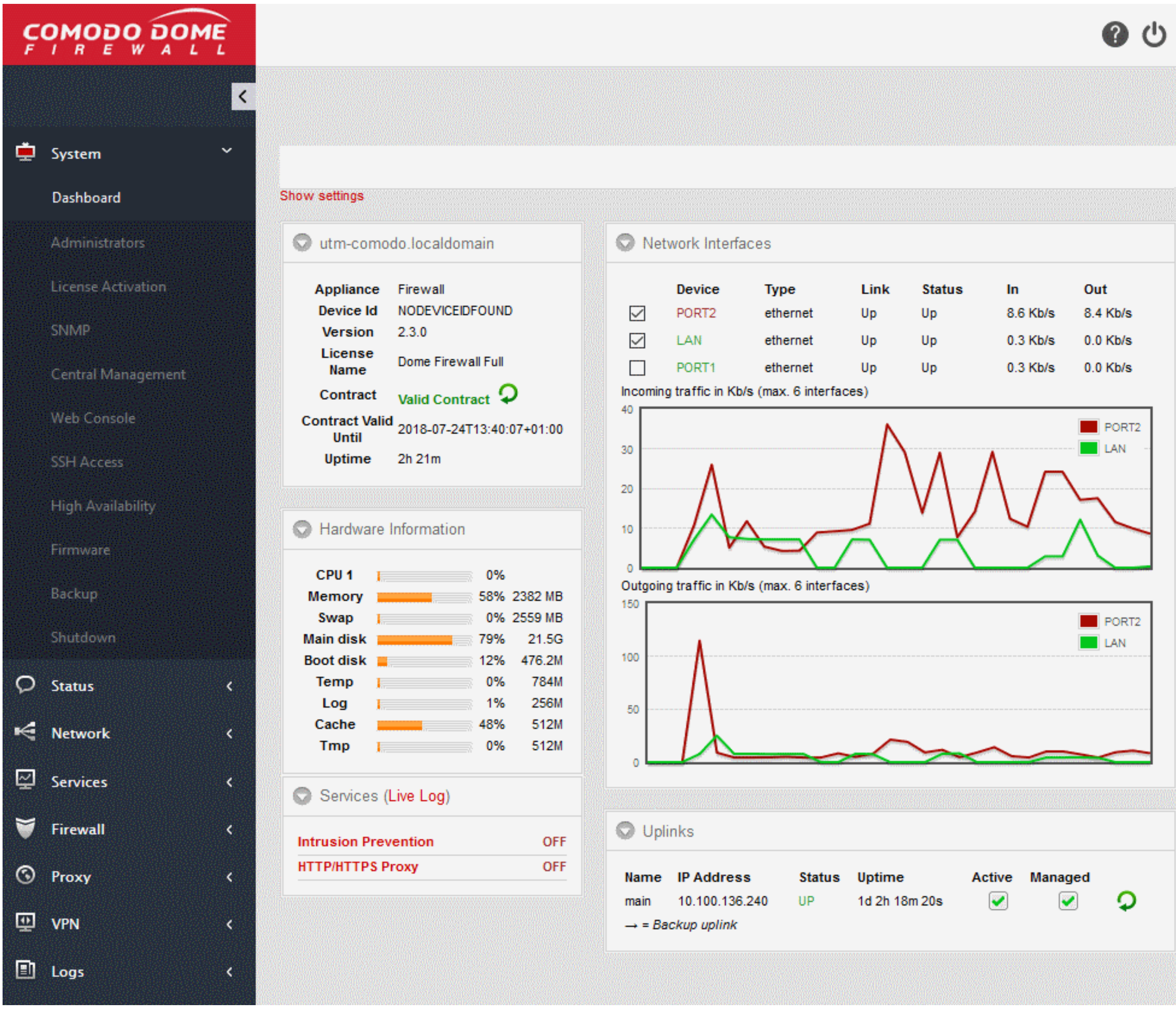
   Firewall Policies can be configured in the 'Policy Firewall' interface.

   - Click Firewall > Firewall in the left-hand navigation
   - Select the 'Policy Firewall' tab.

   More details on policy rules are available in **Managing Policy Firewall Rules**.

2 The Main Interface

The Dome Firewall dashboard is the administrative nerve center of the virtual appliance, providing administrators with visibility and control over all services and settings. The dashboard contains 'must know' statistics about network traffic, service status and uplinks and serves as a launchpad from which administrators can access other settings in the interface.



utm-comodo.localdomain

Appliance	Firewall
Device Id	NODEVICEIDFOUND
Version	2.3.0
License Name	Dome Firewall Full
Contract	Valid Contract
Contract Valid Until	2018-07-24T13:40:07+01:00
Uptime	2h 21m

Network Interfaces

	Device	Type	Link	Status	In	Out
☑	PORT2	ethernet	Up	Up	8.6 Kb/s	8.4 Kb/s
☑	LAN	ethernet	Up	Up	0.3 Kb/s	0.0 Kb/s
□	PORT1	ethernet	Up	Up	0.3 Kb/s	0.0 Kb/s

Hardware Information

CPU 1	0%	
Memory	58%	2382 MB
Swap	0%	2559 MB
Main disk	79%	21.5G
Boot disk	12%	476.2M
Temp	0%	784M
Log	1%	256M
Cache	48%	512M
Tmp	0%	512M

Services (Live Log)

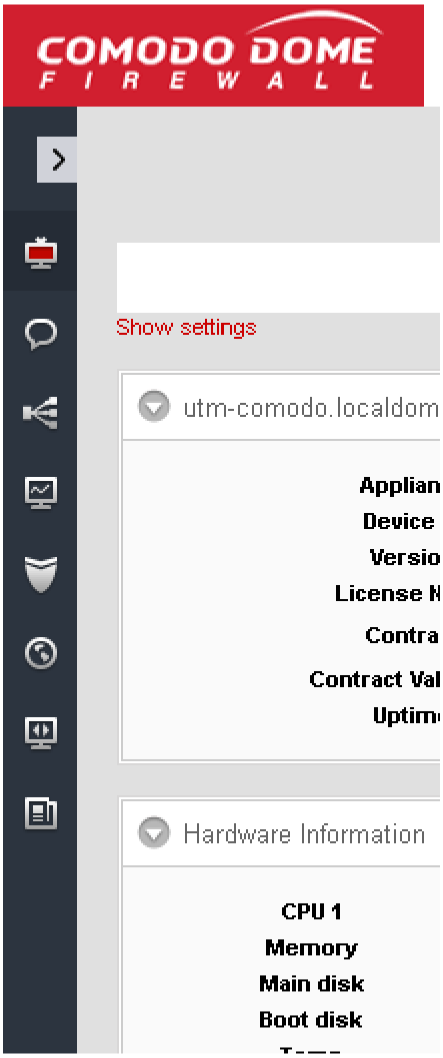
Intrusion Prevention	OFF
HTTP/HTTPS Proxy	OFF

Uplinks

Name	IP Address	Status	Uptime	Active	Managed
main	10.100.136.240	UP	1d 2h 18m 20s	✓	✓

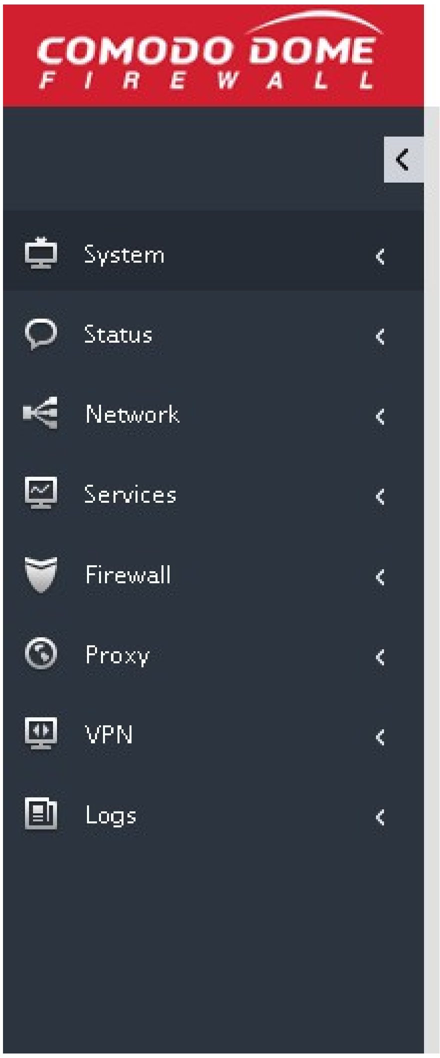
→ = *Backup uplink*

Dome Firewall modules are displayed in the strip along the left of the interface. Clicking the arrow at top-left will expand the strip into a full menu. The following table is a quick overview of the modules:



- **System** - Enables administrators to view and configure general settings such as admin accounts, notifications, passwords, connection to Dome Firewall Central Manager, SSH, user-interface settings and to shut down the system.
- **Status** - Enables administrators to view virtual appliance status data such as system status, network status and SSL VPN connections
- **Network** - Enables administrators to configure general and advanced network settings including hosts, routing, uplinks and VLANs.
- **Services** - Enables administrators to configure various DFW services like DHCP server, advanced threat protection, content flow check, intrusion prevention, traffic monitoring and more.
- **Firewall** - Enables administrators to configure the firewall and apply rules for controlling inbound and outbound traffic to/from the network.
- **Proxy** - Enables administrators to configure the proxy servers for various services like HTTP/HTTPS proxy services, URL filtering and so on.
- **VPN** - Enables administrators to configure the SSLVPN server, SSLVPN client, IPsec-based VPN tunnels and L2TP connections.
- **Logs** - Enables administrators to view logs for system events, firewall, antivirus, intrusion detection and other important areas. You can also configure syslog servers for remote logging.

- Click any module to reveal a sub-menu containing further options:

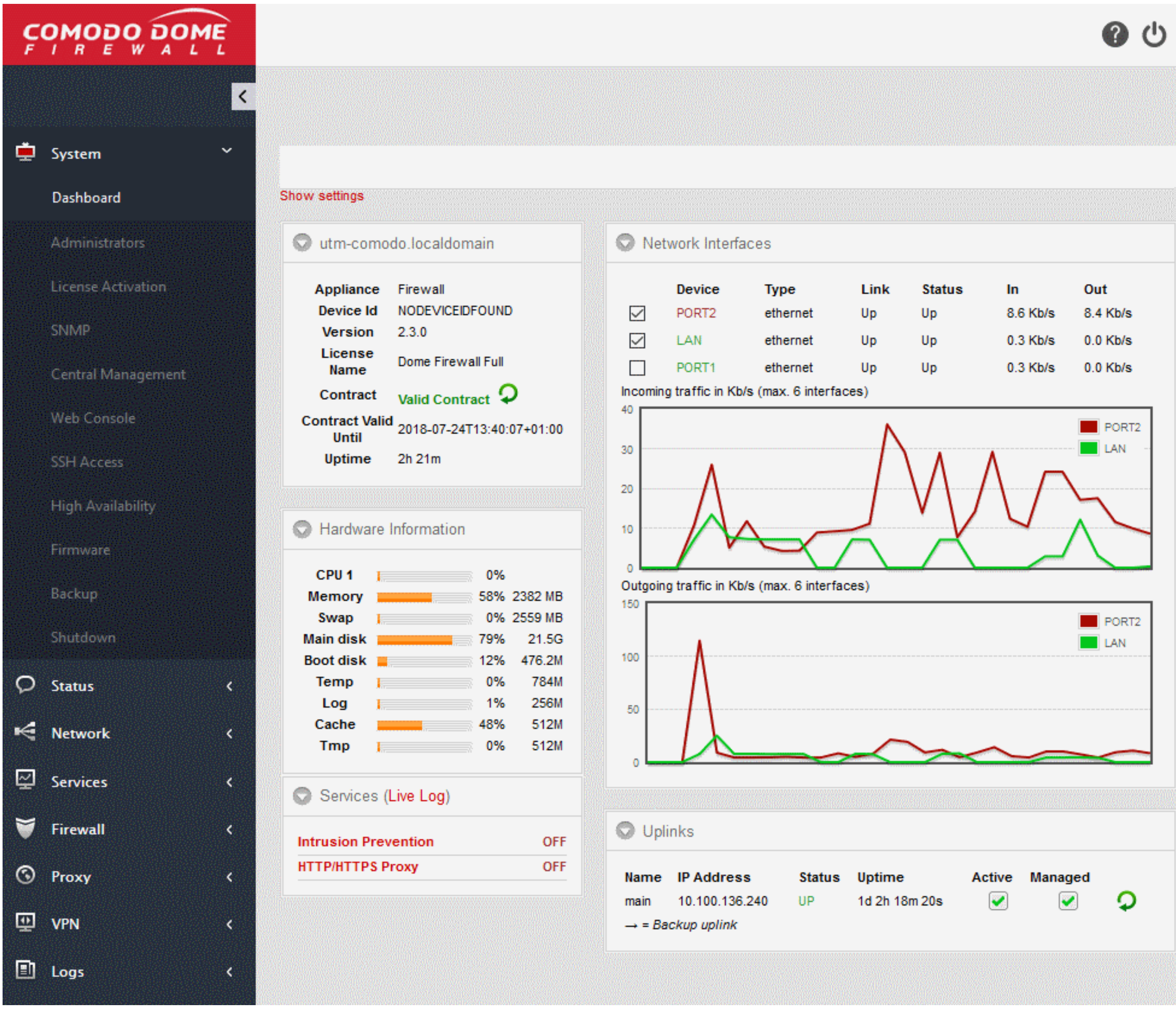


- **The Left Navigation Menu** - The menu on the left contains links to all Dome Firewall modules. Click any link to view or configure each module.
- **The Main Configuration Area** - The configuration area displays information pertinent to the module selected on the left.
  - Different network zones are represented with different colors:
    - RED - Untrusted external network zone, such as a WAN, through which the local network connects to internet. This network zone cannot be managed by the DFW but administrators can grant or limit access to this network zone.
    - GREEN - The local network zone to which the workstations are connected, such as the LAN. This zone is prevented from direct access by the RED zone. The administration console of the DFW can be accessed from any of the workstation connected to the local network.
    - ORANGE - The demilitarized zone (DMZ) that hosts the servers. The servers can directly connect to the internet and provide services like SMTP/POP, SVN and HTTP and so on.
    - BLUE - The WiFi zone used by wireless clients. All wireless clients are confined to this zone, prohibiting access to Orange or Green zones, as they are less secure and are allowed to directly connect to internet.
- **The Title Bar Controls** - The title bar contains controls for:
  - Logout - The administrator can logout of the Dome Firewall Administrative console
  - Help - Clicking the help button at the top will take you to the respective online help page
- **Version and Copyright Information** - Version number and copyright information of the DFW firmware is displayed at the bottom left of the interface.

3 The Dashboard

The dashboard provides a real-time overview of the current running status, traffic, health and usage of the firewall.

The dashboard is displayed by default whenever you login to the administrative interface. You can access the dashboard at any time by clicking 'System' > 'Dashboard' in the left navigation.



utm-comodo.localdomain

Appliance	Firewall
Device Id	NODEVICEIDFOUND
Version	2.3.0
License Name	Dome Firewall Full
Contract	Valid Contract
Contract Valid Until	2018-07-24T13:40:07+01:00
Uptime	2h 21m

Hardware Information

CPU 1		0%	
Memory		58%	2382 MB
Swap		0%	2559 MB
Main disk		79%	21.5G
Boot disk		12%	476.2M
Temp		0%	784M
Log		1%	256M
Cache		48%	512M
Tmp		0%	512M

Services (Live Log)

Intrusion Prevention	OFF
HTTP/HTTPS Proxy	OFF

Network Interfaces

	Device	Type	Link	Status	In	Out
☑	PORT2	ethernet	Up	Up	8.6 Kb/s	8.4 Kb/s
☑	LAN	ethernet	Up	Up	0.3 Kb/s	0.0 Kb/s
□	PORT1	ethernet	Up	Up	0.3 Kb/s	0.0 Kb/s

Incoming traffic in Kb/s (max. 6 interfaces)
40
30
20
10
0
PORT2
LAN
Outgoing traffic in Kb/s (max. 6 interfaces)
150
100
50
0
PORT2
LAN

Uplinks

Name	IP Address	Status	Uptime	Active	Managed
main	10.100.136.240	UP	1d 2h 18m 20s	☑	☑

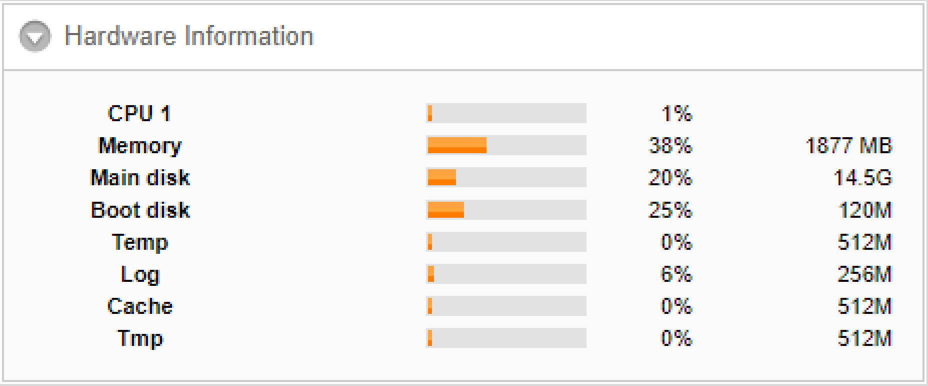
→ = *Backup uplink*

The dashboard contains five tiles which provide details on licensing/system information, hardware resource usage, currently running services, network traffic and uplink status.

- Each tile can be expanded or collapsed by clicking the arrow at top left
- The tiles can be re-positioned by dragging and dropping.
- For more details on configuring the tiles, see **Configuring the Dashboard**

Hardware Information

The Hardware information tile shows resource usage by the firewall.



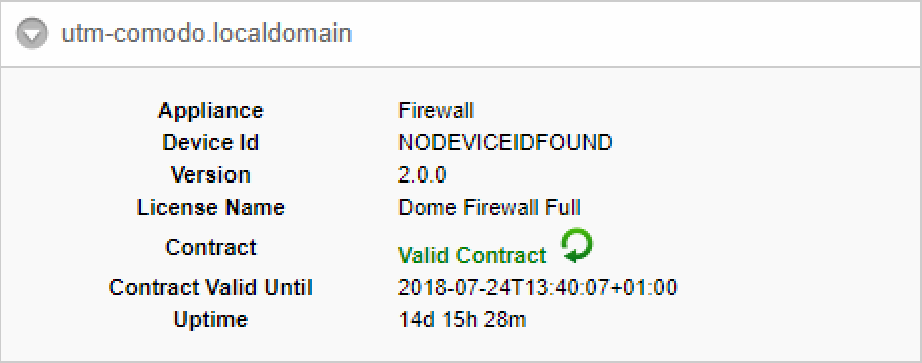
Hardware Information

CPU 1		1%	
Memory		38%	1877 MB
Main disk		20%	14.5G
Boot disk		25%	120M
Temp		0%	512M
Log		6%	256M
Cache		0%	512M
Tmp		0%	512M

- CPU x: The usage of the CPU resources. In a multi-processor virtual appliance, the load on each CPU is indicated separately, with the suffix 'x' denoting the CPU number.
- Memory - The usage of the system memory in the DFW
- Main disk - Usage of the root partition of the hard disk in the DFW virtual appliance. The disk usage should not exceed 95%.
- Boot disk - Usage of the boot partition of the hard disk in the DFW virtual appliance. The disk usage should not exceed 95%.
- Temp - Usage of disk space in /tmp partition, allotted for temporary files in the DFW virtual appliance. The Temp space usage should not exceed 95%.
- Log - Usage of disk space allotted for log files in the DFW virtual appliance. The log space usage should not exceed 95%. The log files are available at /var/logs. If the log space usage exceeds the threshold, the administrator can move the log files to a different storage device and free the disk space.
- Cache - Usage of disk space for cache memory in the DFW virtual appliance.
- Tmp - Usage of disk space by .tmp files created in the virtual appliance.

System Information

Shows the host name and the network domain to which the DFW virtual appliance is connected. The tile displays also displays general information about the virtual appliance:



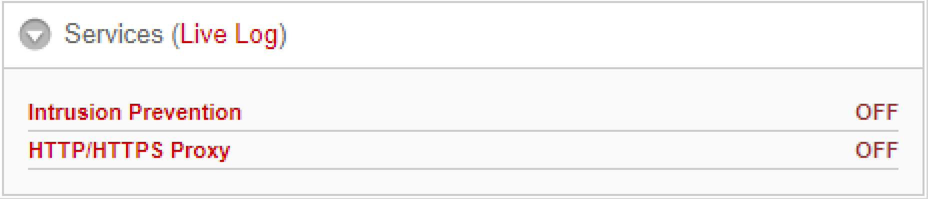
utm-comodo.localdomain

Appliance	Firewall
Device Id	NODEVICEIDFOUND
Version	2.0.0
License Name	Dome Firewall Full
Contract	Valid Contract
Contract Valid Until	2018-07-24T13:40:07+01:00
Uptime	14d 15h 28m

- Appliance - The type of virtual appliance
- Device ID - The identification number of the virtual appliance
- Version - The version number of the DFW firmware installed on the device
- Contract - Indicates whether the license of the firmware is valid. Clicking the circled arrow refreshes the information.
- Contract Valid Until - Expiry date of the license
- Uptime - Indicates the period for which the virtual appliance is Up since the last reboot

Services

Shows the On/Off status and statistics about currently loaded services. Services can include intrusion detection and mail filters.



Services (Live Log)

Intrusion Prevention	OFF
HTTP/HTTPS Proxy	OFF

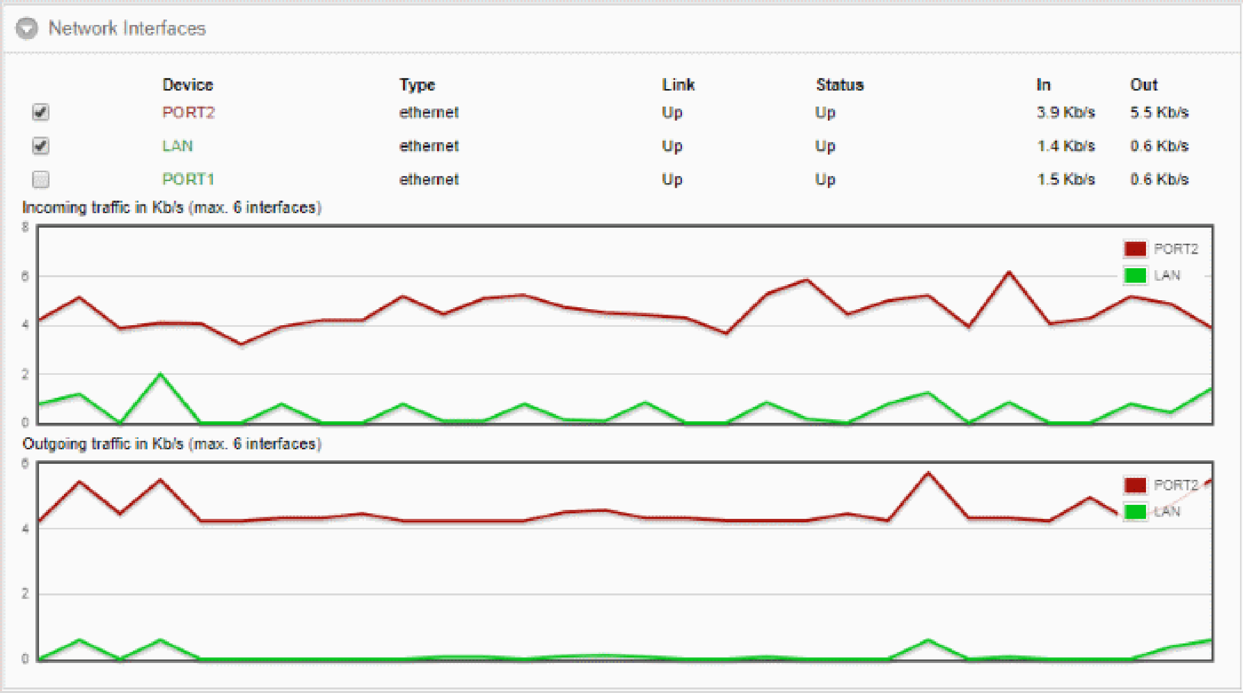
- Click the Live Log in the title bar to open the **Realtime logs** screen.
- Click the service name to view detailed statistics.

The services displayed are:

- Attacks Logged - Shows the number of attacks logged by the DFW
- SMTP Proxy - Shows the statics of mails in queue, total mails received, clean mails and infected mails that were rejected
- HTTP/HTTPS Proxy - Shows the statics of cache hits and misses

Network Interfaces

Shows network interface devices connected to the firewall and realtime charts of incoming and outgoing traffic through these devices.



Network Interfaces

	Device	Type	Link	Status	In	Out
☑	PORT2	ethernet	Up	Up	3.9 Kb/s	5.5 Kb/s
☑	LAN	ethernet	Up	Up	1.4 Kb/s	0.6 Kb/s
□	PORT1	ethernet	Up	Up	1.5 Kb/s	0.6 Kb/s

Incoming traffic in Kb/s (max. 6 interfaces)
8
6
4
2
0
🟥 PORT2
🟩 LAN
Outgoing traffic in Kb/s (max. 6 interfaces)
6
4
2
0
🟥 PORT2
🟩 LAN

Network Interfaces - Column Descriptions	
Column Header	**Description**
Device	The name of the network interface device. The font color indicates the network zone to which the device belongs: Red - External networks like a WAN or the internet Yellow - DMZ zones

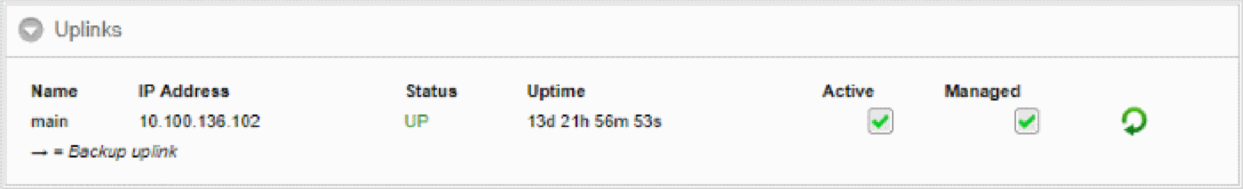
	Green - LAN networks Blue - Wi-Fi networks
Type	Connection type. For example, ethernet or wi-fi.
Link	Whether the connection is active or not.
Status	Running status of the device
In/Out	Incoming/Outgoing traffic through the device

The lower half of the tile shows realtime charts of incoming and outgoing traffic through the devices selected in the upper half.

For more information on managing network interface devices, see **Network Configuration**.

Uplinks

The uplinks area shows defined uplinks defined through which the virtual appliance connects to the internet.



Uplinks

Name	IP Address	Status	Uptime	Active	Managed	
main	10.100.136.102	UP	13d 21h 56m 53s	☑	☑	

→ = *Backup uplink*

The table shows the connection status and running status of each uplink and allows the administrator to enable or disable them. For more details on managing uplinks, see **Adding and Managing Gateway Uplink Devices**.

Uplinks - Column Descriptions

Column Header	Description
Name	The name of the uplinks defined in DFW.
IP Address	IP Address of the uplink
Status	Running status of the uplink. The status column can have one of the following values: Stopped or Inactive - The uplink is not connected to DFW virtual appliance. Connecting - The uplink is connecting to the virtual appliance, but connection is not yet complete Connected or UP - The connection has been established and operational. Disconnecting - The uplink is closing the connection Failure - The connection could not be completed Failure, reconnecting - The connection could not be completed, but the virtual appliance is attempting to reconnect again. Dead link- The uplink is connected, but the defined hosts could not be reached. The uplink is not operational.
Uptime	The period the uplink has been active since the last reboot
Active	Whether the uplink is on or not. You can switch the uplink between enabled and disabled states by selecting/deselecting this checkbox
Managed	Shows whether the uplink is managed by DFW or manually managed. Admins can switch between states by selecting or deselecting the checkbox. In 'Managed' mode, the uplink will be continuously monitored and reconnected whenever there is a loss in

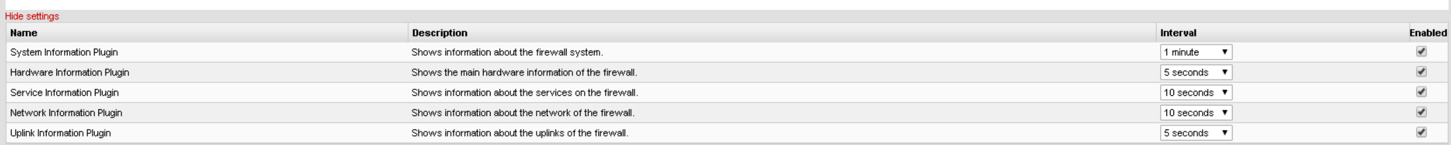
	connectivity. During testing or maintenance, the uplink can be switched to manual mode. • Clicking the circled arrow refreshes the information.

Configuring the Dashboard

Dome Firewall uses dashboard plug-ins to fetch the statistical information from different components of the DFW and displays them as tiles in the dashboard. The plug-ins gather the updated information periodically at specified intervals. The administrator can configure the interval at which the statistical information from each component is fetched and enable/disable the plug-ins, and hence the corresponding tile, from the Dashboard settings pane.

To open the Dashboard Settings pane

- Click 'Show Settings' link at the top left of the Dashboard.



Hide settings

Name	Description	Interval	Enabled
System Information Plugin	Shows information about the firewall system.	1 minute ▼	☑
Hardware Information Plugin	Shows the main hardware information of the firewall.	5 seconds ▼	☑
Service Information Plugin	Shows information about the services on the firewall.	10 seconds ▼	☑
Network Information Plugin	Shows information about the network of the firewall.	10 seconds ▼	☑
Uplink Information Plugin	Shows information about the uplinks of the firewall.	5 seconds ▼	☑

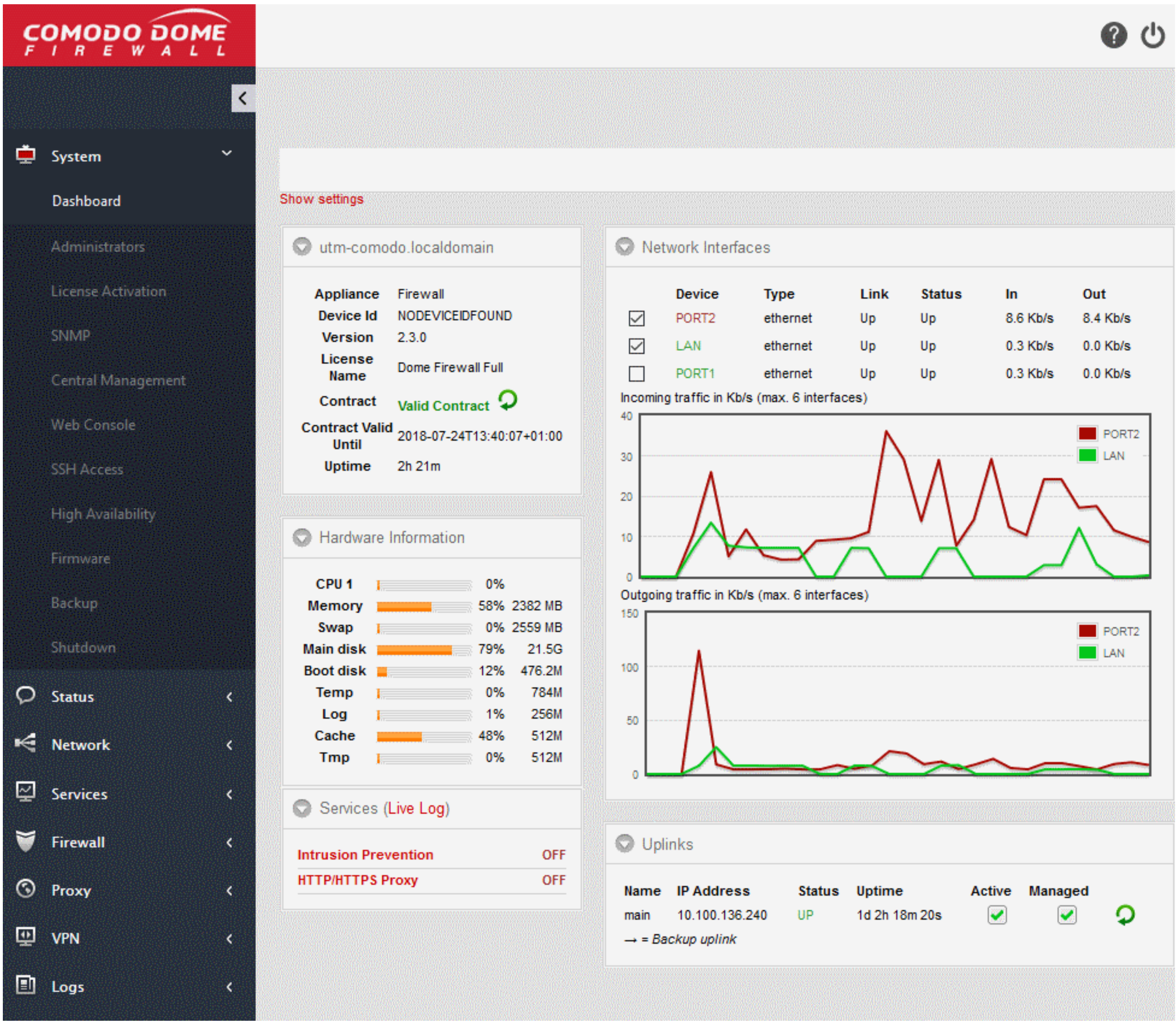
A table with a list of plug-ins used, their descriptions and the current configuration will be displayed.

Dashboard Settings - Column Descriptions	
Column Header	**Description**
Name	The name of the plugin
Description	A short description of the plug-in. Indicates the component of the DFW for which the plug-in fetches the information.
Interval	Enables the administrator to set the time interval at which the plug-in should refresh the information and show in the corresponding tile, be selecting the interval from the drop-down.
Enabled	The checkboxes enable the administrator to enable or disable the plug-in. Only the tiles corresponding to enabled plug-ins are displayed in the dashboard. If a tile needs to be hidden, the corresponding plug-in can be simply disabled.

- Set the refresh intervals and enabled/disabled states of the plug-ins as desired
- Click 'Save' for your changes to take effect
- To close the settings pane, click 'Hide Settings' link at the top left.

4 Viewing and Modifying System Status and General Configuration

The 'System' menu contains links to important firewall configuration areas. From here, admins can configure new networks, manage fellow administrators, configure notifications, connect the firewall to central management, schedule backups and more. Admins can also shutdown the virtual appliance from the system interface.



utm-comodo.localdomain

Appliance	Firewall
Device Id	NODEVICEIDFOUND
Version	2.3.0
License Name	Dome Firewall Full
Contract	Valid Contract
Contract Valid Until	2018-07-24T13:40:07+01:00
Uptime	2h 21m

Network Interfaces

	Device	Type	Link	Status	In	Out
☑	PORT2	ethernet	Up	Up	8.6 Kb/s	8.4 Kb/s
☑	LAN	ethernet	Up	Up	0.3 Kb/s	0.0 Kb/s
□	PORT1	ethernet	Up	Up	0.3 Kb/s	0.0 Kb/s

Hardware Information

CPU 1	0%	
Memory	58%	2382 MB
Swap	0%	2559 MB
Main disk	79%	21.5G
Boot disk	12%	476.2M
Temp	0%	784M
Log	1%	256M
Cache	48%	512M
Tmp	0%	512M

Services (Live Log)

Intrusion Prevention	OFF
HTTP/HTTPS Proxy	OFF

Uplinks

Name	IP Address	Status	Uptime	Active	Managed
main	10.100.136.240	UP	1d 2h 18m 20s	✓	✓

→ = *Backup uplink*

The 'System' menu contains the following items:

- **Dashboard** - At-a-glance summary of the status of the firewall and traffic passing through network interfaces. See **The Dashboard** for more details.
- **Administrators** - Create and manage new admins and admin profile templates. You can configure highly targeted, granular permissions for each profile you create. See **Managing Administrative Accounts** for more details.
- **License Activation** - Lets you view your current license number and activate new firewall licenses. See '**License Activation**' for more details.
- **SNMP** - Configure Simple Network Management Protocol settings. See '**SNMP Settings**' for more details.
- **Central Management** - Connect this firewall to Dome Firewall Central Manager. See **Central Management** for more details
- **Web Console** - Opens a terminal window for administrative tasks. See **Accessing the Web Console** for more details.
- **SSH Access** - Configure remote Secure Shell (SSH) access to the internal network by enabling tunneling of various services. See **Configuring SSH Access** for more details.
- **High Availability** - Configure active-passive failover servers to ensure continuity of operations. See **High Availability** for more details.
- **Firmware** - View current firmware version and download firmware updates if available. See **Viewing and Updating Firmware Version** for more details.

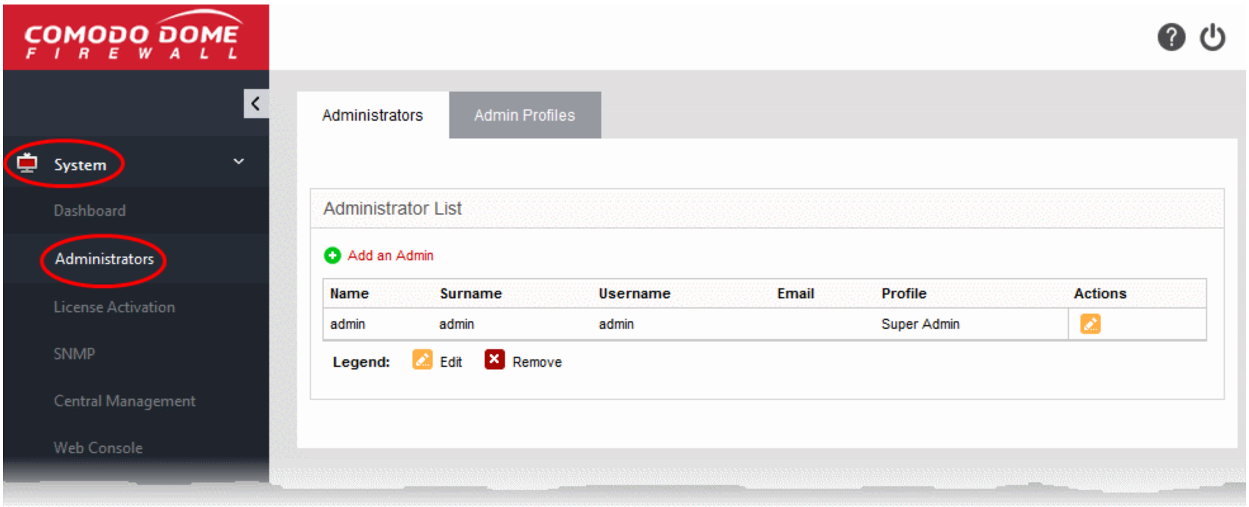
- **Backup** - Configure backups of the current firewall state and setup scheduled backups. Admins can restore the firewall by importing a backup in the event of system failure. See **Creating and Scheduling Backup of DFW state** for more details.
- **Shutdown** - Power-off the DFW virtual appliance. See **Shutting Down the Dome Firewal Virtual Appliance** for more details.

4.1 Manage Administrative Accounts

- Super admins can create new administrators with specific permissions to configure and manage the various firewall modules.
- An administrators privileges are determined by the profile assigned to them. You should first configure an admin profile then assign the profile to an administrator
- Administrator activities are logged as part of access control. Logged items include date, time, type of event, subject id, component name and the event outcome.
- Click 'System' > 'Administrators' to open the configuration interface.

To configure administrators and roles

- Click 'System' > 'Administrators' in the left-hand menu:



Name	Surname	Username	Email	Profile	Actions
admin	admin	admin		Super Admin	✎

The interface contains two tabs:

- **Administrators** - Create and manage fellow administrator accounts. See **Adding and Managing Administrators** for more details.
- **Admin Profiles** - Create and manage administrative roles with different privilege levels. These profiles can then be applied to individual administrators. See **Managing Administrative Roles** for more details.

4.1.1 Adding and Managing Administrators

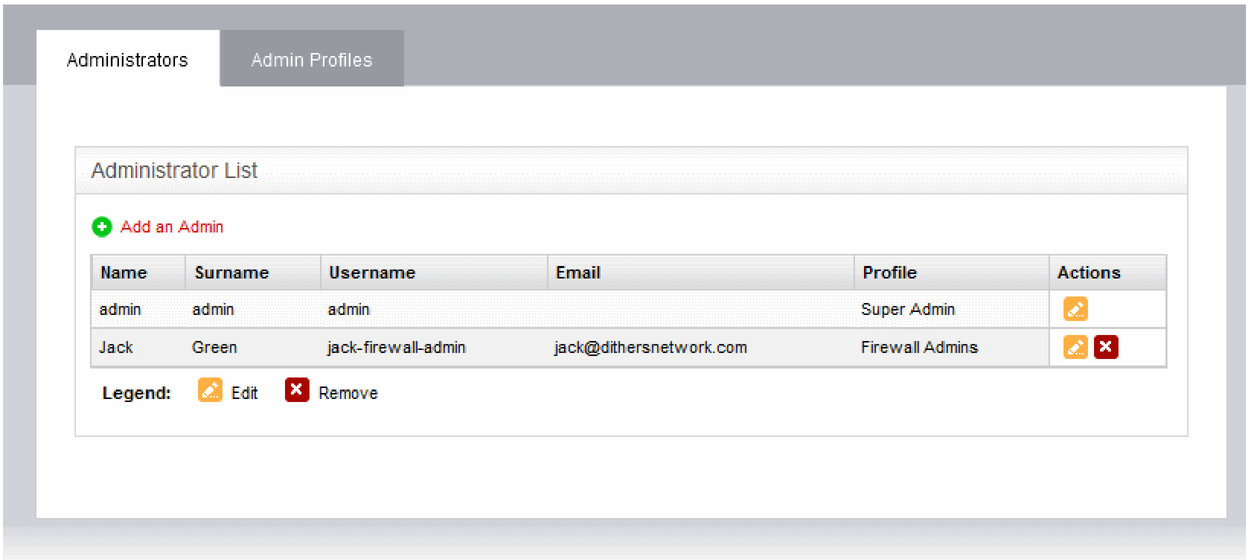
- The 'Administrators' interface lists all existing admins and allows you to create and manage administrators.
- Comodo Dome Firewall ships with a super-admin account with the username 'admin', password 'comodo'.
- You should edit this account to change the username and password.
- At least one super admin account must be active on the virtual appliance. You cannot delete the last remaining super-admin account.

Tip : Please choose strong passwords at least 8 characters long and which contains a mixture of uppercase and lowercase letters, numbers and special characters.

Tip: We advise most operations are carried out using created accounts rather than the default, built-in account. This will allow you to manage authorizations more efficiently.

To open the 'Administrators' interface

- Click 'System' > 'Administrators' in the left-hand navigation.
- Click the 'Administrators' tab



Name	Surname	Username	Email	Profile	Actions
admin	admin	admin		Super Admin	✎
Jack	Green	jack-firewall-admin	jack@dithersnetwork.com	Firewall Admins	✎ ✖

Legend: ✎ Edit ✖ Remove

Administrators List Table - Column Descriptions	
Column	**Description**
Name	The first/given name of the administrator
Surname	The last name of the administrator
Username	The username for the administrator to login to the Dome Firewall administrative console
Email	The email address of the administrator
Profile	The administrative role assigned to the administrator. The administrator will have access to different interfaces of the console depending on the role assigned.
Actions	Displays control buttons for editing/removing the administrator. ✎ - Edits the administrator ✖ - Removes the administrator

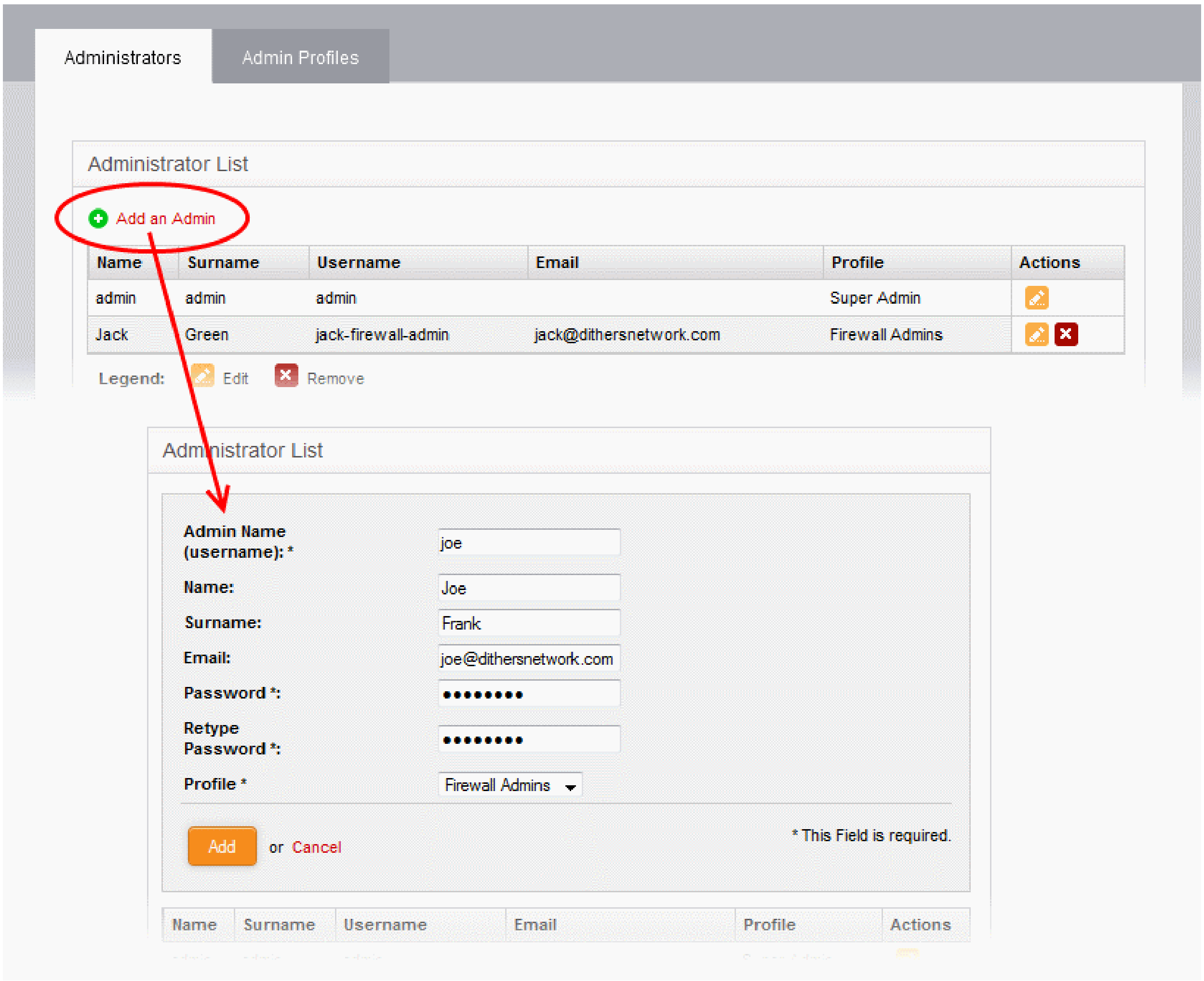
The following sections provide detailed guidance on:

- **Adding a new administrator**
- **Editing an existing administrator**
- **Removing an administrator**

Tip: It is recommended to first create the administrative role(s) before adding administrators. All the created administrative roles will be available for assigning to the administrator added from a drop-down. See **Managing Administrative Roles** for more details on adding roles.

To add a new administrator account

- Click the 'Add an Admin' link from the top left of the 'Administrator List' interface. The interface for adding a new administrator will appear.



Administrator List

Add an Admin

Name	Surname	Username	Email	Profile	Actions
admin	admin	admin		Super Admin	✎
Jack	Green	jack-firewall-admin	jack@dithersnetwork.com	Firewall Admins	✎ ✖

Legend: ✎ Edit ✖ Remove

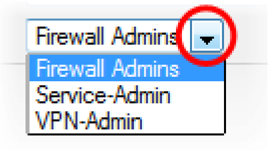
Administrator List

Admin Name (username): *	joe
Name:	Joe
Surname:	Frank
Email:	joe@dithersnetwork.com
Password *:	••••••••
Retype Password *:	••••••••
Profile *	Firewall Admins

Add or Cancel

* This Field is required.

- Enter the details of the new administrator as given below:
  - Admin Name (username): Enter the username for the new administrator to login
  - Name: Enter the first name of the administrator
  - Surname: Enter the last name of the administrator
  - Email: Enter the email address of the administrator
  - Password: Enter the password for the administrator to login and re-enter the same for conformation in the 'Retype Password' field
  - Profile: The drop-down will display a list of administrative roles you created from the 'Admin Profiles' interface. Choose the role to be assigned to the administrator from the drop-down.



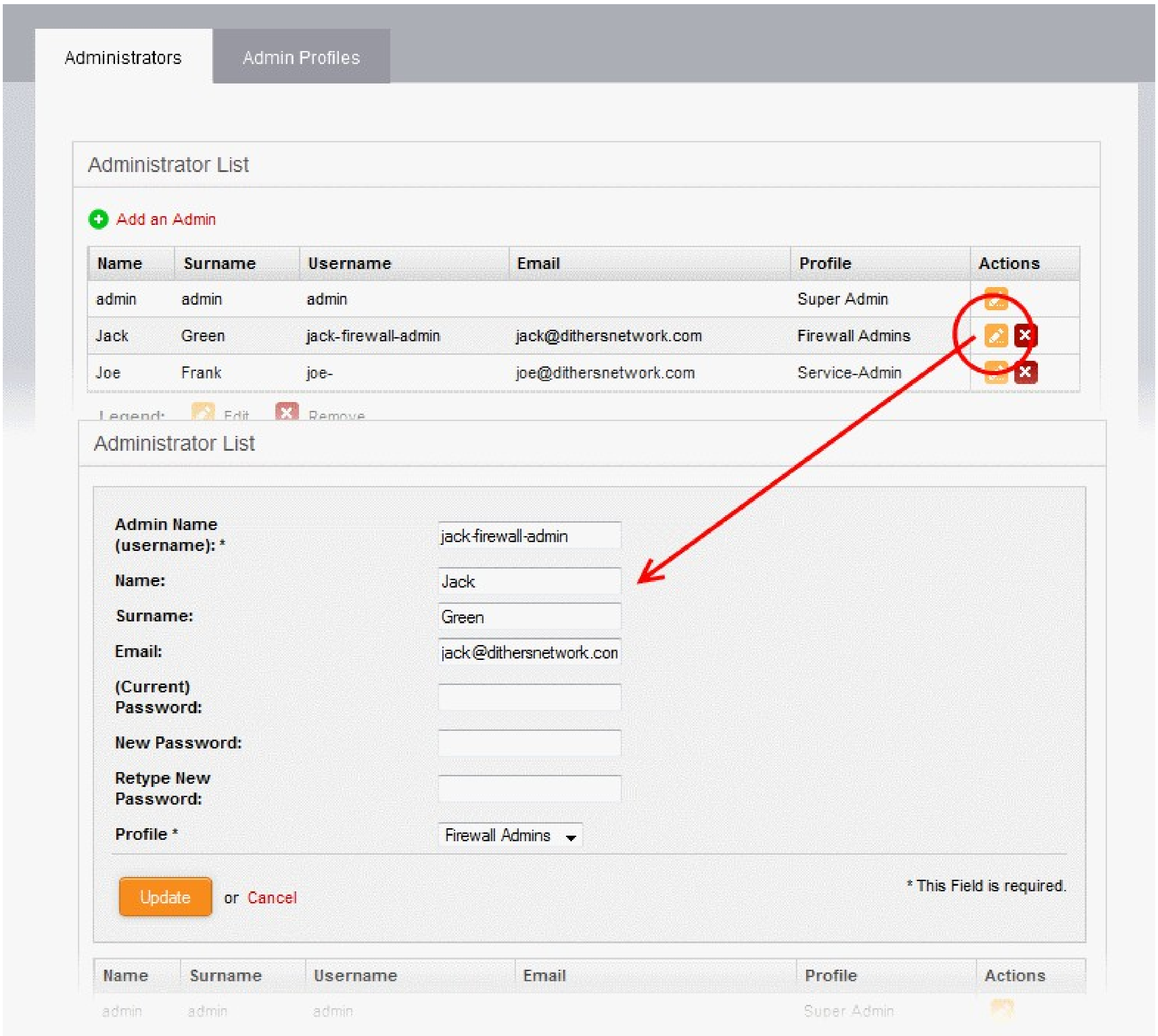
- Click 'Add'.

The administrator will be added to the virtual appliance and can login to the administrative interface.

The global administrator needs to communicate the login credentials to the new administrator through any out-of-band communication like email to enable the new administrator to login.

To edit an administrator

- Click the 'Edit' button ✎ in the row of the administrator to be edited. The interface for editing the details, changing the username and password and /or changing the role of the administrator will appear.



Administrator List

Add an Admin

Name	Surname	Username	Email	Profile	Actions
admin	admin	admin		Super Admin	✎
Jack	Green	jack-firewall-admin	jack@dithersnetwork.com	Firewall Admins	✎ ✖
Joe	Frank	joe-	joe@dithersnetwork.com	Service-Admin	✎ ✖

Legend: ✎ Edit ✖ Remove

Administrator List

Admin Name (username): *	jack-firewall-admin
Name:	Jack
Surname:	Green
Email:	jack@dithersnetwork.con
(Current) Password:	
New Password:	
Retype New Password:	
Profile *	Firewall Admins

* This Field is required.

Name	Surname	Username	Email	Profile	Actions
admin	admin	admin		Super Admin	✎

- The Edit interface is similar to 'Add Administrator' interface. Edit the details as required and click 'Update'. See **section above** for more details.
- For changing the password, it is essential to enter the existing password in the 'current password' field.

To remove an administrator

- Click the 'Delete' button ✖ in the row of the administrator to be removed. The administrator account will be removed immediately.

4.1.2 Managing Administrative Roles

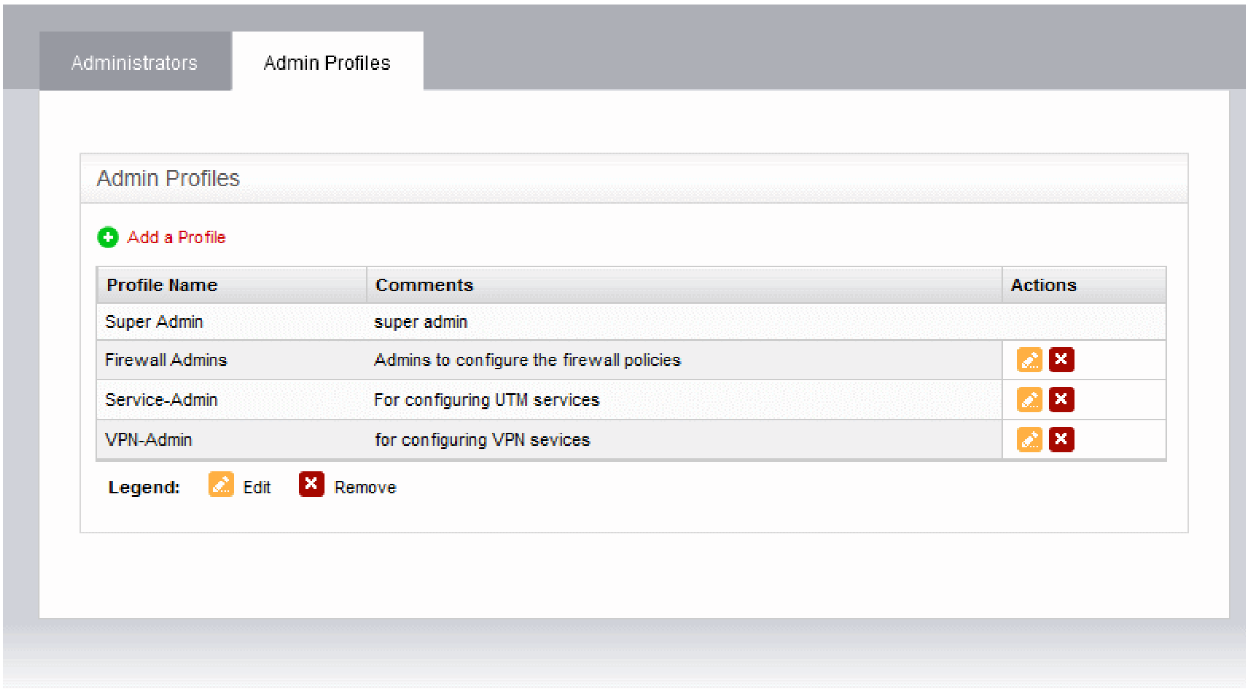
- The 'Admin Profiles' interface displays a list of roles that have been created in Dome Firewall VA.
- Each role can have different privileges to access and configure firewall modules.
- You create a profile to define a role. You can then apply the profile to one or more admins in the 'Administrators' tab.
- The super administrator can create and manage new roles. The super admin role cannot be deleted.

Comodo Dome Firewall ships with a default administrative role 'super admin' for the global administrator. The profile cannot be edited and deleted, as at least one super admin account must be active on the virtual appliance.

To open the 'Admin Profiles' interface

- Click 'System' > 'Administrators' in the left-hand navigation.

- Click the 'Admin Profiles' tab



Admin Profiles

Add a Profile

Profile Name	Comments	Actions
Super Admin	super admin	
Firewall Admins	Admins to configure the firewall policies	✎ ✖
Service-Admin	For configuring UTM services	✎ ✖
VPN-Admin	for configuring VPN sevices	✎ ✖

Legend: ✎ Edit ✖ Remove

Admin Profiles Table - Column Descriptions	
Column	**Description**
Profile Name	Create a short but descriptive label for the role. You can change this at any time by clicking the 'Edit' icon.
Comments	A short description of the role.
Actions	Control buttons for editing/removing the admin profile. ✎ - Edit name, description and role privileges ✖ - Remove the profile

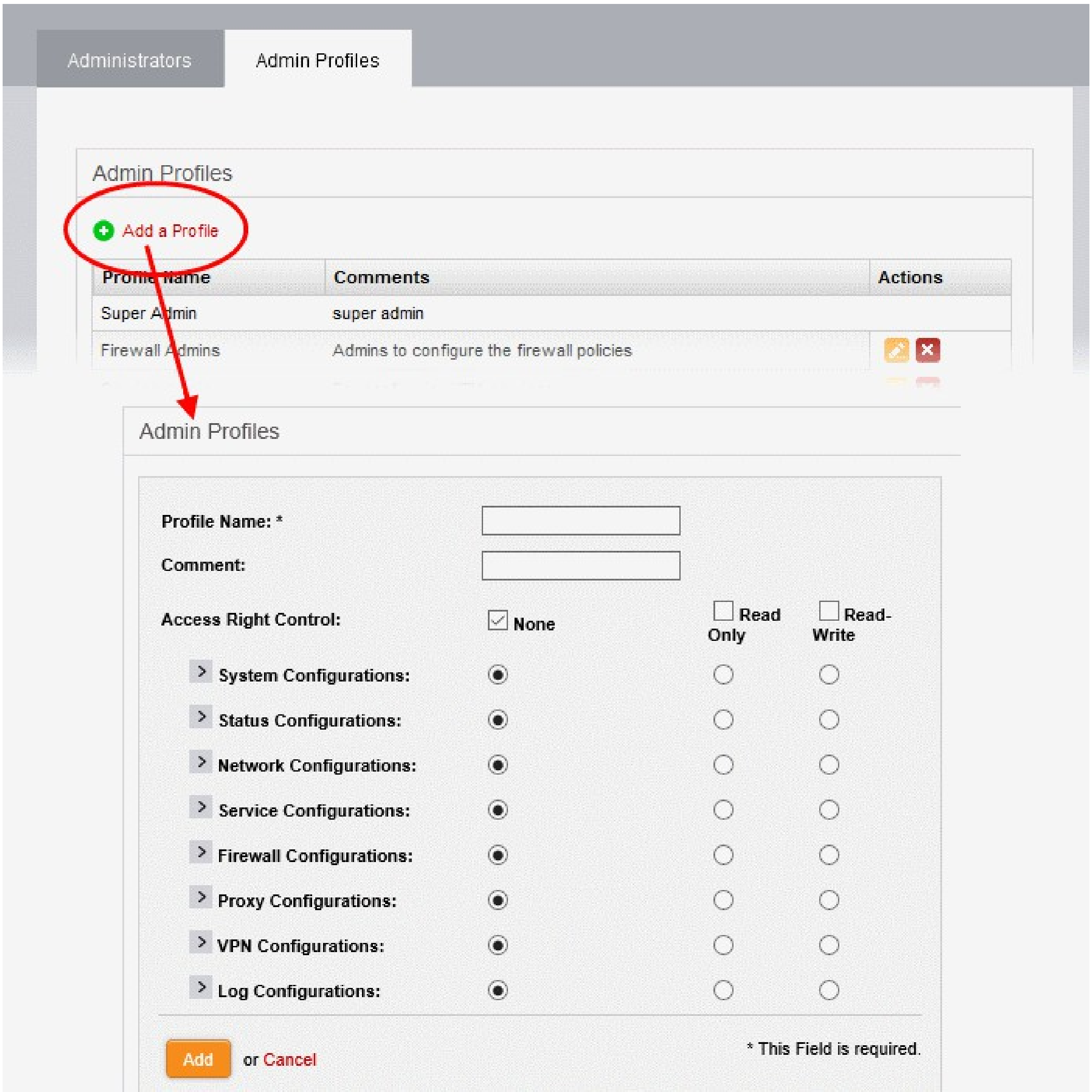
Note: Role management activities like adding, editing and removing profiles are logged. Items logged are, date, time, type of event, subject id, component name and output of the event . Role management is a part of access control.

The following sections provide detailed guidance on:

- **Adding a new admin profile**
- **Editing an admin profile**
- **Removing an admin profile**

To add an admin profile

- Click the 'Add a Profile' link from the top left of the 'Admin Profiles' interface. The interface for adding a new profile will appear.



Admin Profiles

Add a Profile

Profile Name	Comments	Actions
Super Admin	super admin	
Firewall Admins	Admins to configure the firewall policies	

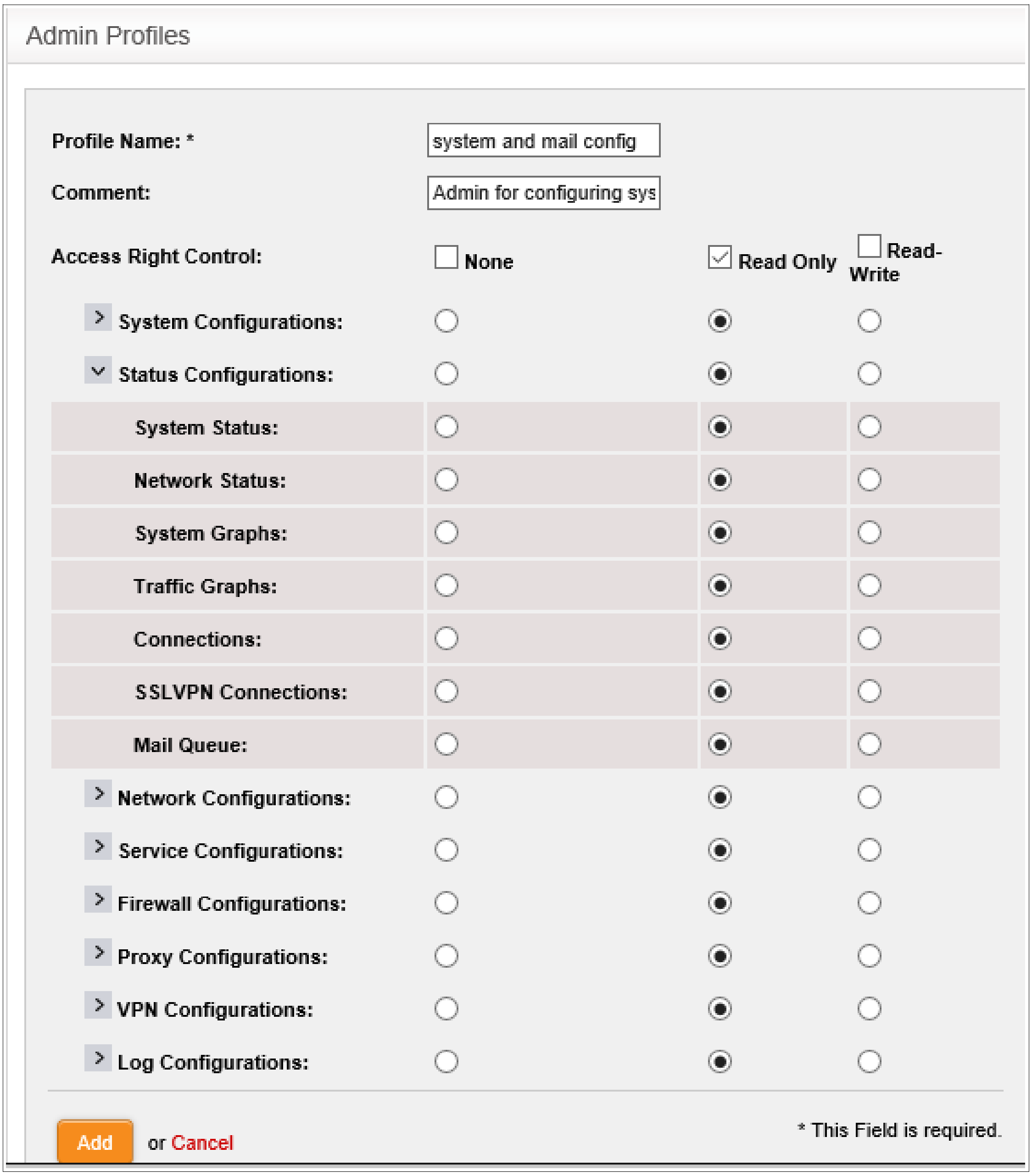
Admin Profiles

Profile Name: *			
Comment:			
Access Right Control:	☑ None	□ Read Only	□ Read-Write
System Configurations:	●	○	○
Status Configurations:	●	○	○
Network Configurations:	●	○	○
Service Configurations:	●	○	○
Firewall Configurations:	●	○	○
Proxy Configurations:	●	○	○
VPN Configurations:	●	○	○
Log Configurations:	●	○	○

Add or Cancel

* This Field is required.

- Enter the details of the new admin role as given below:
  - Profile Name: Enter a name to identify the profile role
  - Comment: Enter a short description of the new role
  - Access Right Control: Select the modules accessible and options configurable by the administrators assigned with the new role. The default is 'None' (no access) for all modules.
    - To provide full access to all modules, select the 'Read-Write' checkbox. Use the radio buttons underneath the checkbox to enable this privilege on a per-module basis.
    - To provide read-only access to all modules, select 'Read-Only' checkbox. Use the radio buttons underneath the checkbox to enable this privilege on a per-module basis.
    - To block access to all modules, select the 'None' checkbox. Use the radio buttons underneath the checkbox to block access on a per-module basis.
  - You can expand each module by clicking the arrow next to the module label. This allows you to define even more granular access rights:



Admin Profiles

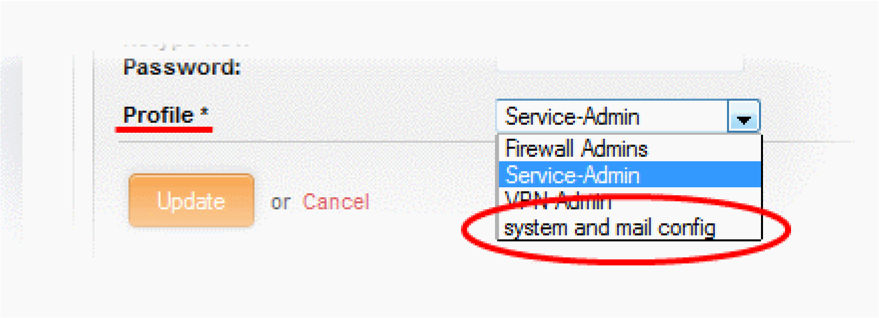
Profile Name: * system and mail config

Comment: Admin for configuring sys

Access Right Control:	□ None	☑ Read Only	□ Read-Write
System Configurations:	○	●	○
Status Configurations:	○	●	○
System Status:	○	●	○
Network Status:	○	●	○
System Graphs:	○	●	○
Traffic Graphs:	○	●	○
Connections:	○	●	○
SSLVPN Connections:	○	●	○
Mail Queue:	○	●	○
Network Configurations:	○	●	○
Service Configurations:	○	●	○
Firewall Configurations:	○	●	○
Proxy Configurations:	○	●	○
VPN Configurations:	○	●	○
Log Configurations:	○	●	○

- Click 'Add' to save the new role

The new role will be available for selection while adding a new administrator or editing an existing administrator.

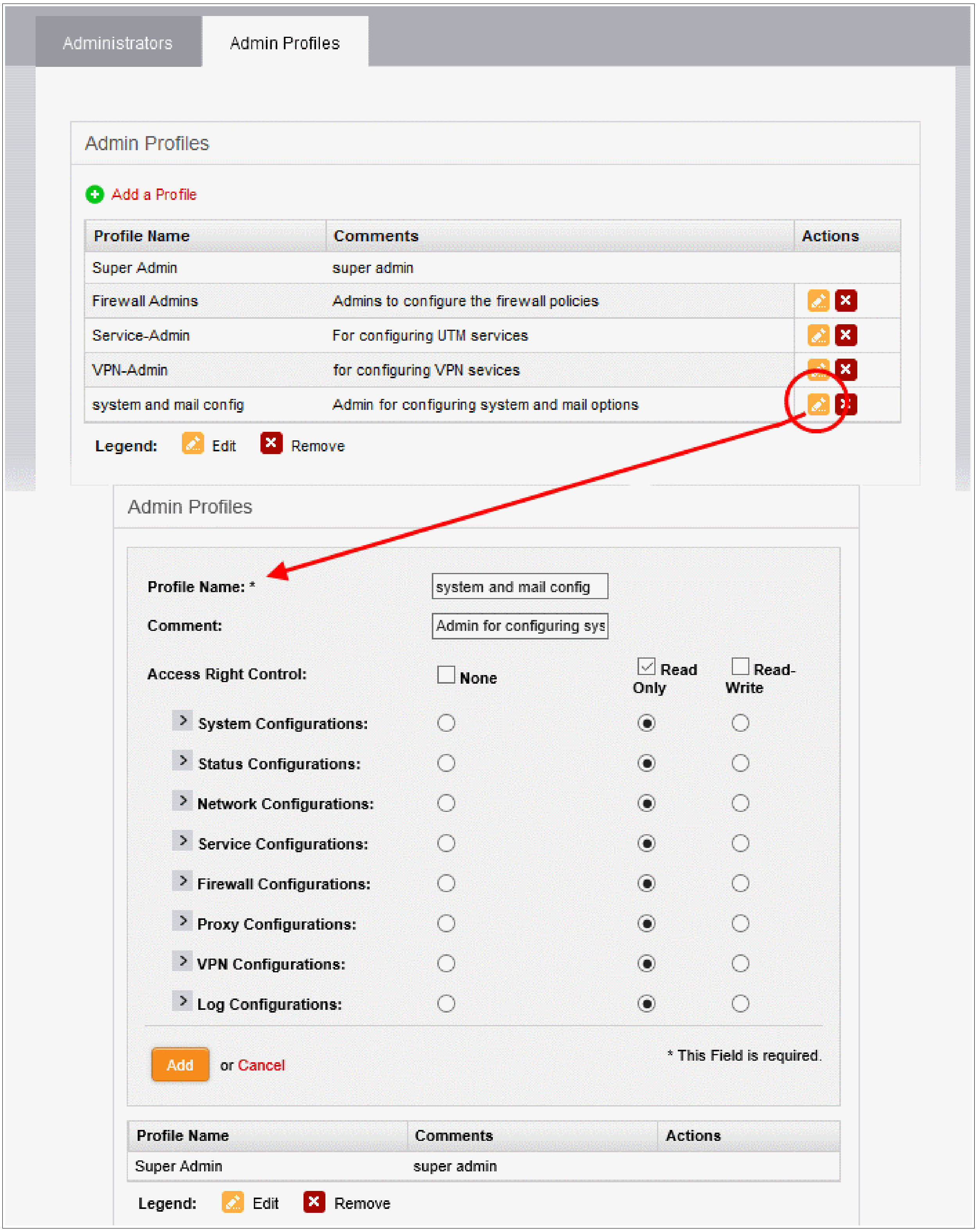


Password:

Profile * Service-Admin

To edit an admin profile

- Click the 'Edit' button in the row of the admin profile to be edited. The interface for editing the details and changing the privileges will appear.



Admin Profiles

Add a Profile

Profile Name	Comments	Actions
Super Admin	super admin	
Firewall Admins	Admins to configure the firewall policies	✎ ✖
Service-Admin	For configuring UTM services	✎ ✖
VPN-Admin	for configuring VPN sevices	✎ ✖
system and mail config	Admin for configuring system and mail options	✎ ✖

Legend: ✎ Edit ✖ Remove

Admin Profiles

Profile Name: * system and mail config

Comment: Admin for configuring sys

Access Right Control:	□ None	☑ Read Only	□ Read-Write
System Configurations:	○	●	○
Status Configurations:	○	●	○
Network Configurations:	○	●	○
Service Configurations:	○	●	○
Firewall Configurations:	○	●	○
Proxy Configurations:	○	●	○
VPN Configurations:	○	●	○
Log Configurations:	○	●	○

Add or Cancel * This Field is required.

Profile Name	Comments	Actions
Super Admin	super admin	

Legend: ✎ Edit ✖ Remove

- The Edit interface is similar to 'Add Admin Profile' interface. Edit the details as required and click 'Update' for your changes to take effect. See **section above** for more details.

To remove an admin profile

- Remove the profile from the administrators to whom it was applied from the Administrators interface by editing the administrator. Refer to the explanation of **editing an administrator** in the section **Adding and Managing Administrators** for more details.
- Click the 'Delete' button ✖ in the row of the admin profile from the Admin Profiles interface. The role will be removed immediately.

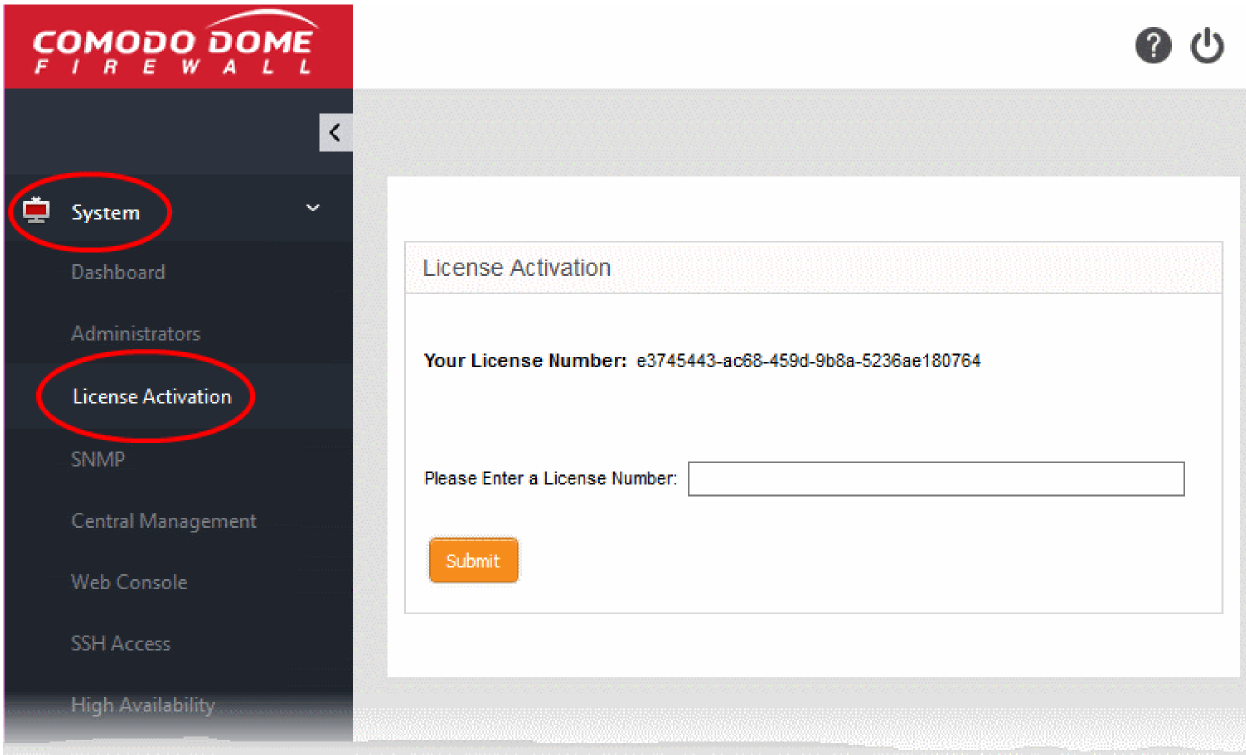
4.2 License Activation

You need to purchase a DFW license and activate it to use the application without interruption.

- The license can be purchased from Comodo at https://accounts.comodo.com
- Sign in to your Comodo Accounts Manager (CAM) account if you have one already. Else create a new CAM account and login.
- Click 'Sign up to Comodo Dome', select the DFW version that you want to subscribe for and complete the purchase process.
- The order confirmation with DFW license details will be sent to your registered email address.

To activate your DFW license

- Click 'System' > 'License Activation' from the left hand side navigation.

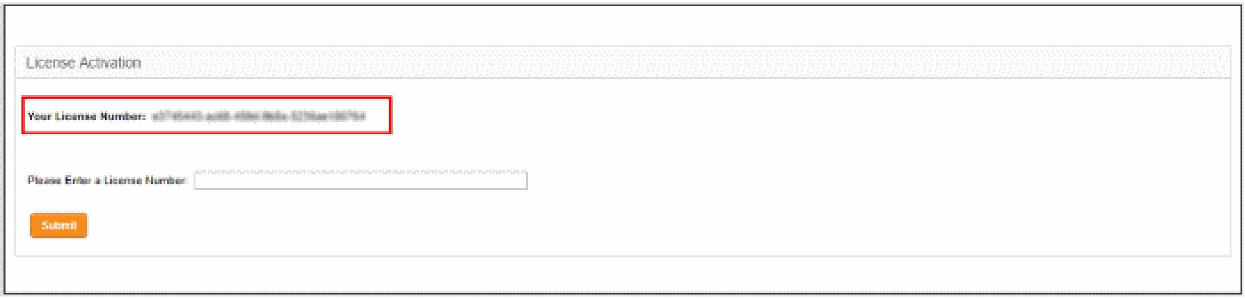


License Activation

Your License Number: e3745443-ac68-459d-9b8a-5236ae180764

Please Enter a License Number:

- Enter the license details in the 'License Number' field and click 'Submit'
- The license will be verified and if found valid, your DFW will be activated



License Activation

Your License Number: [redacted]

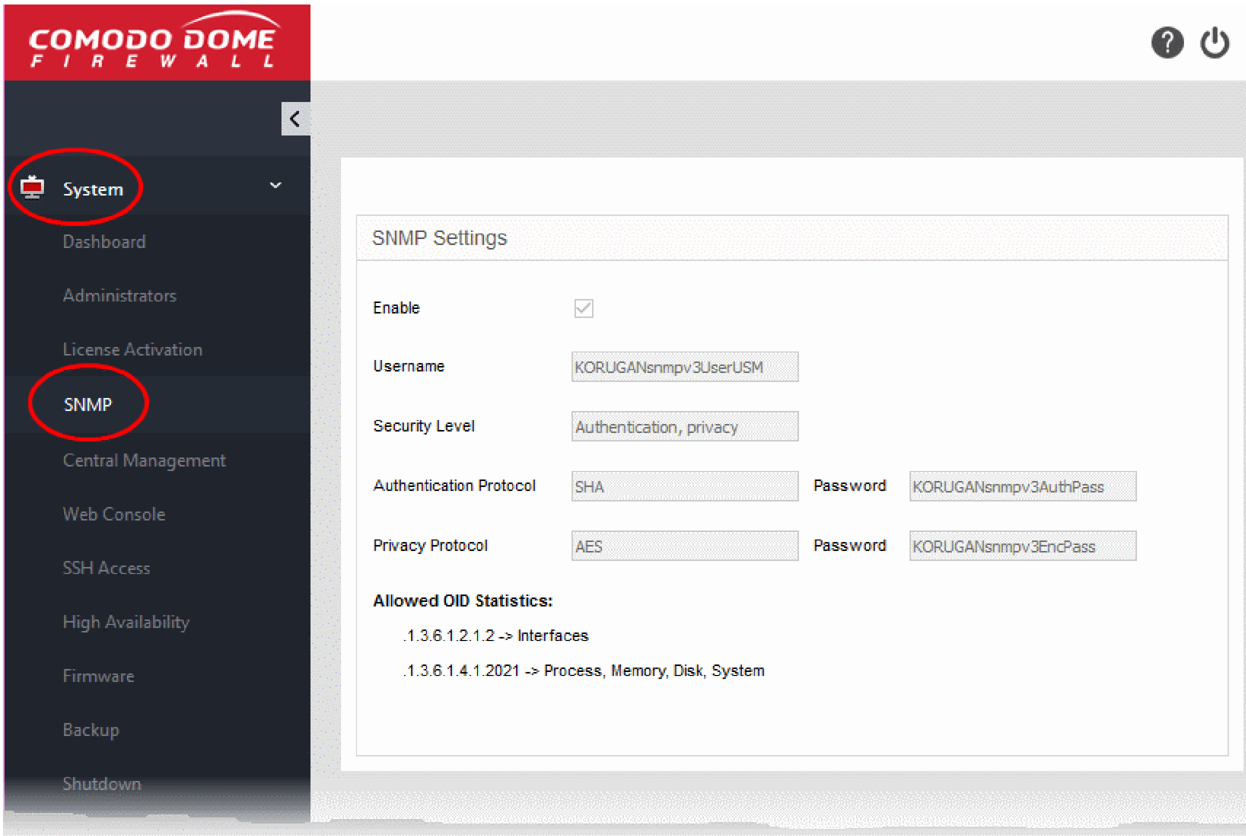
Please Enter a License Number:

4.3 SNMP Settings

Simple Network Management Protocol (SNMP) is the standard way of monitoring software and hardware to collect performance metrics and then display this statistics in the dashboard. SNMP is enabled by default and you can only view the settings.

To view SNMP settings

- Click 'System' > 'SNMP' from the left hand side navigation.



SNMP Settings

Enable ☑

Username KORUGANsnmpv3UserUSM

Security Level Authentication, privacy

Authentication Protocol SHA Password KORUGANsnmpv3AuthPass

Privacy Protocol AES Password KORUGANsnmpv3EncPass

Allowed OID Statistics:

.1.3.6.1.2.1.2 -> Interfaces

.1.3.6.1.4.1.2021 -> Process, Memory, Disk, System

The settings are non editable.

4.4 Central Management

- Dome Firewall Central Manager allows you to remotely manage multiple Dome Firewall appliances from a single centralized console.
- The firewall virtual appliance has an in-built client which can communicate with the central manager. This allows the appliance to receive commands from the manager and apply them to the firewall.
- The 'Central Management' interface allows you to enable the client service and configure it to connect to the central manager.
- Note: You need the IP address of the central manager to which you wish to enroll your firewall appliance.

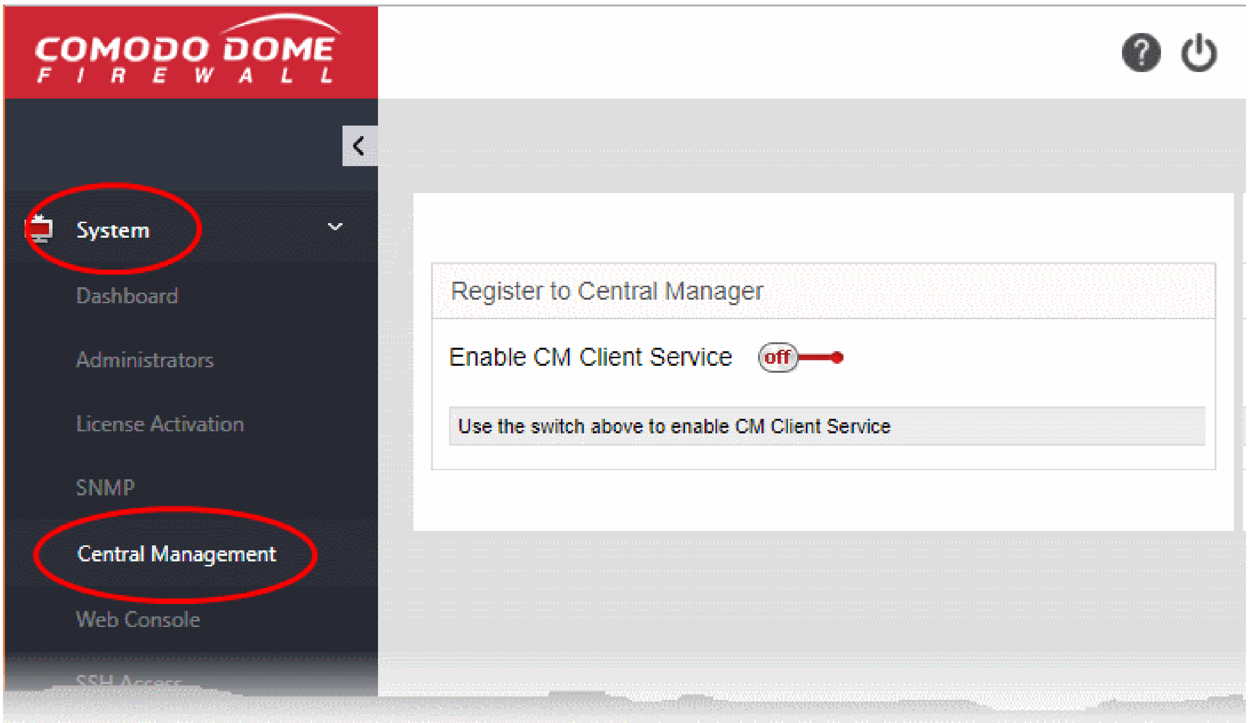
After enrolling an appliance, the central manager allows admins to remotely execute various tasks, including:

- Create and apply rules to the device. You can apply firewall policy rules, source network address translation (SNAT) rules, destination network address translation (DNAT) rules, system access rules and more.
- Create and manage firewall address objects, object groups, web filtering profiles, advanced threat protection profiles and intrusion prevention profiles
- Manage interfaces connected to different ports of the remote firewall device

The full guide for the central manager is available at **https://help.comodo.com/topic-436-1-920-12359-Introduction-to-Dome-Firewall-Central-Manager.html**

To add your firewall appliance to a central manager

- Click 'System' on the left then choose 'Central Management'

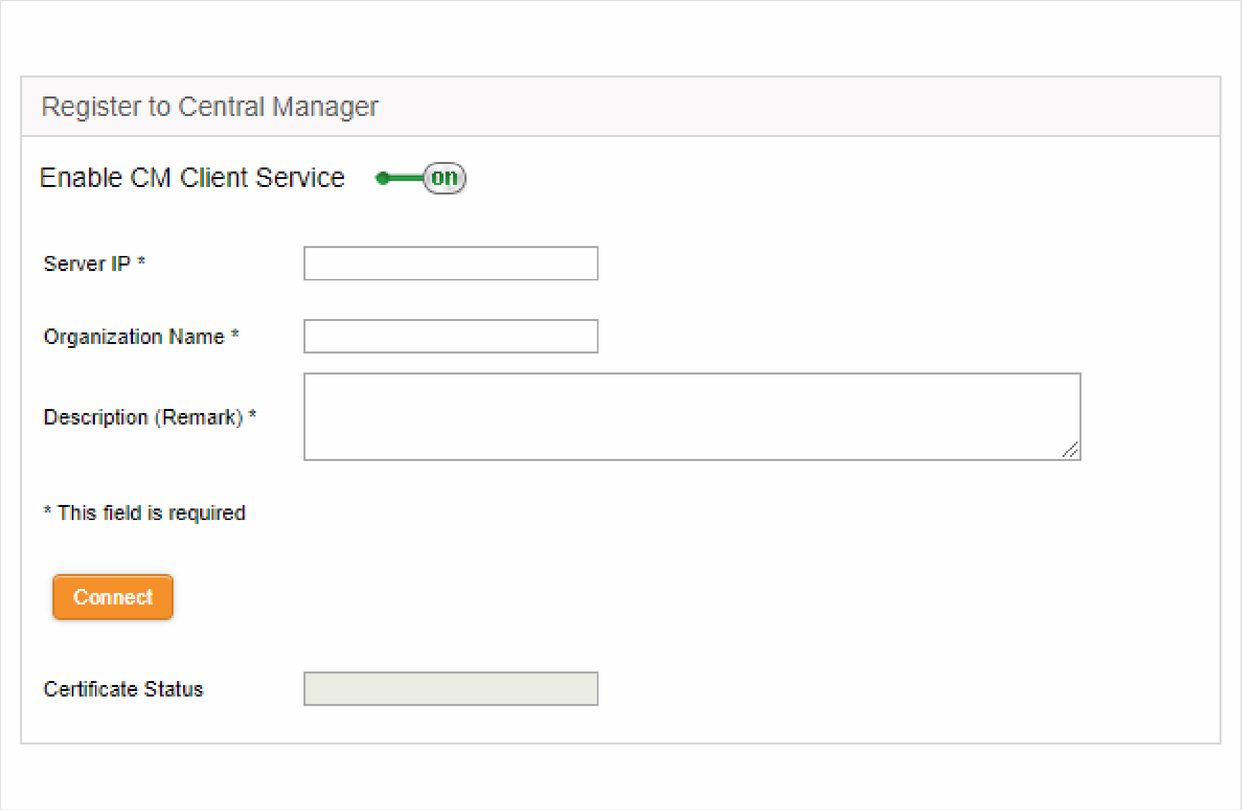


Register to Central Manager

Enable CM Client Service off

Use the switch above to enable CM Client Service

- Move the 'Enable CM Client Service' switch to the 'ON' position



Register to Central Manager

Enable CM Client Service on

Server IP *

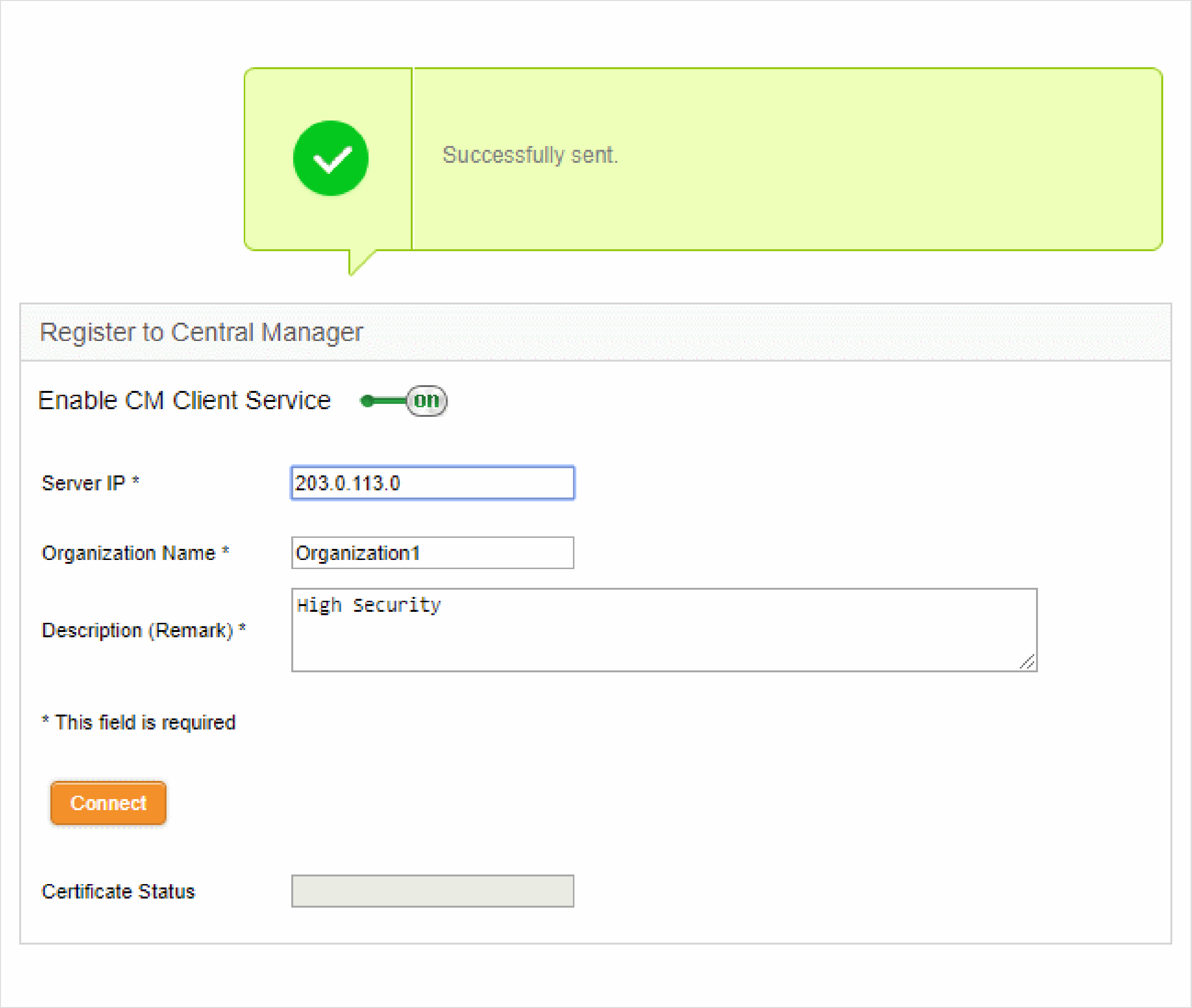
Organization Name *

Description (Remark) *

* This field is required

Certificate Status

- Enter the parameters required to connect your firewall appliance to central manager
    - Server IP - The IP address of the Comodo Dome Firewall Central Manager
    - Organization Name - The name of your organization. Your firewall device will be assigned to this organization in Dome central manager. You can assign multiple devices to the same organization so they can be managed collectively in central manager.
    - Description - Type any additional information you see fit to provide about the firewall. This information will be shown to the central manager administrator charged with approving new devices.
- Click 'Connect' to send an enrollment request to the central manager admin.



Successfully sent.

Register to Central Manager

Enable CM Client Service

Server IP *	203.0.113.0
Organization Name *	Organization1
Description (Remark) *	High Security

* This field is required

Certificate Status

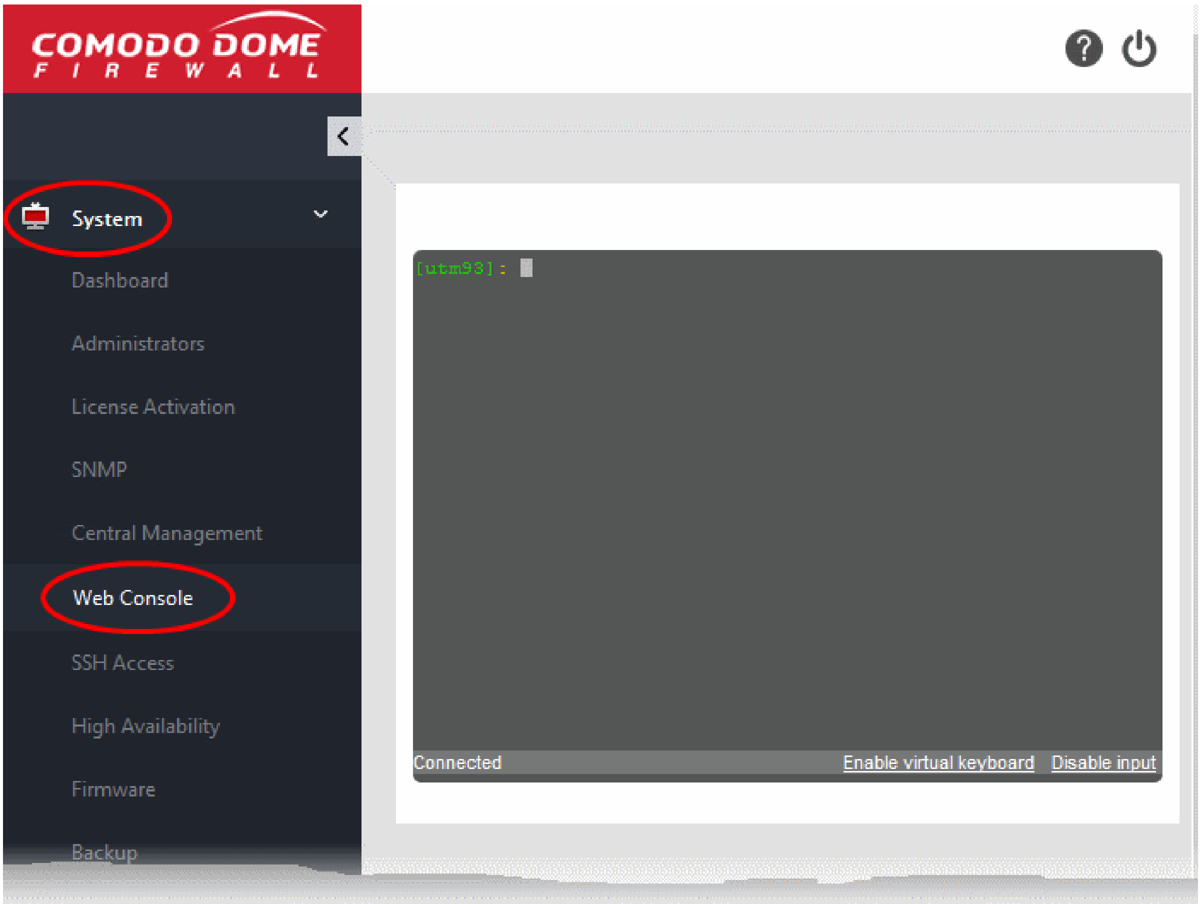
- The firewall now needs to be approved by the central manager admin. This can be done in central manager by clicking the 'Approve Device' link in the left-hand menu.
- Once approved, the appliance status can be remotely managed from the central manager.

4.5 Access the Web Console

- Comodo Dome Firewall allows you to execute tasks through a command line interface (CLI). Admins that have shell access can use the CLI to execute commands to manage and configure the firewall.
- Note: Misuse of the web console could risk the security of your operations. Access to the console should be provided with caution because it allows access to information and assets inaccessible via Dome Firewall's GUI interfaces.

To access the CLI

- Click 'System' > 'Web Console' tab from the left hand side navigation



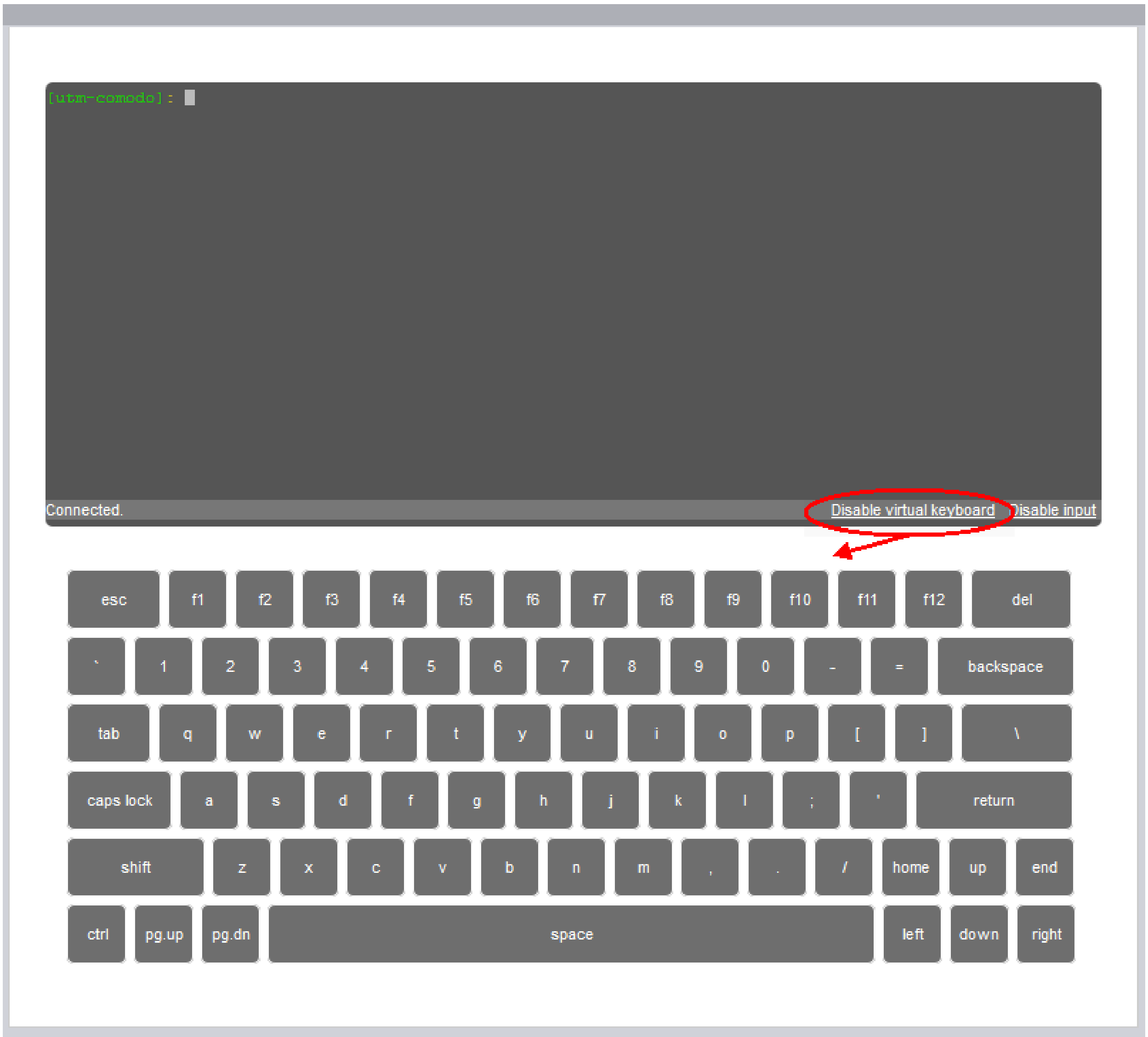
```
[utm93]:
```

A command line interface, resembling a Linux Terminal window, will open inside the browser window. The CLI connects with DFW and indicates the connection status at the bottom left. The administrator can enter the commands for management and configuration of the DFW.

The CLI also provides a virtual keyboard for secure input of the configuration data to the console.

To use the virtual keyboard

- Click the Enable virtual keyboard link at the bottom right.



```
[utm-comodo]:
```

Connected.

A keyboard will be displayed beneath the console for entering the commands

To disconnect the CLI console

- Type 'Exit' and press Enter.

The console will be disconnected from the DFW and the status at the bottom left will change to 'Disconnected'.

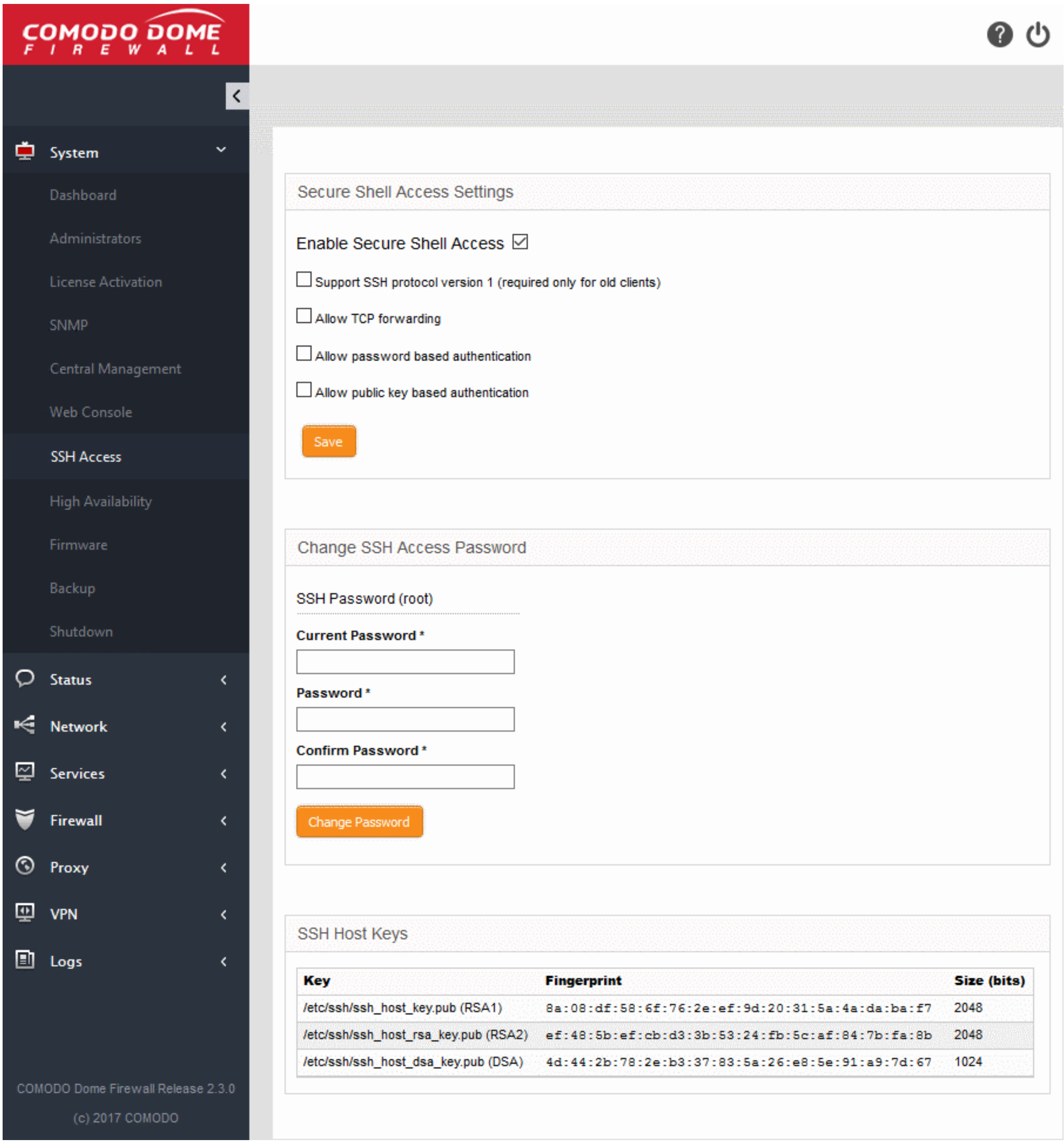
Tip: You can temporarily disable the input to the console from your physical keyboard by clicking the Disable input link at the bottom left. To re-enable the input, simply click the Enable input link at the same spot. This will not apply to the virtual keyboard.

4.6 Configure SSH Access

- Click 'System' on the left then select 'SSH access'

The SSH access interface allows you to enable remote SSH access to the DFW virtual appliance and thereby to enable access from clients in external network to the clients connected to local network and running any service that can be tunneled through SSH, like Telnet.

Note: SSH access grants access to important information and configuration data which are inaccessible via Dome Firewall's GUI interfaces. Administrators should provide SSH access and authorization with caution.



Secure Shell Access Settings

Enable Secure Shell Access ☑

□ Support SSH protocol version 1 (required only for old clients)

□ Allow TCP forwarding

□ Allow password based authentication

□ Allow public key based authentication

Save

Change SSH Access Password

SSH Password (root)

Current Password *

Password *

Confirm Password *

Change Password

SSH Host Keys

Key	Fingerprint	Size (bits)
/etc/ssh/ssh_host_key.pub (RSA1)	8a:08:df:58:6f:76:2e:ef:9d:20:31:5a:4a:da:ba:f7	2048
/etc/ssh/ssh_host_rsa_key.pub (RSA2)	ef:48:5b:ef:cb:d3:3b:53:24:fb:5c:af:84:7b:fa:8b	2048
/etc/ssh/ssh_host_dsa_key.pub (DSA)	4d:44:2b:78:2e:b3:37:83:5a:26:e8:5e:91:a9:7d:67	1024

Secure Shell Access Settings:

- Enable Secure Shell Access - Allows you to enable/disable the SSH access.
- Support SSH protocol version 1 - Select this option only if you are using old SSH client that do not support the newer versions of the SSH protocol.
- Allow TCP forwarding - Select this option to allow other protocols like TCP to tunnel through SSH.
- Allow password based authentication - Select this option if you plan to use password type authentication for administrators logging-in to the DFW administrative console through SSH access. The password can be specified in the **Change SSH Access Password** field.
- Allow public key based authentication - Select this option if you plan to use public key type authentication for administrators logging-in to the DFW administrative console through SSH access. As a prerequisite, The public keys need to be added to the file */root/.ssh/authorized_keys*.
- Select the required options and click 'Save' for your configurations to take effect.

Change SSH Access Password

The administrator can specify the password for SSH access from external network.

- SSH Password (root) - The password for the administrator that can login to the shell for administration. Logins can be made either via the serial console, or remotely with an SSH client.
  - Enter the password and confirm the same in the required boxes and click 'Change password' for the new password to take effect.

Note: Passwords should be at least eight characters long and not easily guessed. They should contain a mixture of upper and lower case letters, numbers and special characters.

SSH host keys

The SSH host keys table displays a list of public SSH host keys of the DFW virtual appliance, generated during the initial connection of the openSSH server, along with their fingerprint and key size in bits.

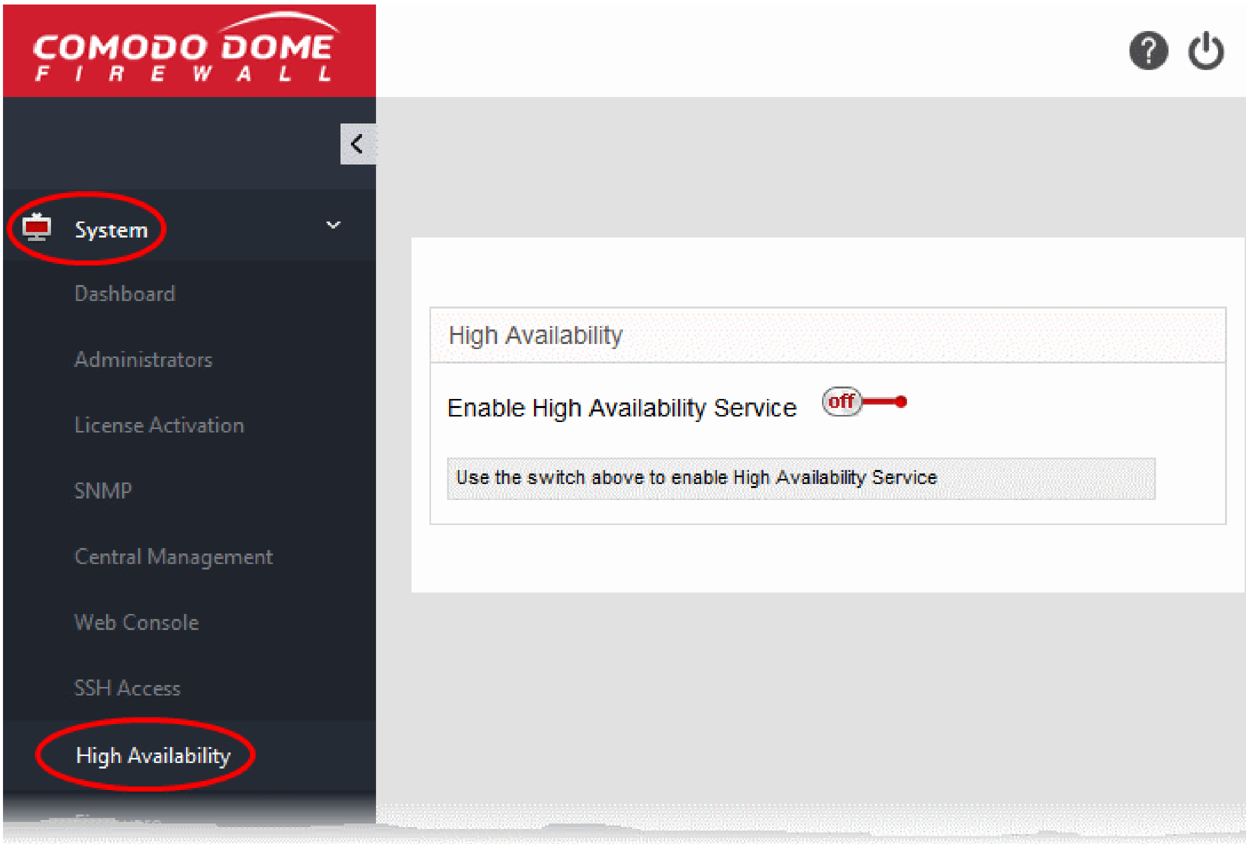
Note: For a client to be accessible from an external network through SSH access, the client needs to be reachable from the external device. You can create a firewall rule under Firewall > System access to allow access to the client from the external device. See **Configuring System Access** for more details.

4.7 High Availability

- Click 'System' on the left then select 'High Availability'

The 'High Availability' screen allows you to configure an 'Active-Passive' failover formation for your Dome Firewall virtual appliance. This helps ensure continuity of operations and avoids a single point of failure.

- To configure the feature, you need to specify the IP address of a second Dome Firewall virtual appliance.
- Once set up, the slave Dome Firewall server will take over operations should the master server fail.
- The two devices share a virtual IP address.
- Please note that SSH Access must be enabled for this feature to work. See **Configure SSH Access** for guidance on enabling SSH Access.



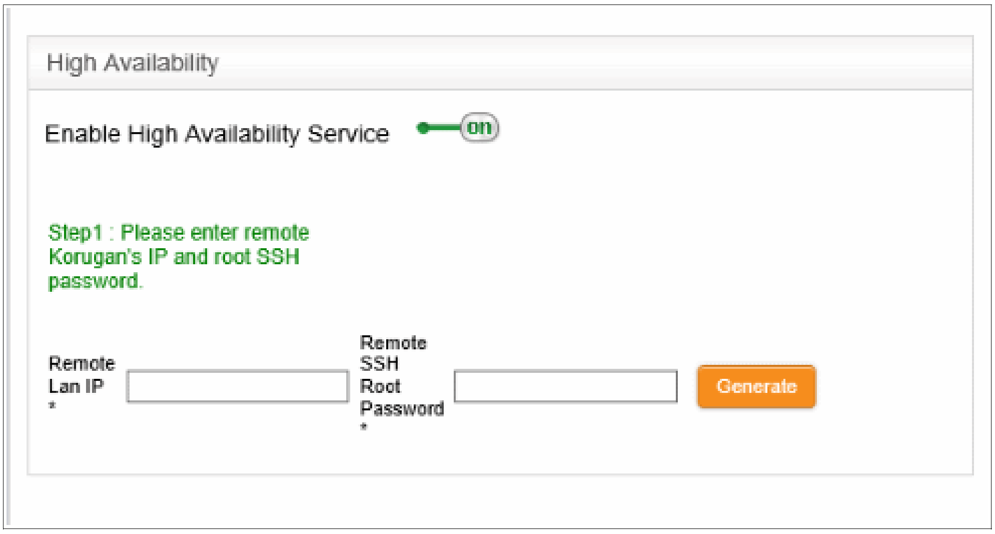
High Availability

Enable High Availability Service off

Use the switch above to enable High Availability Service

To enable High Availability

- Click 'System' > 'High Availability'
- Toggle the 'Enable High Availability Service' switch to 'On':



High Availability

Enable High Availability Service on

Step1 : Please enter remote Korugan's IP and root SSH password.

Remote Lan IP *

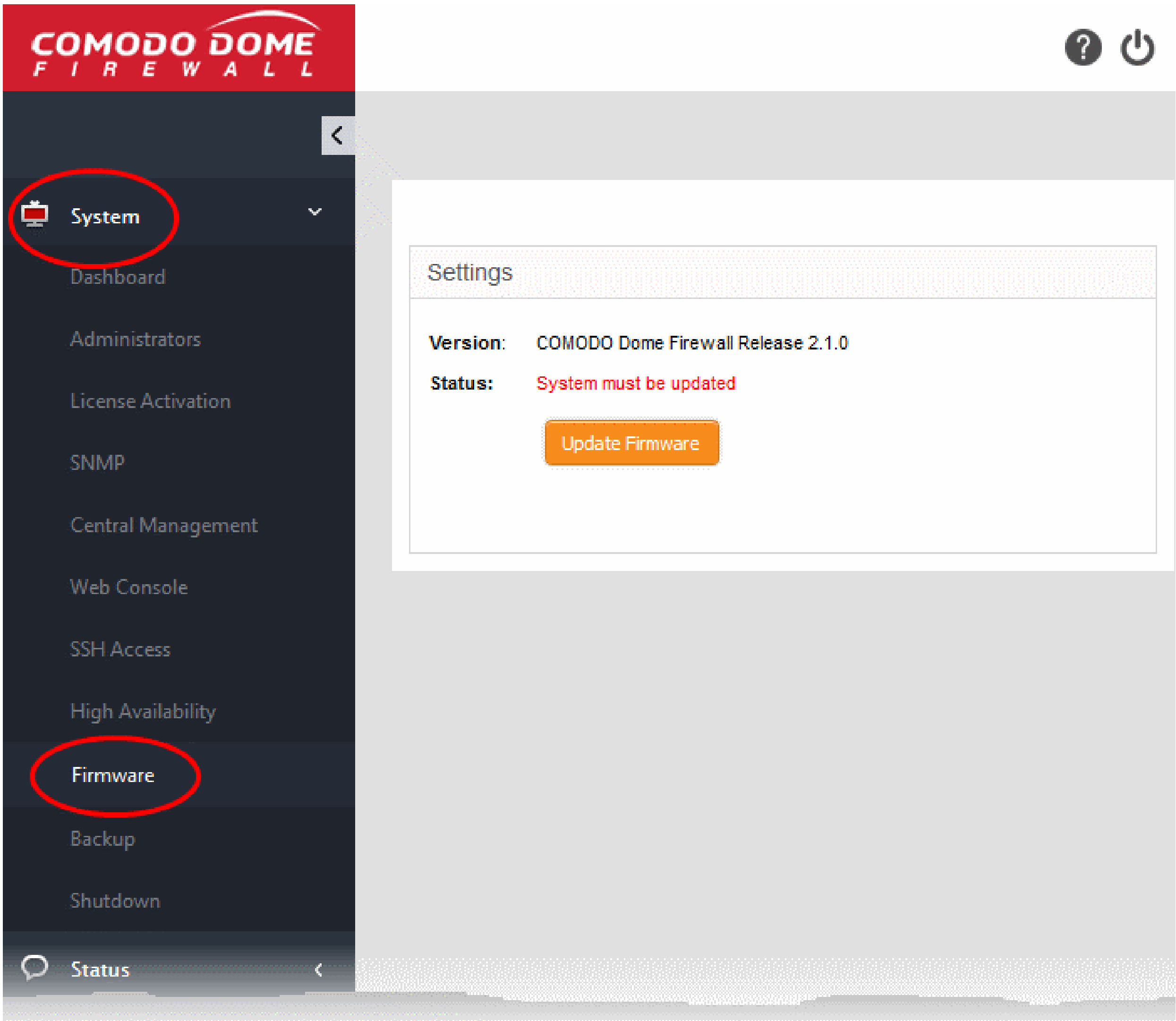
Remote SSH Root Password *

- Enter your 'Remote LAN IP'. For example, if two Dome Firewall devices, 1 (10.10.10.2) and 2 (10.10.10.3), share a remote LAN IP address such as 10.10.10.1, you need to enter this address in both master and slave Dome Firewall devices. The IP address 10.10.10.1 is directed to device 1 (10.10.10.2) and during fail-over is redirected to device 2 (10.10.10.3).
- Enter 'Remote SSH Root Password' to provide secure remote login over an unsecured network.
- Click 'Generate' to establish connection to the slave Dome Firewall device and thus provide high availability.

4.8 View and Update Firmware Version

- Click 'System' on the left then select 'Firmware'.

The 'Firmware Settings' screen displays the version number of the firmware installed on the DFW virtual appliance and its update status. Also, if an new version is available, the administrator can initiate the update process.



Version: COMODO Dome Firewall Release 2.1.0

Status: System must be updated

- **Version** - Shows the version number of the Comodo Dome Firewall Firmware installed on your DFW virtual appliance
- **Status** - Indicates whether your firmware is up-to-date.
  - If it indicates 'System must be updated', click the 'Update Firmware' button to initiate the update process.
  - The firmware will be automatically downloaded and installed.

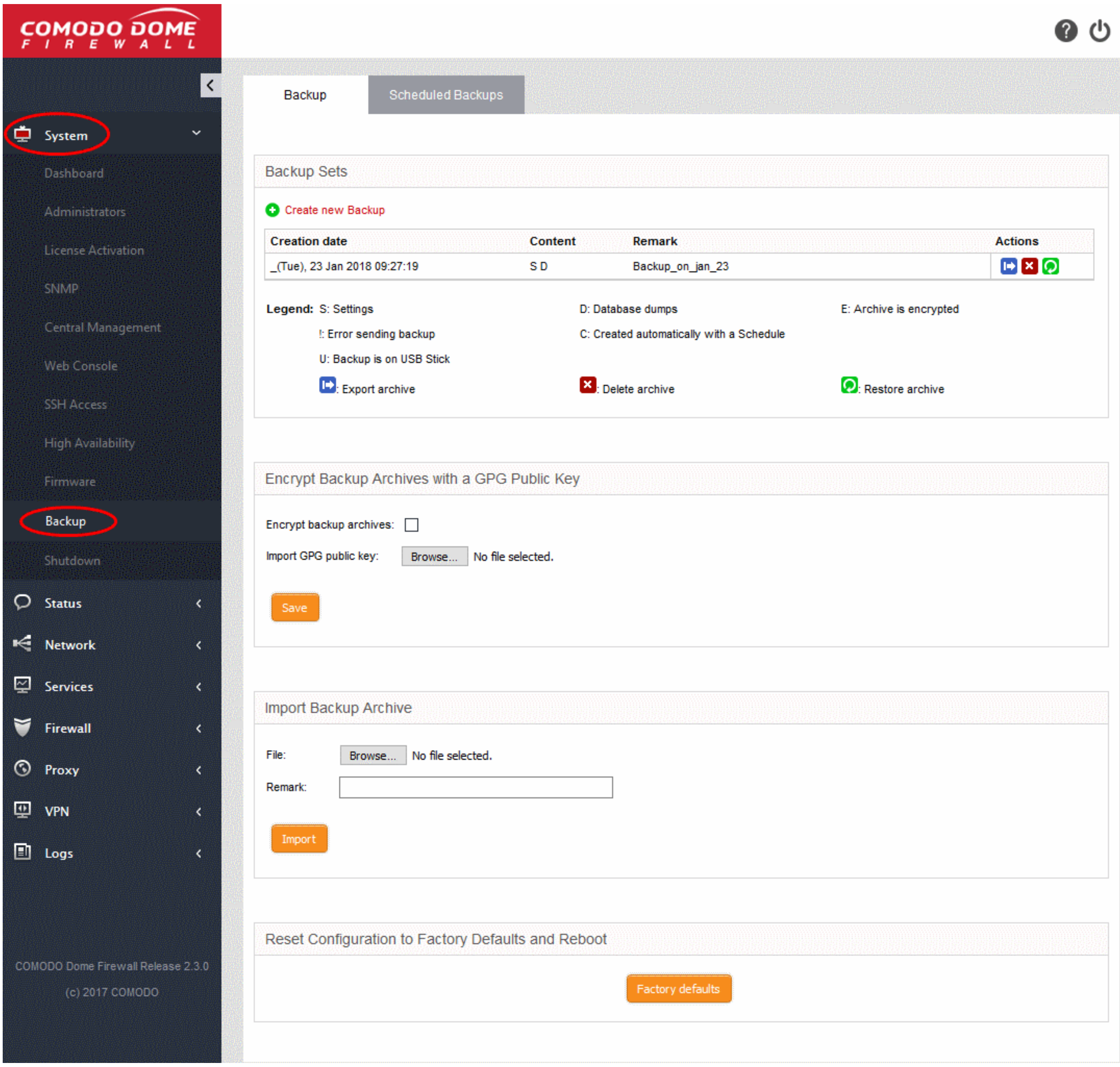
4.9 Create and Schedule Backup of DFW State

- Comodo Dome Firewall allows you to backup the current state of the firewall at any time. Each backup includes the configuration settings, logs and database dumps.
- Backups can be manually created at any time or automatically created according to a schedule.
- Backups can be encrypted and can be stored locally, on a USB stick or emailed for storage in a remote location.

- You can restore the firewall to any backup by clicking the 'Restore Archive' button.
- If required, you can also restore the virtual appliance to default settings and reconfigure the virtual appliance from the scratch.

To open the Backup interface

- Click 'System' > 'Backup' in the left-hand navigation



Backup Sets

Create new Backup

Creation date	Content	Remark	Actions
_(Tue), 23 Jan 2018 09:27:19	S D	Backup_on_jan_23	

Legend: S: Settings D: Database dumps E: Archive is encrypted
!: Error sending backup C: Created automatically with a Schedule
U: Backup is on USB Stick
: Export archive : Delete archive : Restore archive

Encrypt Backup Archives with a GPG Public Key

Encrypt backup archives: □

Import GPG public key: Browse... No file selected.

Save

Import Backup Archive

File: Browse... No file selected.

Remark:

Import

Reset Configuration to Factory Defaults and Reboot

Factory defaults

The 'Backup Sets' area at the top shows a list of backups created so far. If a USB drive containing backups is plugged-in to the virtual appliance then those backups will also be shown in the list.

The page also allows you to export backups for archiving, restore from a backup, import a backup and to reset the firewall to factory settings.

<table>
<tr><th colspan="2">Backup Sets - Column Descriptions</th></tr>
<tr><th>Column Header</th><th>Description</th></tr>
<tr><td>Creation date</td><td>Precise date and time at which the backup was created</td></tr>
<tr><td>Content</td><td>Shows backup components, attributes and any error messages:
<table>
<tr><th>Character</th><th>Expansion</th><th>Description</th></tr>
<tr><td>C</td><td>Chronological</td><td>This is a scheduled backup that was created automatically</td></tr>
<tr><td>D</td><td>Database dumps</td><td>Contains database dumps</td></tr>
<tr><td>E</td><td>Encrypted</td><td>The backup is encrypted</td></tr>
<tr><td>S</td><td>Settings</td><td>Contains configurations and settings</td></tr>
<tr><td>U</td><td>USB</td><td>The backup is stored on a USB drive</td></tr>
<tr><td>!</td><td>Error</td><td>The backup operation failed</td></tr>
</table>
</td></tr>
<tr><td>Remark</td><td>A short description entered by the administrator during backup creation</td></tr>
<tr><td>Actions</td><td>Displays control buttons for exporting, deleting and restoring the backups
➡ - Exports the backup to your local device
✖ - Deletes the backup
↻ -Restores the firewall using this backup.</td></tr>
</table>

The following sections explain in backup task in more detail:

- **Manually creating a backup**
- **Scheduling backup operations**
- **Encrypting Backup Archives**
- **Exporting a backup**
- **Importing a backup from an archive**
- **Rolling back the virtual appliance to a previous time point**
- **Resetting the virtual appliance to factory defaults**

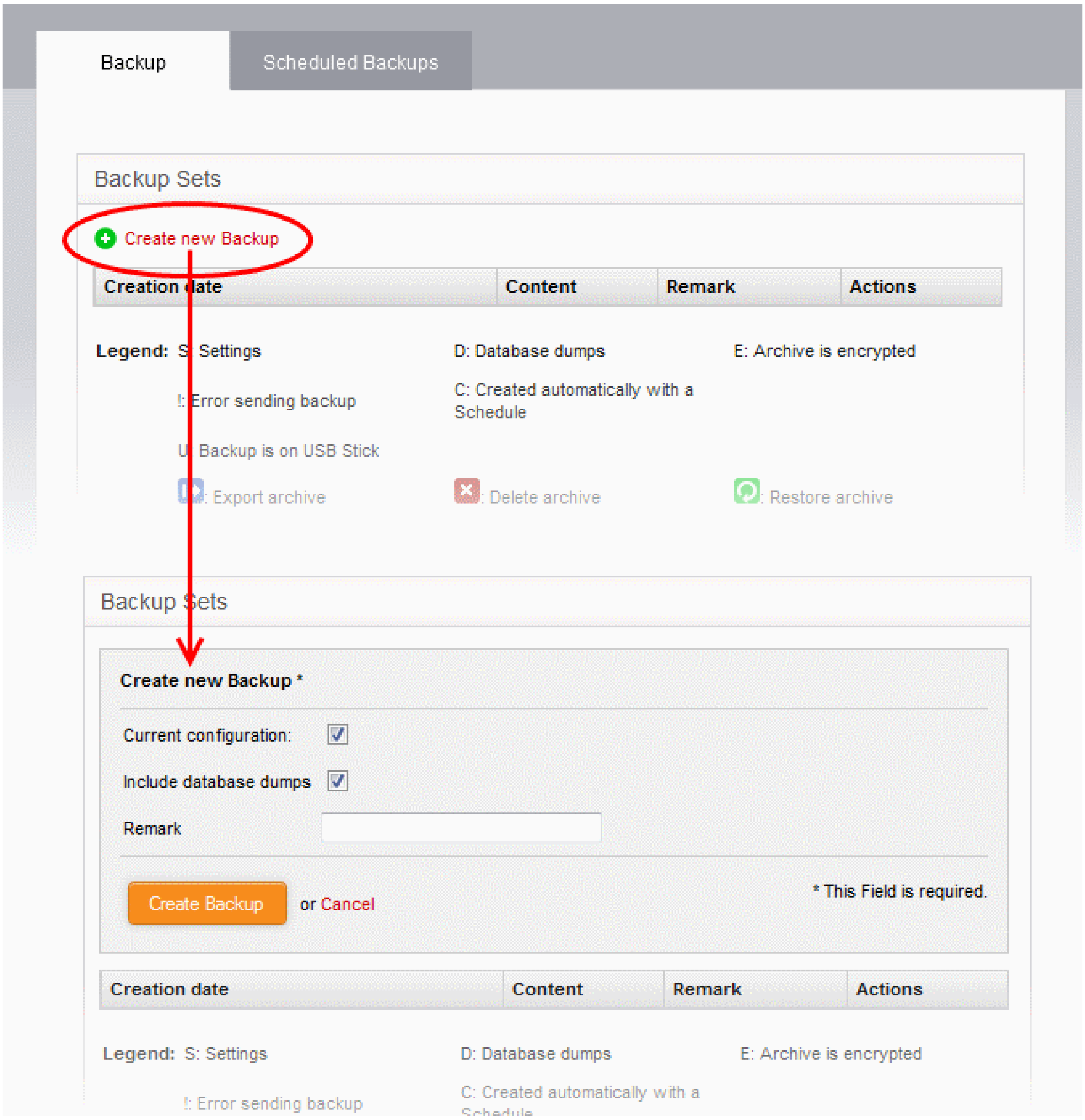
4.9.1 Manually Create a Backup

Admins can manually create a backup at any desired time. For example, you may wish to do this before making a critical configuration change. The backup can be stored either locally in the virtual appliance or on a USB drive.

To create a backup

- Open the Backup interface by clicking 'System' > 'Backup' from the left hand side navigation
- Ensure that the Backup tab is open
- Click the 'Create new backup' link above the list of backups

The 'Create new Backup' pane will open.



Backup Sets

Create new Backup

Creation date	Content	Remark	Actions

Legend: S: Settings | D: Database dumps | E: Archive is encrypted

!: Error sending backup | C: Created automatically with a Schedule

U: Backup is on USB Stick

: Export archive | : Delete archive | : Restore archive

Backup Sets

Create new Backup *

Current configuration: ☑

Include database dumps ☑

Remark

Create Backup or Cancel

* This Field is required.

Creation date	Content	Remark	Actions

Legend: S: Settings | D: Database dumps | E: Archive is encrypted

!: Error sending backup | C: Created automatically with a Schedule

- Choose the components to be included in the backup:
  - Current configuration - Includes the current configuration of the virtual appliance in the backup. Deselect the checkbox if you do not want the current configuration to be backed up.
  - Include database dumps - Adds the DFW database content and logs to the backup. Deselect the checkbox if you do not want these components to be included.
- Enter a short description or remark for the backup in the text box. This description will appear in the 'Remark' column in the list of backup archives.
- If you want to store the backup in a USB drive ensure that you have plugged-in the USB drive to the virtual appliance. A new option 'Create Backup on USB Stick' will appear below the 'Remark' text box. Select the option to save the backup to the USB drive.
- Click 'Create Backup'.

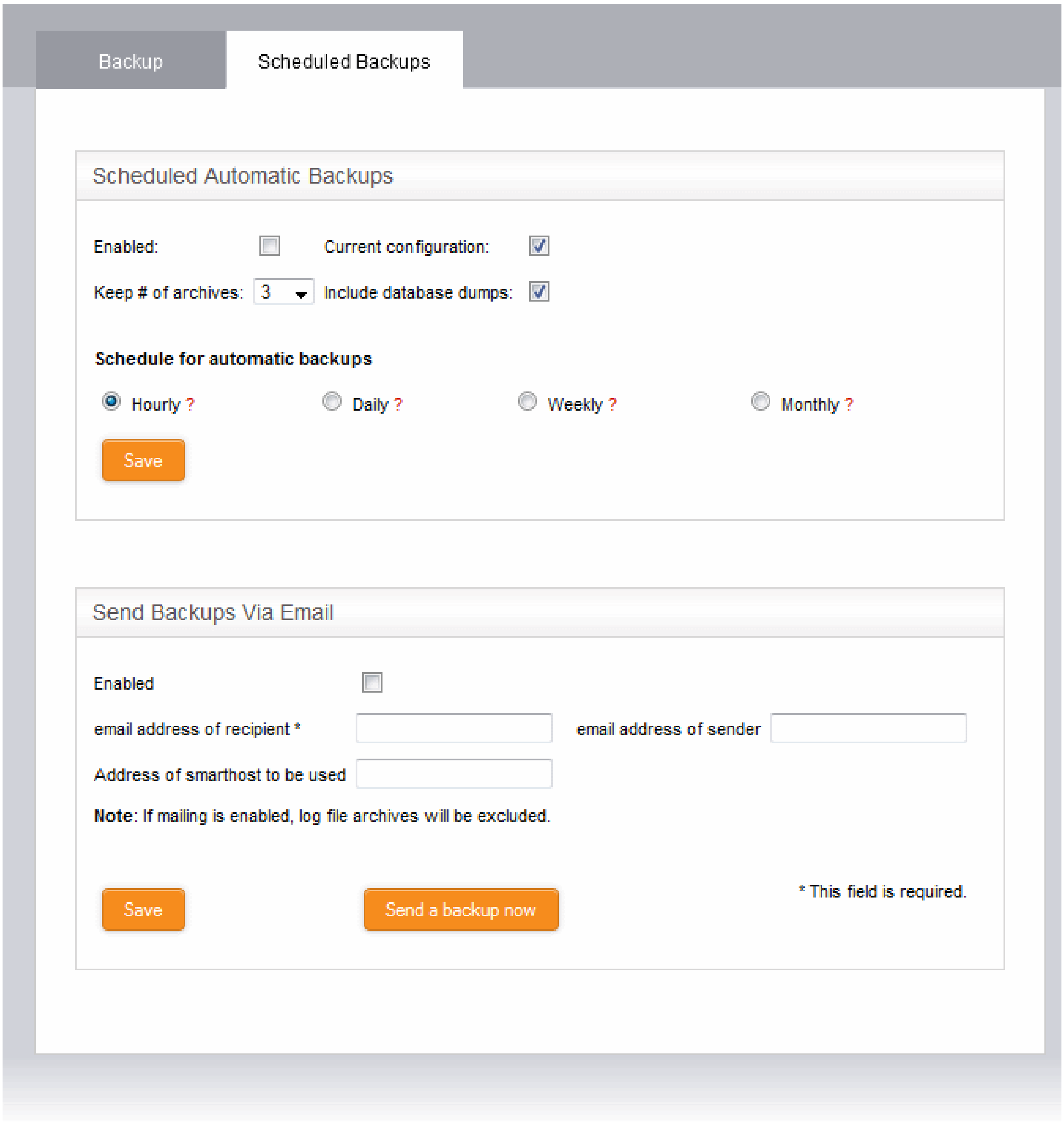
The backup will be created and added to the list of backups. If encryption is enabled, the backup file will be encrypted and saved. See **Encrypting Backup Archives** for more details.

4.9.2 Schedule Backup Operations

The administrator can configure scheduled backup operations to automatically create backups at selected periodical intervals. The backups can be configured to be stored locally or to be emailed to a specified email address for storing the backup archive at a remote location.

To create a backup schedule

- Open the Backup interface by clicking 'System' > 'Backup' from the left hand side navigation
- Click the 'Scheduled backups' tab to open Scheduled backups interface



Scheduled Automatic Backups

Enabled: □ Current configuration: ☑

Keep # of archives: 3 Include database dumps: ☑

Schedule for automatic backups

● Hourly ? ○ Daily ? ○ Weekly ? ○ Monthly ?

Send Backups Via Email

Enabled □

email address of recipient * email address of sender

Address of smarthost to be used

Note: If mailing is enabled, log file archives will be excluded.

* This field is required.

Scheduled automatic backups

- Configure the scheduled backup job under the Scheduled automatic backups
  - Enabled - Select this check box to activate the backup schedule
  - Current Configuration - Select this option if you want the configuration at the time of creating the backup to be included in the backup

- Include database dumps - Adds the DFW database content and logs to the backup. Deselect the checkbox if you do not want these components to be included.
- Keep # of archives - Select the number of previous scheduled backup archives that the DFW should retain, from the drop-down. The backup archives older than these will be deleted, whenever a new backup is created.
- Schedule for automatic Backups - Select the time interval for creating the automated backups:
  - Hourly - The backups will be created at every first minute of an hour
  - Daily - The back up will be created at 01:25 am everyday
  - Weekly - The back up will be created at 02:47 am on Sunday everyweek
  - Monthly - The back up will be created at 03:52 am on first day of every month
- Click Save for your configuration to take effect.

Send backups via email

- Configure the email options if you wish the backup archives to be sent to a specified email address. The backup archives will be sent as email attachments. The log file archives will be excluded from the backup archives.
  - Enabled - Select this check box to receive backup archives through emails
  - Email address of recipient - Email address to which the backup archives are to be sent
  - Email address of sender - Email account from which the emails are to be sent. This can be same as the recipient email
  - Address of smarthost to be used - The IP address of the SMTP server to send the emails
- Click Save for your configuration to take effect.
- To test the email backup operation, click 'Send a backup now'. A backup of the current state of the DFW virtual appliance will be created and sent to the specified email address.

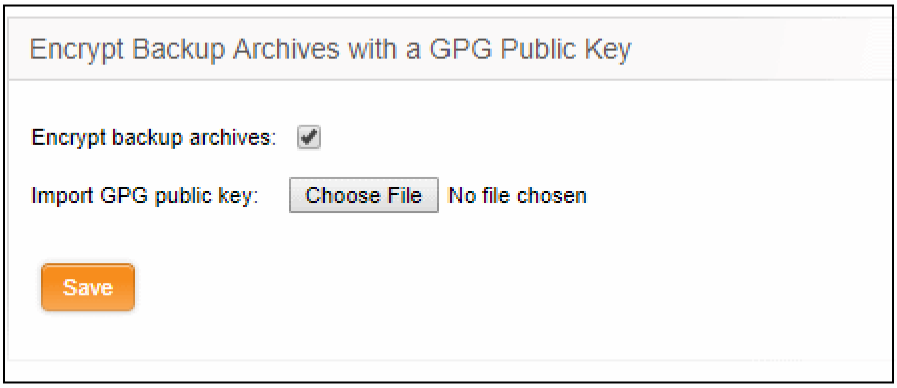
4.9.3 Encrypt Backup Archives

Comodo Dome Firewall can encrypt and store the backup archives created on both manual backup operation and scheduled backups using a GNU Privacy Guard (GPG) public key. The administrator can choose the encrypt the backup archives containing sensitive configurations like passwords.

> Note: Before configuration for backup encryption, ensure that the GPG public certificate is available in the local storage of the computer from which the administrative console is accessed.

To configure backup encryption

- Click 'System' on the left then choose 'Backup'.
- Select the 'Backup' tab.
- Configure the options under 'Encrypt backup archives with a GPG public key'

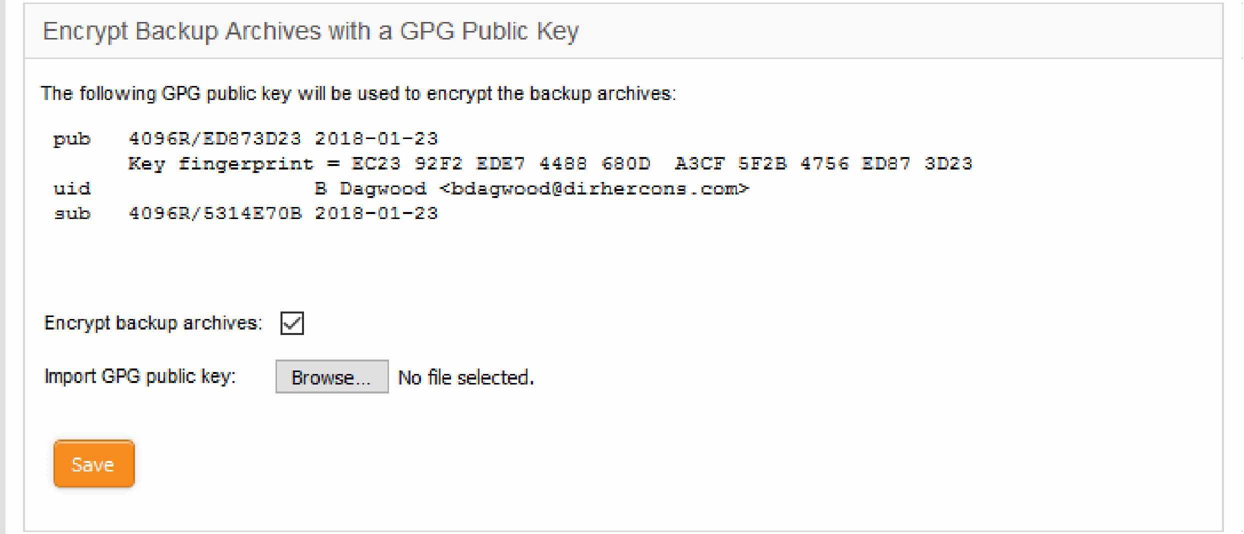


Encrypt Backup Archives with a GPG Public Key

Encrypt backup archives: ☑

Import GPG public key: Choose File No file chosen

- Encrypt backup archives - Select this option to implement encryption on your backup
- Import GPG public key - Click 'Choose File' > navigate to the location of the public key > click 'Open'.



Encrypt Backup Archives with a GPG Public Key

The following GPG public key will be used to encrypt the backup archives:

```
pub   4096R/ED873D23 2018-01-23
      Key fingerprint = EC23 92F2 EDE7 4488 680D  A3CF 5F2B 4756 ED87 3D23
uid                  B Dagwood <bdagwood@dirhercons.com>
sub   4096R/5314E70B 2018-01-23
```

Encrypt backup archives: ☑

Import GPG public key: Browse... No file selected.

The key will be uploaded and displayed.

- Click 'Save' to upload the public key and save the configuration.

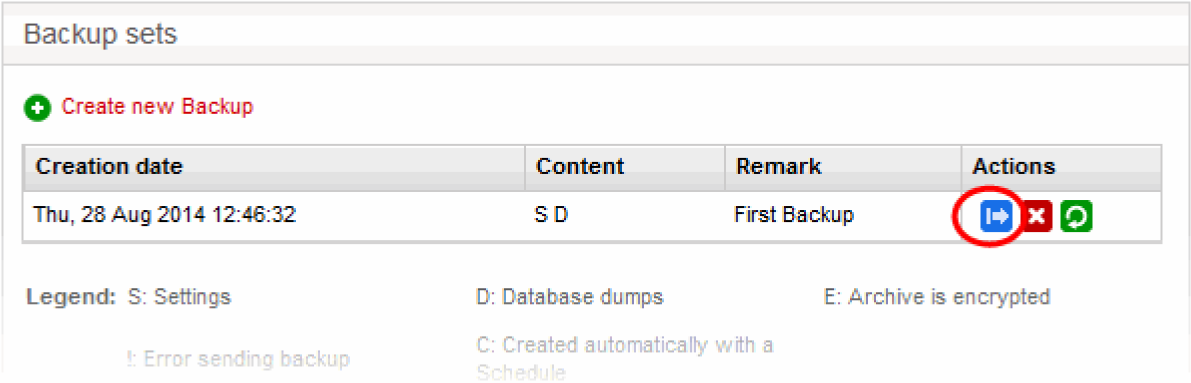
4.9.4 Export a Backup

The backup archives stored in the DFW virtual appliance and the USB drives can be exported and saved in the computer from which the administrative console is accessed. The administrator can store important backup archives with different configurations in a specified workstation, so that the virtual appliance can be restored to the required configuration, even in the case where the backup archives stored in it were accidentally deleted. See '**Importing a Backup**' for more details on importing a backup archive from the computer to the virtual appliance and the section '**Rolling Back the virtual appliance to a PreviousTime Point**' for restoring the virtual appliance using the backup archive.

Note: To store a backup archive from a USB drive in the local workstation, the USB drive should have been plugged-in to the virtual appliance for the archives in it to be listed in the Backup interface.

To export a backup archive

- Open the Backup interface by clicking 'System' > 'Backup' from the left hand side navigation.
- Ensure that the Backup tab is open. The list of available backup archives is displayed with their details and control buttons under Backup sets. If the USB drive containing backup archives is plugged-in to the virtual appliance, the backups stored in it are also displayed.



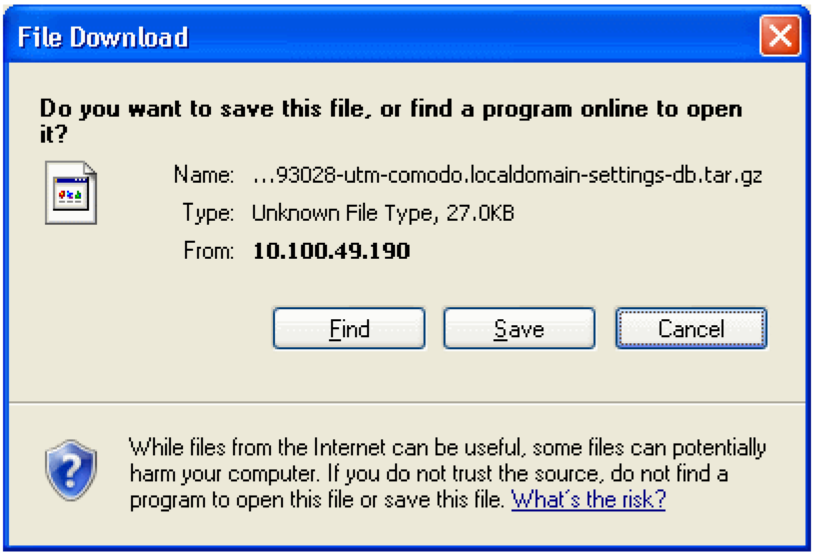
Backup sets

Creation date	Content	Remark	Actions
Thu, 28 Aug 2014 12:46:32	S D	First Backup	

Legend: S: Settings D: Database dumps E: Archive is encrypted

!: Error sending backup C: Created automatically with a Schedule

- Click the Export button ➡ in the row of the required backup archive. The File Download dialog will be displayed.



File Download

Do you want to save this file, or find a program online to open it?

Name: ...93028-utm-comodo.localdomain-settings-db.tar.gz

Type: Unknown File Type, 27.0KB

From: **10.100.49.190**

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

- Click 'Save', navigate to a safe location in your hard drive and click 'Save' in the 'Save As' dialog.

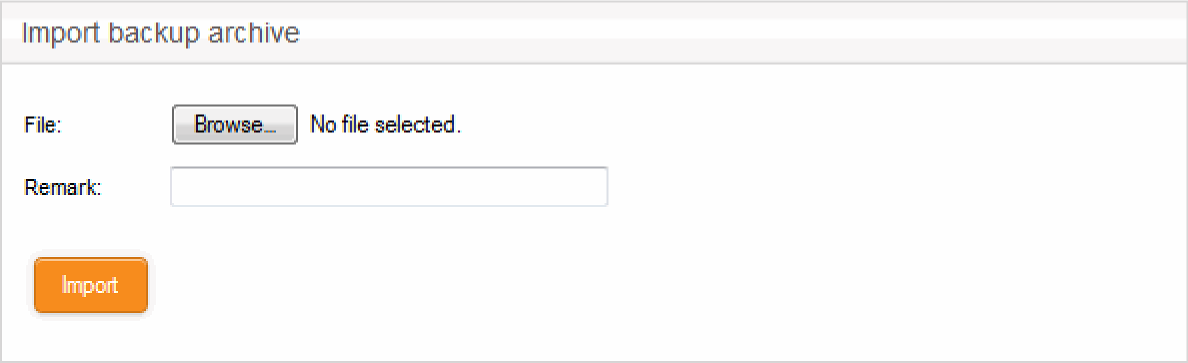
The backup archive will be saved in .tar.gz archive file format with the default file name 'backup-<time stamp>-<hostname of the virtual appliance>-<component1 in backup>-<component 2 in backup>.tar.gz'. The time stamp that indicates the time point at which the backup was created is of the format YYYYMMDDHHMMSS.

4.9.5 Import a Backup Archive from a Local Computer

The exported backup archives, exported from the administrative console and stored in a local computer through which the console is accessed, can be imported into the console for rolling back the virtual appliance to the respective time point. See **Exporting a backup** for more details on storing a backup archive from the console to the local computer.

To import a backup archive

- Login to the Comodo Dome Firewall administrative interface from the computer in which the backup is stored
- Open the Backup interface by clicking 'System' > 'Backup' from the left hand side navigation.
- Ensure that the Backup tab is open.



Import backup archive

File: No file selected.

Remark:

- Click 'Browse' next to File under 'Import backup archive', navigate to the location where the backup is stored, select the backup and click 'Open' in the 'Choose file to Upload' dialog.
- Enter a short description or remark for the imported backup in the 'Remark' text box. This description will appear in the 'Remark' column in the list of backup archives.

- Click 'Import' to save the backup archive in the virtual appliance.

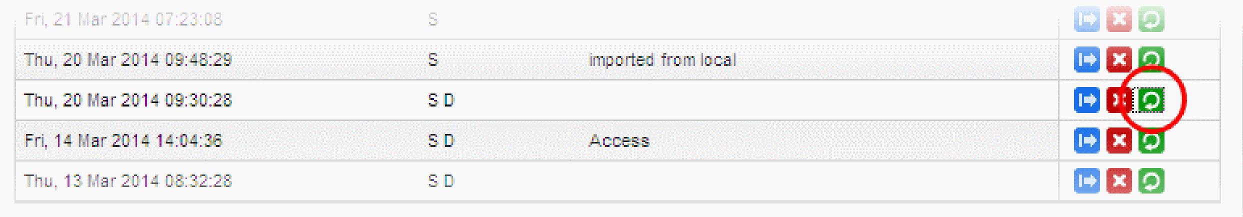
On completion of import operation, the backup archive will be added to the list of backup archives under Backup Sets and will be available for restoring and rolling back the virtual appliance to the respective time point. See **Rolling Back the virtual appliance to a Previous Time Point** for more details on this.

4.9.6 Roll Back the Virtual Appliance to a Previous Time Point

The backup archives enable the administrator to rollback the state of the virtual appliance to any of the previous time point in case of any malfunction or wrong settings made. Restoring a backup from the Backup interface automatically applies the configuration contained it and restarts the virtual appliance to roll back the virtual appliance to the respective time point.

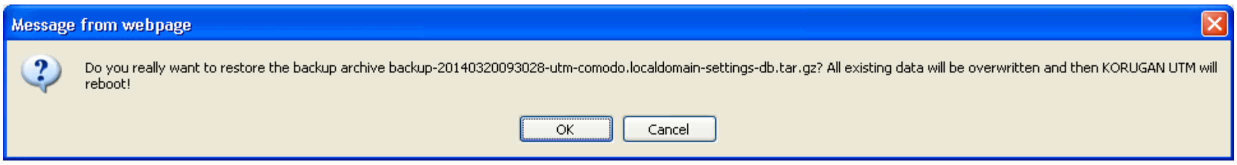
To restore a backup

- Open the Backup interface by clicking 'System' > 'Backup' from the left hand side navigation.
- Ensure that the Backup tab is open. The list of available backup archives is displayed with their details and control buttons under Backup sets. If the USB drive containing backup archives is plugged-in to the virtual appliance, the backups stored in it are also displayed.



Fri, 21 Mar 2014 07:23:08	S		
Thu, 20 Mar 2014 09:48:29	S	imported from local	
Thu, 20 Mar 2014 09:30:28	S D		
Fri, 14 Mar 2014 14:04:36	S D	Access	
Thu, 13 Mar 2014 08:32:28	S D		

- Click the 'Restore' button in the row of the required backup archive. A Confirmation dialog will appear.



Message from webpage

Do you really want to restore the backup archive backup-20140320093028-utm-comodo.localdomain-settings-db.tar.gz? All existing data will be overwritten and then KORUGAN UTM will reboot!

- Click OK in the confirmation dialog.

Comodo Dome Firewall will be applied with the configurations as contained in the selected backup and the database dumps and log files will be replaced with those in the backup and the DFW will restart with the state at the time point at which the backup was created.

4.9.7 Reset the Virtual Appliance to Factory Defaults

If the administrator wants to clear all the configuration data, database dumps and the logs or in case of any abnormality in operation due to wrong configuration settings, the DFW virtual appliance can be reset to factory settings and rolled back to a state it which it was newly purchased.

Resetting the virtual appliance clears all the configuration data and the stored passwords and restores the default credentials. The administrator needs to reconfigure the administrative console login credentials, network connections and so on from the scratch.

> **Note**: As a fail-safe measure, the virtual appliance creates a backup of the current state before resetting to factory defaults.

To reset the virtual appliance

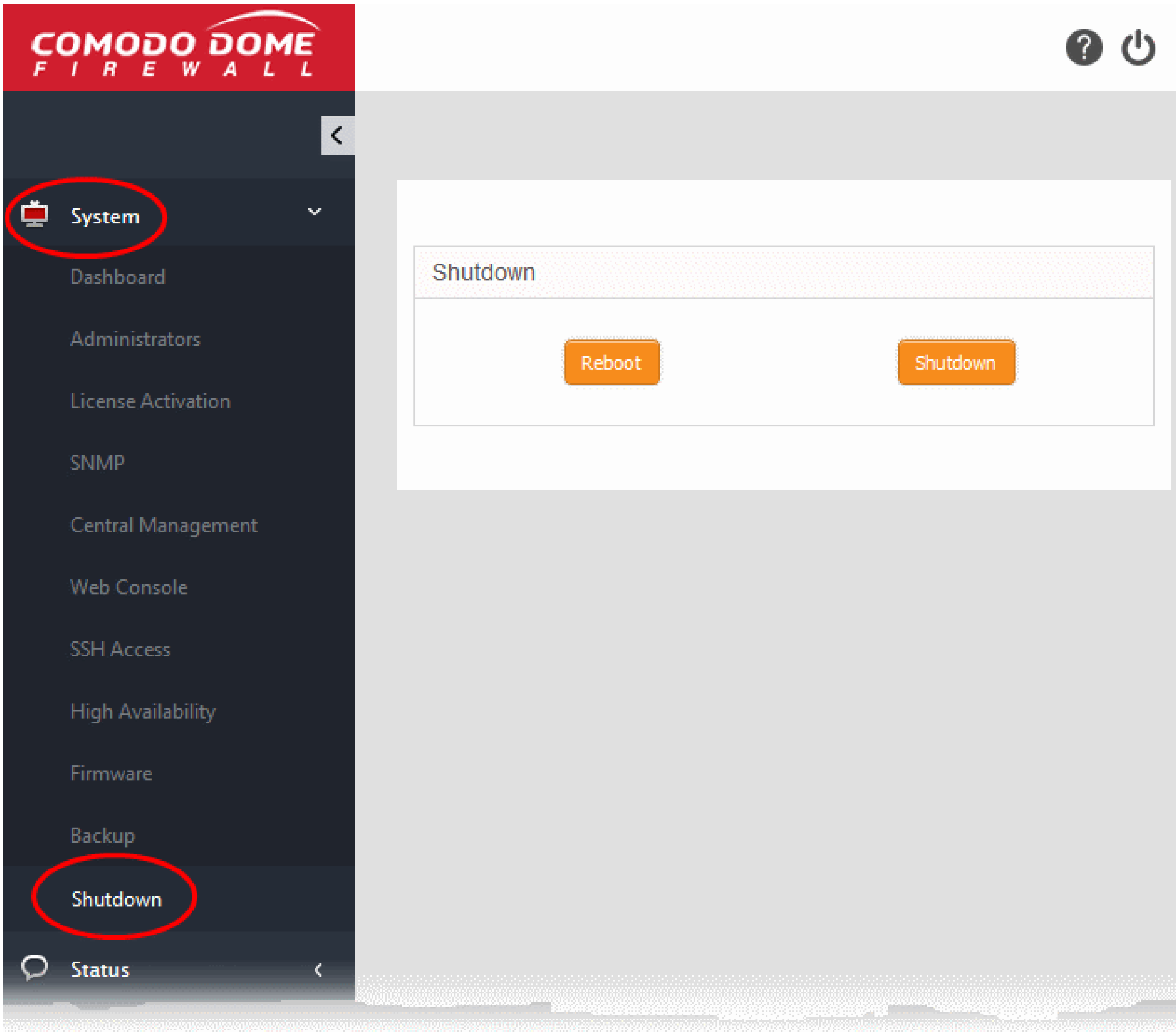
- Open the Backup interface by clicking 'System' > 'Backup' from the left hand side navigation.
- Ensure that the Backup tab is open.

- Click the Factory defaults button under 'Reset configuration to factory defaults and reboot'. A confirmation dialog will appear.
- Click OK in the dialog. The virtual appliance will be reset and restarted with the default factory settings.

4.10 Shutdown or Restart the Dome Firewall Virtual Appliance

- Click 'System' on the left then select 'Shutdown'.

You can shutdown or reboot the virtual appliance for various reasons like the UPS power going low or the operation of the device going unstable.



Shutdown

- Click 'Shutdown' to shutdown the virtual appliance.

Caution: The virtual appliance will be shutdown immediately without any confirmation dialog. You can only shutdown the virtual appliance from the web console, but cannot start the virtual appliance from the console. You can switch on the virtual appliance from the Virtual Box.

Restart

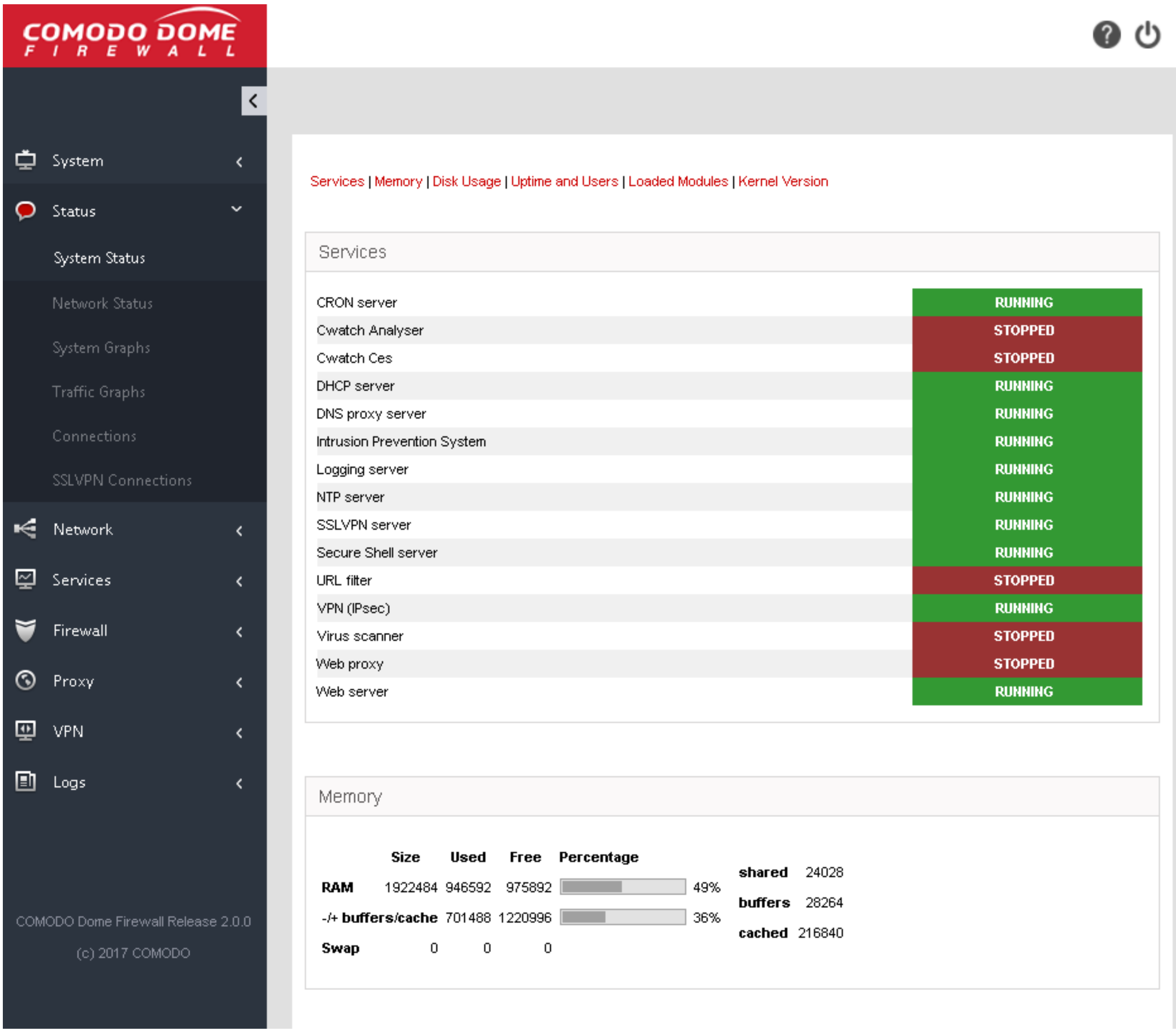
- Click 'Reboot'.to restart the virtual appliance.

The virtual appliance will start rebooting immediately. After the restart, the virtual appliance will automatically connect to the administrative console and can be accessed without the need to login again.

Shutdown and reboot activities are logged. Logs include date, time, type of event, subject id, component name and outcome of the event.

5 Viewing DFW Virtual Appliance Status

- Click 'Status' in the left-hand menu to view all available status modules.
- The 'Status' modules show important data about firewall and network components, providing admins with a comprehensive overview of their network's performance, security and overall health.



Services

CRON server	RUNNING
Cwatch Analyser	STOPPED
Cwatch Ces	STOPPED
DHCP server	RUNNING
DNS proxy server	RUNNING
Intrusion Prevention System	RUNNING
Logging server	RUNNING
NTP server	RUNNING
SSLVPN server	RUNNING
Secure Shell server	RUNNING
URL filter	STOPPED
VPN (IPsec)	RUNNING
Virus scanner	STOPPED
Web proxy	STOPPED
Web server	RUNNING

Memory

	Size	Used	Free	Percentage	
RAM	1922484	946592	975892	49%	
-/+ buffers/cache		701488	1220996	36%	
Swap	0	0	0		

shared	24028
buffers	28264
cached	216840

- **System Status** - Statistics about the current running state of the firewall. This includes running services, memory and disk use, active modules, uptime and user access. See **System Status** for more details.
- **Network Status** - Details about active network interfaces. See **Network Status** for more details.
- **System Graphs** - Real-time resource usage data, including CPU, physical memory, disk space and more. See **System Usage Summaries** for more details.
- **Traffic Graphs** - Real-time data on traffic passing through each network zone type. Types include LAN, internet, WiFi and DMZ. See **Network Traffic** for more details.

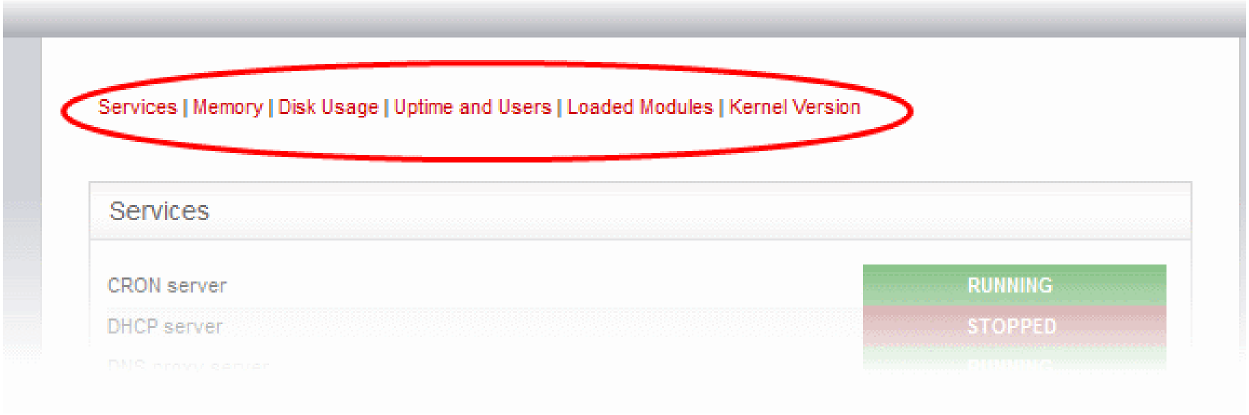
- **Connections** - Shows connections to, from and through the DFW virtual appliance. Includes connection source, destination, protocol and status. See **Network Connections** for more details.
- **SSL VPN Connections** - Shows users that have connected via SSL VPN and currently running VPN services. See **SSL VPN Connections** for more details.

5.1 System Status

System status contains the following items:

- **Services** - Services which are currently loaded and their running status
- **Memory** - System memory usage
- **Disk Usage** - Hard disk usage
- **Uptime and Users** - Shows how long Dome FW has been running since the last restart, and which users are currently logged-on to the system.
- **Loaded Modules** - Shows kernel modules currently loaded into memory
- **Kernel Version** - Shows current kernel version number

You can navigate between sections by using the links at the top of the screen:

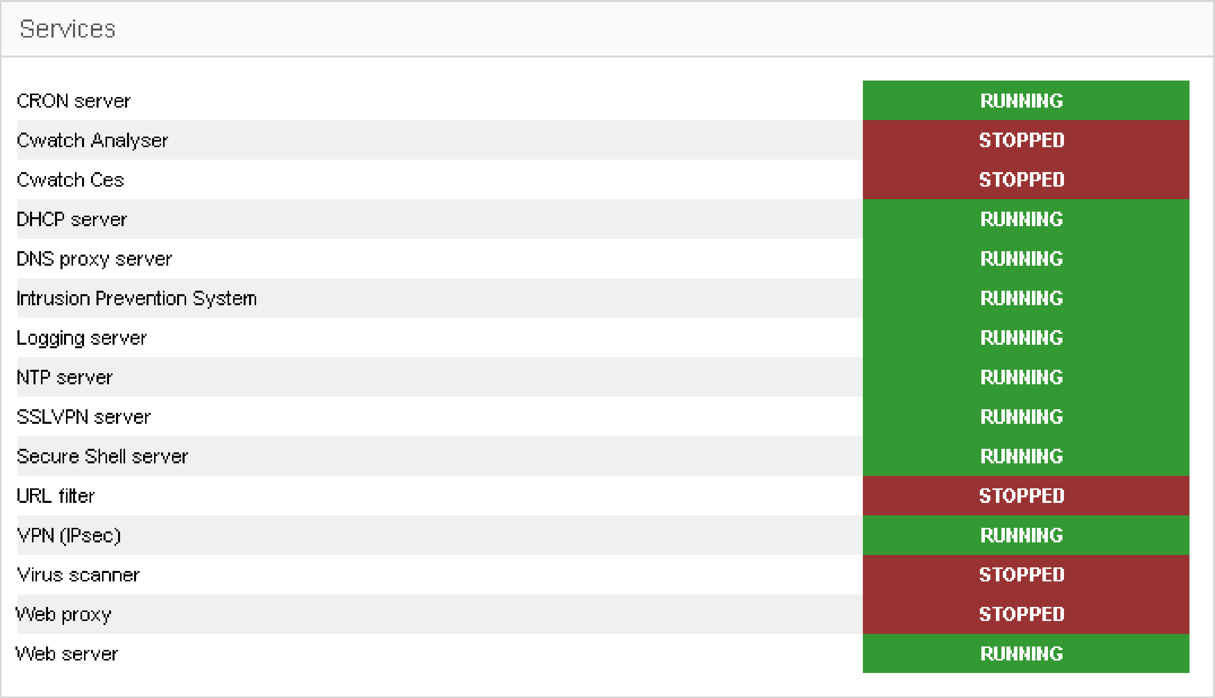

Services | Memory | Disk Usage | Uptime and Users | Loaded Modules | Kernel Version

Services

CRON server RUNNING
DHCP server STOPPED

Services

The 'Services' pane shows a list of services that are currently loaded to the DFW virtual appliance and whether they are running or stopped. A service may be stopped if the corresponding daemon or script is not enabled.

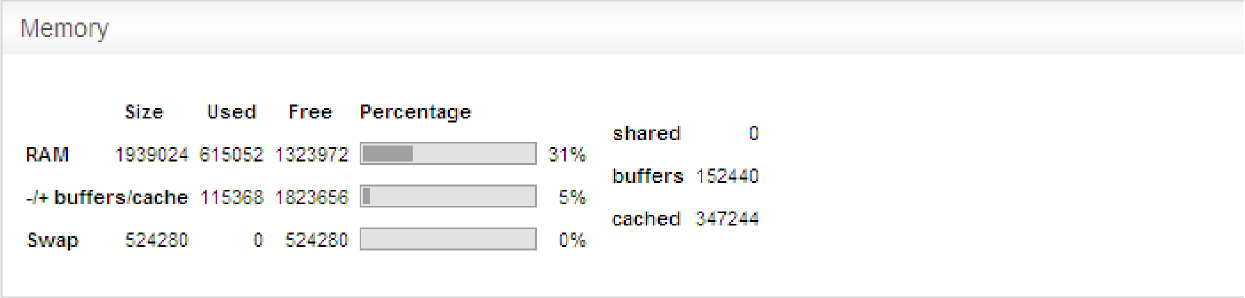


Services

CRON server	RUNNING
Cwatch Analyser	STOPPED
Cwatch Ces	STOPPED
DHCP server	RUNNING
DNS proxy server	RUNNING
Intrusion Prevention System	RUNNING
Logging server	RUNNING
NTP server	RUNNING
SSLVPN server	RUNNING
Secure Shell server	RUNNING
URL filter	STOPPED
VPN (IPsec)	RUNNING
Virus scanner	STOPPED
Web proxy	STOPPED
Web server	RUNNING

Memory

The memory pane shows the usage status of the physical memory in the virtual appliance.



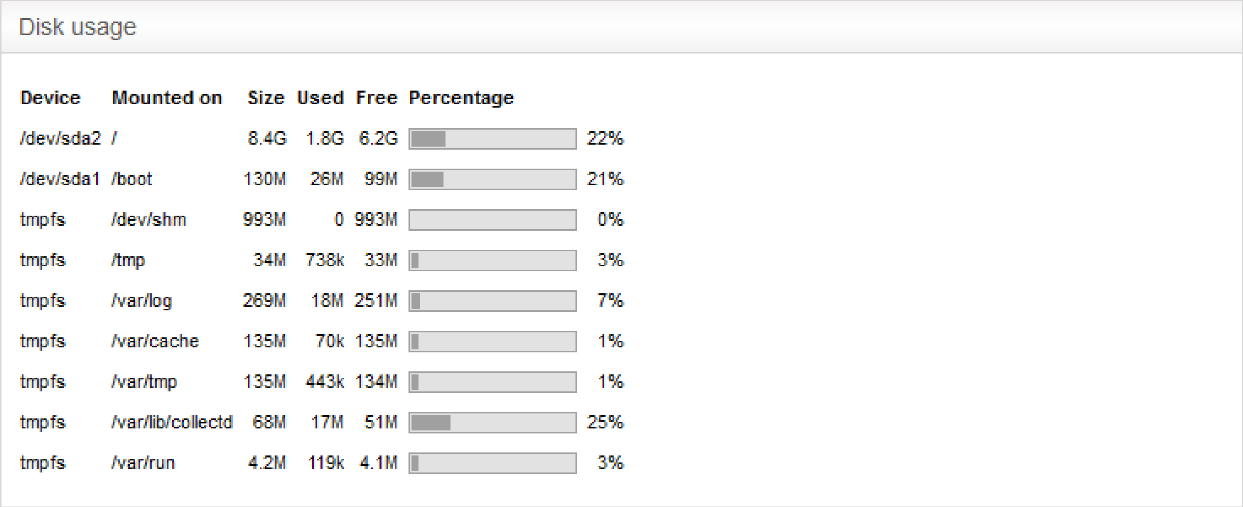
Memory

	Size	Used	Free	Percentage			
RAM	1939024	615052	1323972	31%		shared	0
-/+ buffers/cache		115368	1823656	5%		buffers	152440
Swap	524280	0	524280	0%		cached	347244

Memory Usage - Row Descriptions	
Row	**Description**
RAM	Shows the total RAM size, used memory size, free available memory size in KB and a bar indicating in the memory usage in percentage. It can be close to 100% if the virtual appliance is running for long time since the Linux kernel uses all available RAM as disk cache to speed up I/O operations.
=/- buffers/cache	Shows the size of memory actually used by currently running processes. The memory used by processes should not exceed 80% of the total memory, otherwise, the active processes will be swapped to disk, which will reduce the performance of the system. If the memory usage exceeds the threshold for long periods of time RAM should be added to maintain the system performances.
Swap	Shows the memory dedicated for swapping services/processes and its usage status. The average swap usage will be below 20%, if not all the services are used all the time.

Disk usage

The 'Disk Usage' pane shows the hard disk drives/ partitions mounted on the virtual appliance, their mount point and the space of each disk partition similar to the output of Linux Disk Free (df) command.



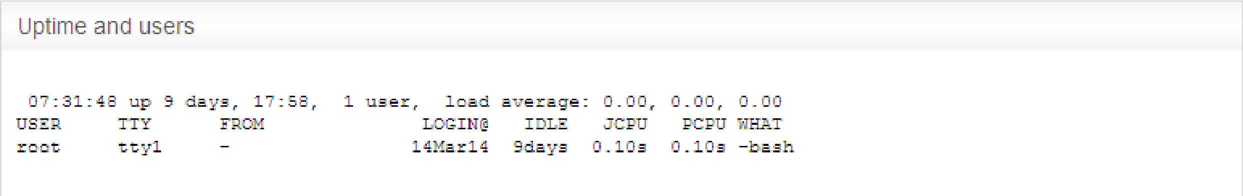
Disk usage

Device	Mounted on	Size	Used	Free	Percentage
/dev/sda2	/	8.4G	1.8G	6.2G	22%
/dev/sda1	/boot	130M	26M	99M	21%
tmpfs	/dev/shm	993M	0	993M	0%
tmpfs	/tmp	34M	738k	33M	3%
tmpfs	/var/log	269M	18M	251M	7%
tmpfs	/var/cache	135M	70k	135M	1%
tmpfs	/var/tmp	135M	443k	134M	1%
tmpfs	/var/lib/collectd	68M	17M	51M	25%
tmpfs	/var/run	4.2M	119k	4.1M	3%

Disk Usage - Column Descriptions	
Column	**Description**
Device	The disk device or partition for various DFW modules. Examples: • The main disk (/dev/sda1). • The boot disk (/dev/sda1 /boot) • The data disk (/dev/mapper/local-var). • The temporary file system (/tmp) • the log partition (/var/log).
Mounted on	The mount point of the partition.
Size	The total size of the partition.
Used	Used space in the disk
Free	Free Space in the disk
Percentage	The usage of the disk space in percentage The used space in partitions that store the data and the logs grow over time. It is recommended to ensure that their usage does not exceed 95% to maintain the efficiency of the system.

Uptime and users

The 'Uptime and Users' pane indicate the period for which the DFW virtual appliance is continuously running from the last boot time and the list of users that are currently logged-in.



Uptime and users

```
 07:31:48 up 9 days, 17:58,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     -                14Mar14  9days  0.10s  0.10s -bash
```

The first line displays the following items in order:

- Current time
- The period for which the DFW virtual appliance is up and running from the last boot time

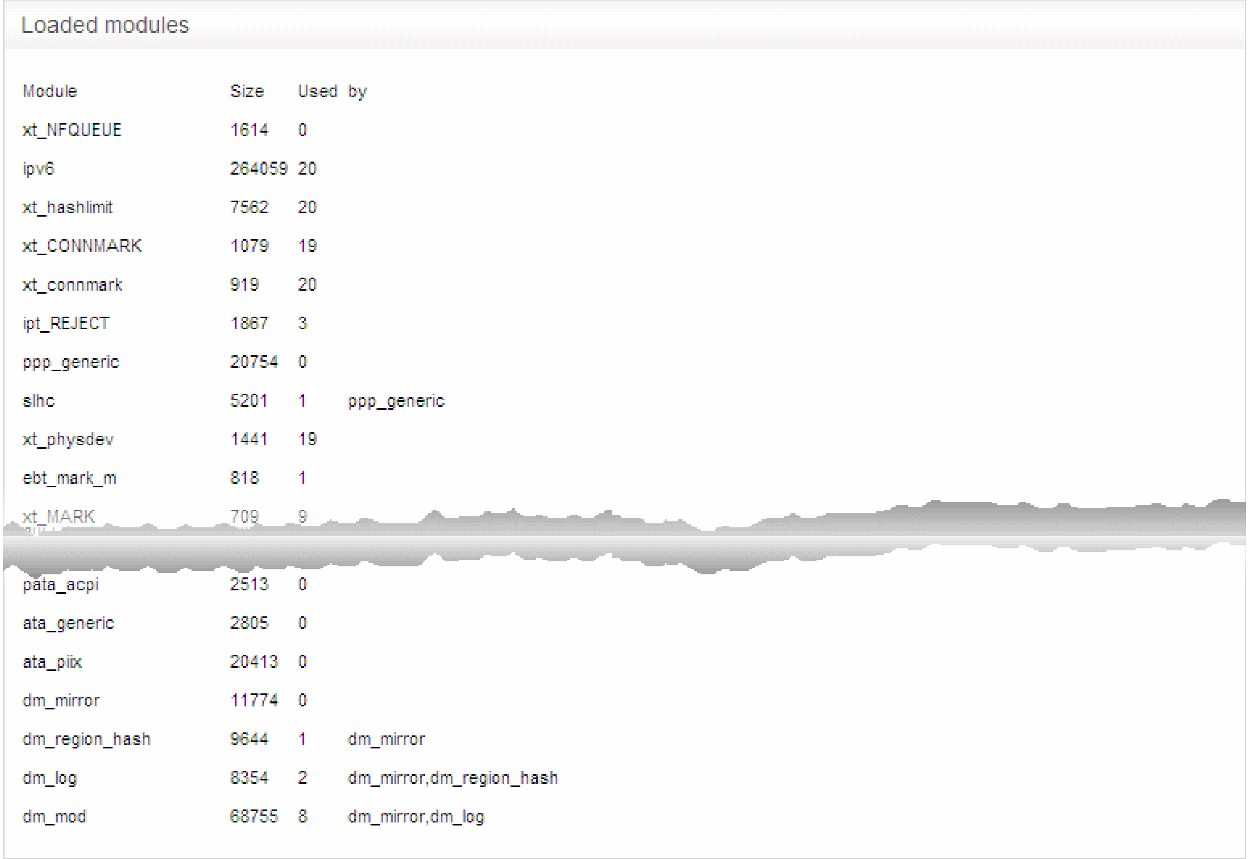
- The number of users currently logged into the system
- The average load on the system for the past 1, 5 and 15 minutes.

Following the first line, a table displays the details of the currently logged-in users.

Users - Column Descriptions	
Column	**Description**
USER	The username/type
TTY	The name of the terminal from which the user is connected
FROM	The remote host name from which the user is connected
LOGIN@	The date and time at which the user logged-in to the system, for the current session
IDLE	The period for which the user is idle
JCPU	The time spent by the processes initiated by the terminal through which the used has connected to the system, excluding the past background jobs. However, it includes the background jobs that are currently running.
PCPU	The time spent by the currently running processes, initiated by the actions listed under 'What' column.
WHAT	Shows what the user is doing.

Loaded modules

The 'Loaded Modules' pane displays the Kernel modules that are currently loaded to the system.



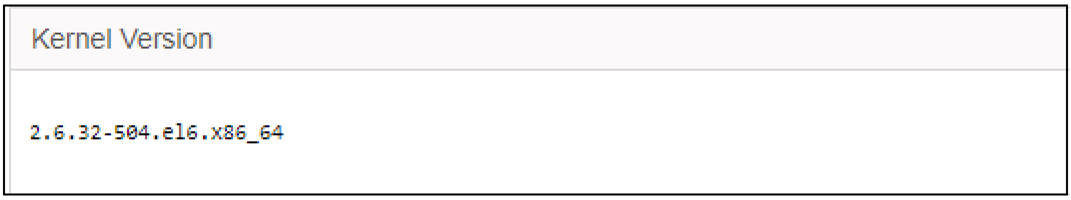
Loaded modules

Module	Size	Used	by
xt_NFQUEUE	1614	0	
ipv6	264059	20	
xt_hashlimit	7562	20	
xt_CONNMARK	1079	19	
xt_connmark	919	20	
ipt_REJECT	1867	3	
ppp_generic	20754	0	
slhc	5201	1	ppp_generic
xt_physdev	1441	19	
ebt_mark_m	818	1	
xt_MARK	709	9	
pata_acpi	2513	0	
ata_generic	2805	0	
ata_piix	20413	0	
dm_mirror	11774	0	
dm_region_hash	9644	1	dm_mirror
dm_log	8354	2	dm_mirror,dm_region_hash
dm_mod	68755	8	dm_mirror,dm_log

Loaded Modules - Column Descriptions	
Column	**Description**
Module	The name of the module
Size	Size of the module
Used by	Number of times the module is used and the parent modules that referred this module

Kernel version

The Kernel version pane displays the version number of the kernel currently used.

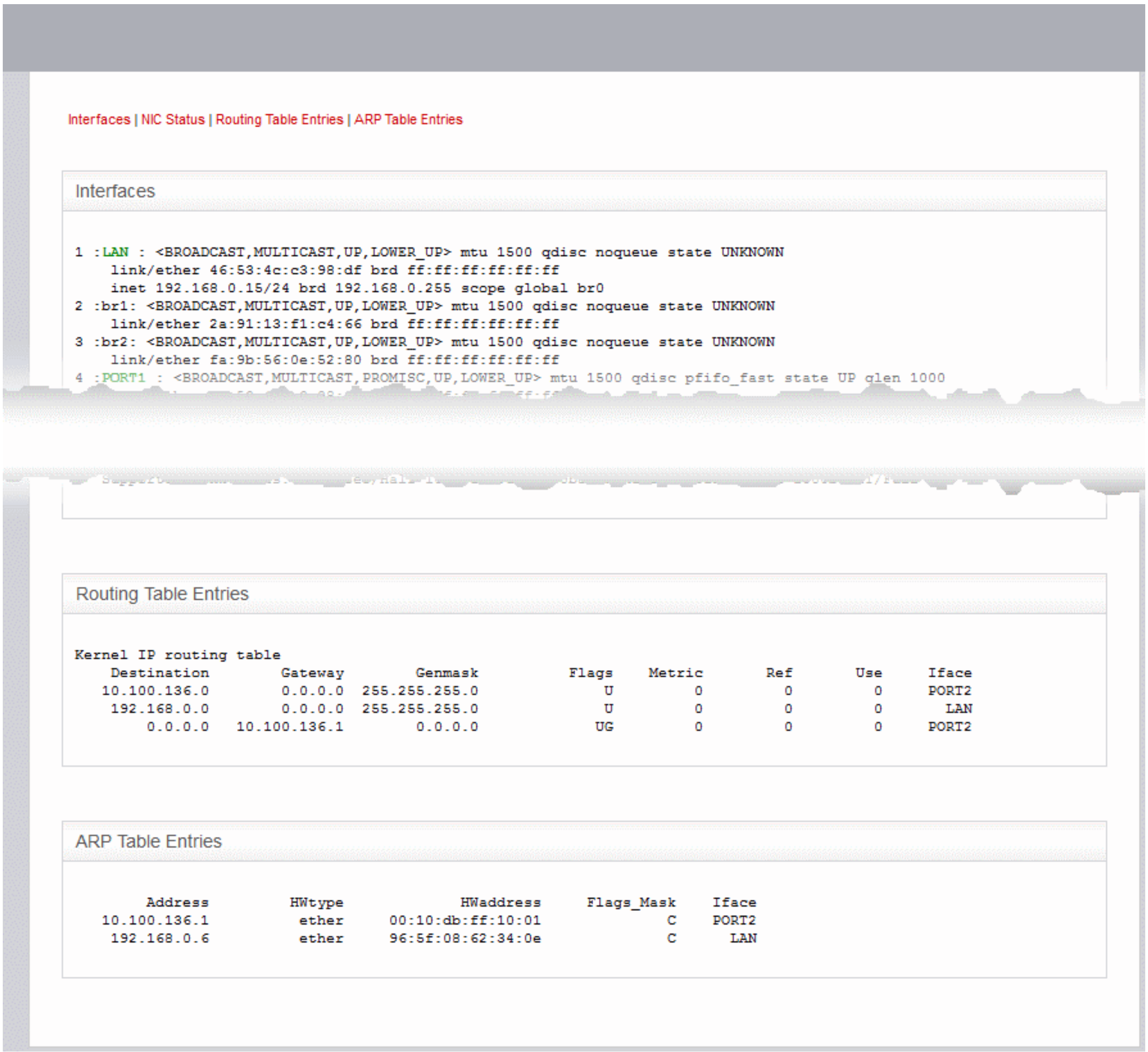


Kernel Version

```
2.6.32-504.el6.x86_64
```

5.2 Network Status

The Network Status screen displays real-time logs containing status information about components like connected Network Interfaces, Network Interface Controllers (NICs), routing table entries and address Resolution Protocol (ARP).



Interfaces | NIC Status | Routing Table Entries | ARP Table Entries

Interfaces

```
1 :LAN : <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 46:53:4c:c3:98:df brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.15/24 brd 192.168.0.255 scope global br0
2 :br1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 2a:91:13:f1:c4:66 brd ff:ff:ff:ff:ff:ff
3 :br2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether fa:9b:56:0e:52:80 brd ff:ff:ff:ff:ff:ff
4 :PORT1 : <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
```

Routing Table Entries

```
Kernel IP routing table
    Destination         Gateway         Genmask          Flags   Metric      Ref      Use    Iface
   10.100.136.0         0.0.0.0   255.255.255.0              U        0        0        0    PORT2
    192.168.0.0         0.0.0.0   255.255.255.0              U        0        0        0      LAN
        0.0.0.0    10.100.136.1         0.0.0.0             UG        0        0        0    PORT2
```

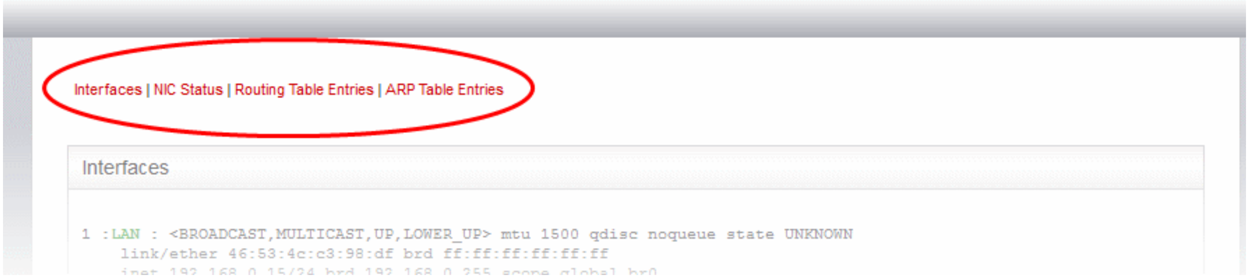
ARP Table Entries

```
        Address          HWtype            HWaddress      Flags_Mask    Iface
   10.100.136.1           ether    00:10:db:ff:10:01               C    PORT2
    192.168.0.6           ether    96:5f:08:62:34:0e               C      LAN
```

The screen displays the following information panes one below the other:

- **Interfaces**
- **NIC Status**
- **Routing Table Entries**
- **ARP Entries**

Administrators can navigate to the required pane by clicking the shortcut links at the top of the screen.



Interfaces | NIC Status | Routing Table Entries | ARP Table Entries

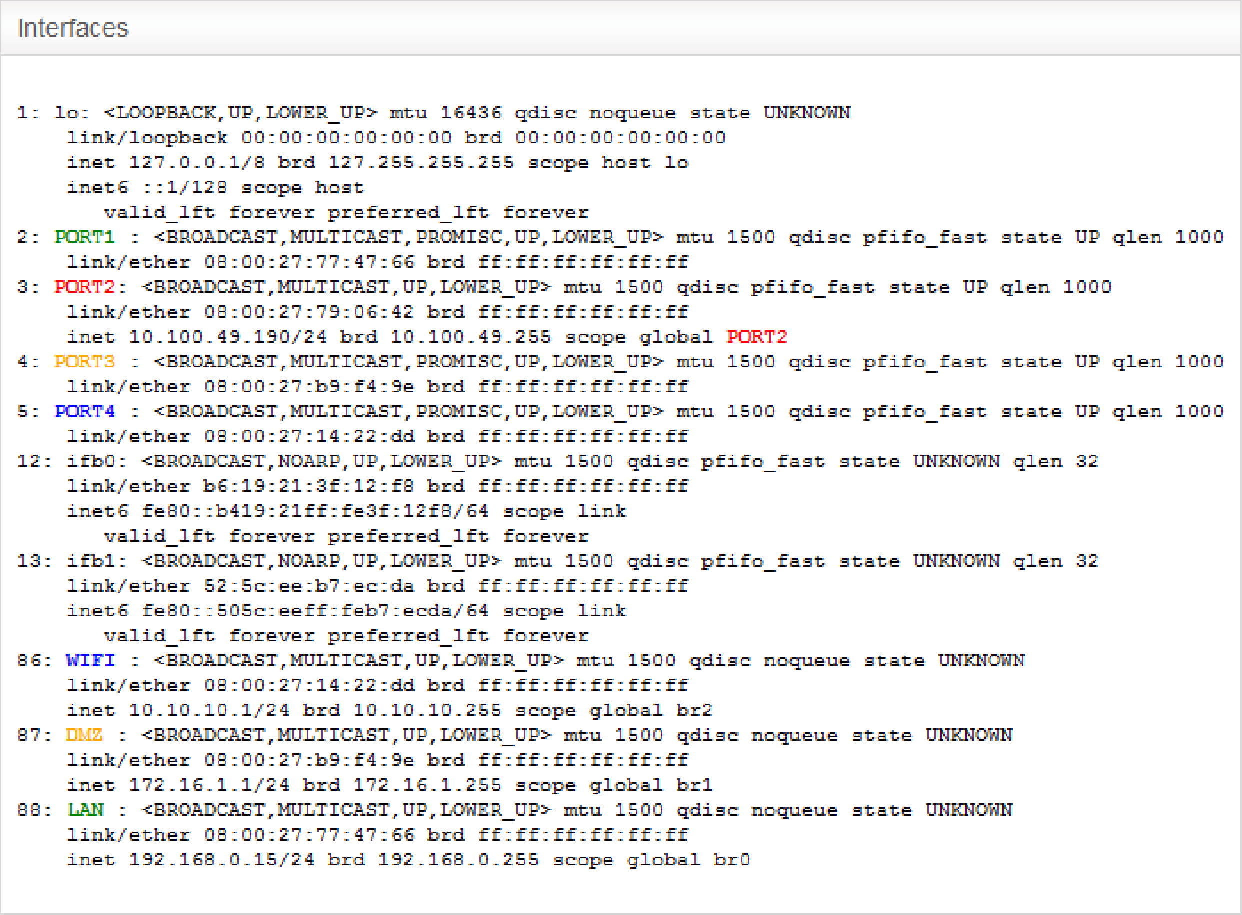
Interfaces

```
1 :LAN : <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 46:53:4c:c3:98:df brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.15/24 brd 192.168.0.255 scope global br0
```

Interfaces

The 'Interfaces' pane displays a list of all network interfaces connected to the virtual appliance along with their associated MAC address, IP address, and additional communication parameters. Example connected interfaces can include Ethernet interfaces, bridges or virtual devices. The interfaces that are active are indicated by colors, corresponding to the network zones that that serve:

- Red - External network zone like WAN connected to internet
- Yellow - DMZ zone
- Green - Internal network like Local Area Network (LAN)
- Blue - Wi-Fi zone

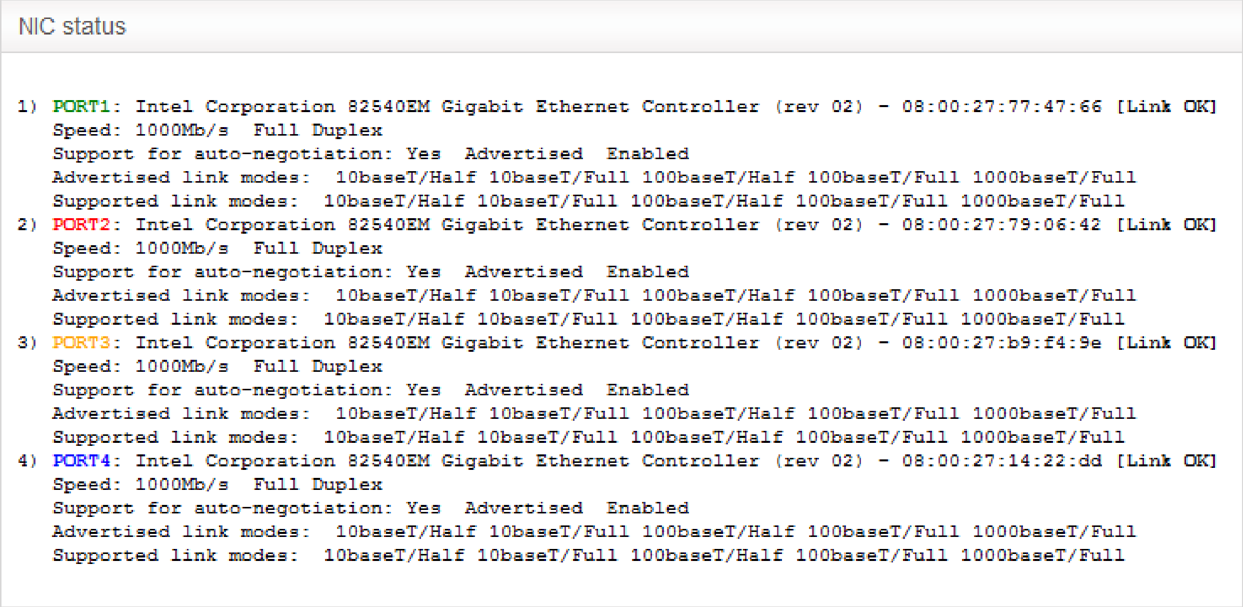


Interfaces

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: PORT1 : <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:77:47:66 brd ff:ff:ff:ff:ff:ff
3: PORT2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:79:06:42 brd ff:ff:ff:ff:ff:ff
    inet 10.100.49.190/24 brd 10.100.49.255 scope global PORT2
4: PORT3 : <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:b9:f4:9e brd ff:ff:ff:ff:ff:ff
5: PORT4 : <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:14:22:dd brd ff:ff:ff:ff:ff:ff
12: ifb0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 32
    link/ether b6:19:21:3f:12:f8 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::b419:21ff:fe3f:12f8/64 scope link
       valid_lft forever preferred_lft forever
13: ifb1: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 32
    link/ether 52:5c:ee:b7:ec:da brd ff:ff:ff:ff:ff:ff
    inet6 fe80::505c:eeff:feb7:ecda/64 scope link
       valid_lft forever preferred_lft forever
86: WIFI : <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 08:00:27:14:22:dd brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.1/24 brd 10.10.10.255 scope global br2
87: DMZ : <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 08:00:27:b9:f4:9e brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.1/24 brd 172.16.1.255 scope global br1
88: LAN : <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 08:00:27:77:47:66 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.15/24 brd 192.168.0.255 scope global br0
```

NIC Status

The 'NIC status' pane displays Network Interface Controllers (NICs) connected to the virtual appliance along with their current configuration and capabilities.

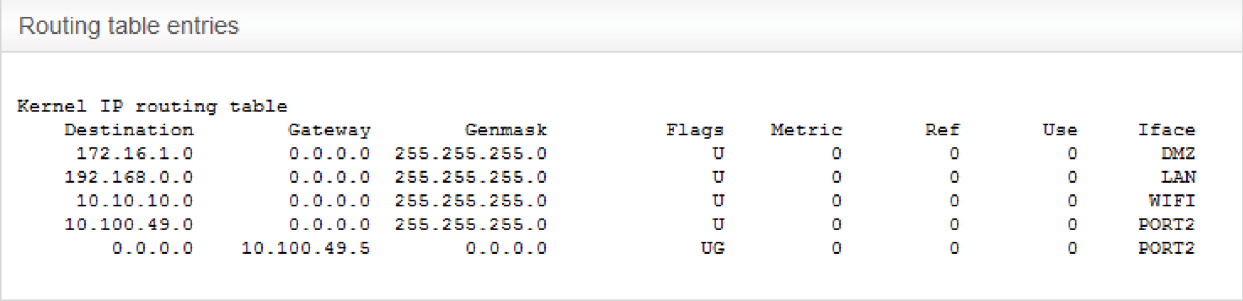


NIC status

```
1) PORT1: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02) - 08:00:27:77:47:66 [Link OK]
   Speed: 1000Mb/s  Full Duplex
   Support for auto-negotiation: Yes  Advertised  Enabled
   Advertised link modes:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
   Supported link modes:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
2) PORT2: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02) - 08:00:27:79:06:42 [Link OK]
   Speed: 1000Mb/s  Full Duplex
   Support for auto-negotiation: Yes  Advertised  Enabled
   Advertised link modes:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
   Supported link modes:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
3) PORT3: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02) - 08:00:27:b9:f4:9e [Link OK]
   Speed: 1000Mb/s  Full Duplex
   Support for auto-negotiation: Yes  Advertised  Enabled
   Advertised link modes:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
   Supported link modes:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
4) PORT4: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02) - 08:00:27:14:22:dd [Link OK]
   Speed: 1000Mb/s  Full Duplex
   Support for auto-negotiation: Yes  Advertised  Enabled
   Advertised link modes:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
   Supported link modes:  10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
```

Routing Table Entries

The Routing Table Entries pane displays a list of routes configured for the network interfaces. Each line shows the traffic route within the corresponding network zones for the interface shown in the last column.



Routing table entries

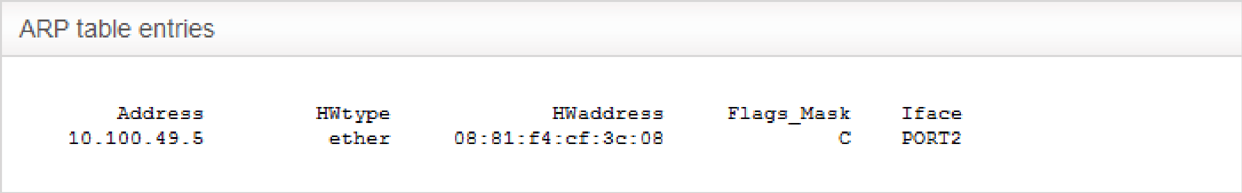
```
Kernel IP routing table
    Destination        Gateway        Genmask           Flags    Metric       Ref       Use     Iface
     172.16.1.0        0.0.0.0  255.255.255.0               U         0         0         0       DMZ
    192.168.0.0        0.0.0.0  255.255.255.0               U         0         0         0       LAN
     10.10.10.0        0.0.0.0  255.255.255.0               U         0         0         0      WIFI
    10.100.49.0        0.0.0.0  255.255.255.0               U         0         0         0     PORT2
        0.0.0.0    10.100.49.5        0.0.0.0              UG         0         0         0     PORT2
```

Routing Tables Entries - Column Descriptions	
Column	**Description**
Destination	The destination network or the host
Gateway	The gateway address. ('*' if none is set)
Genmask	The network mask of the destination network. The possible values are: • 255.255.255.255 for a host destination. • 0.0.0.0 for the default route.
Flags	Displays the flags indicating the status. The possible values are: • U - The route is up and operational. • H - The route is to a specific host (not to a network). • G - The route uses an external gateway • R - The route was installed by a dynamic routing protocol running in the system, using the *reinstate* option • D - The route was dynamically installed by daemon or redirect

	• M - Modified by routing daemon or redirect • A - The route is a cached one, and has an associated entry in the ARP table • C - The route was from a Kernel routing cache • L - The route is a local route • B - The destination of the route is a broadcast address • I - The route has a loopback interface • ! - The route will be rejected
Metric	Indicates the distance to the target (in hops).
Ref	Indicates the references made to this route
Use	The number of lookups made for this route
Iface	The network interface to which the packets are to be sent.

ARP Entries

The 'Address Resolution Protocol' (ARP) table shows a list of the physical (MAC) addresses which are associated with IP addresses in the local network.



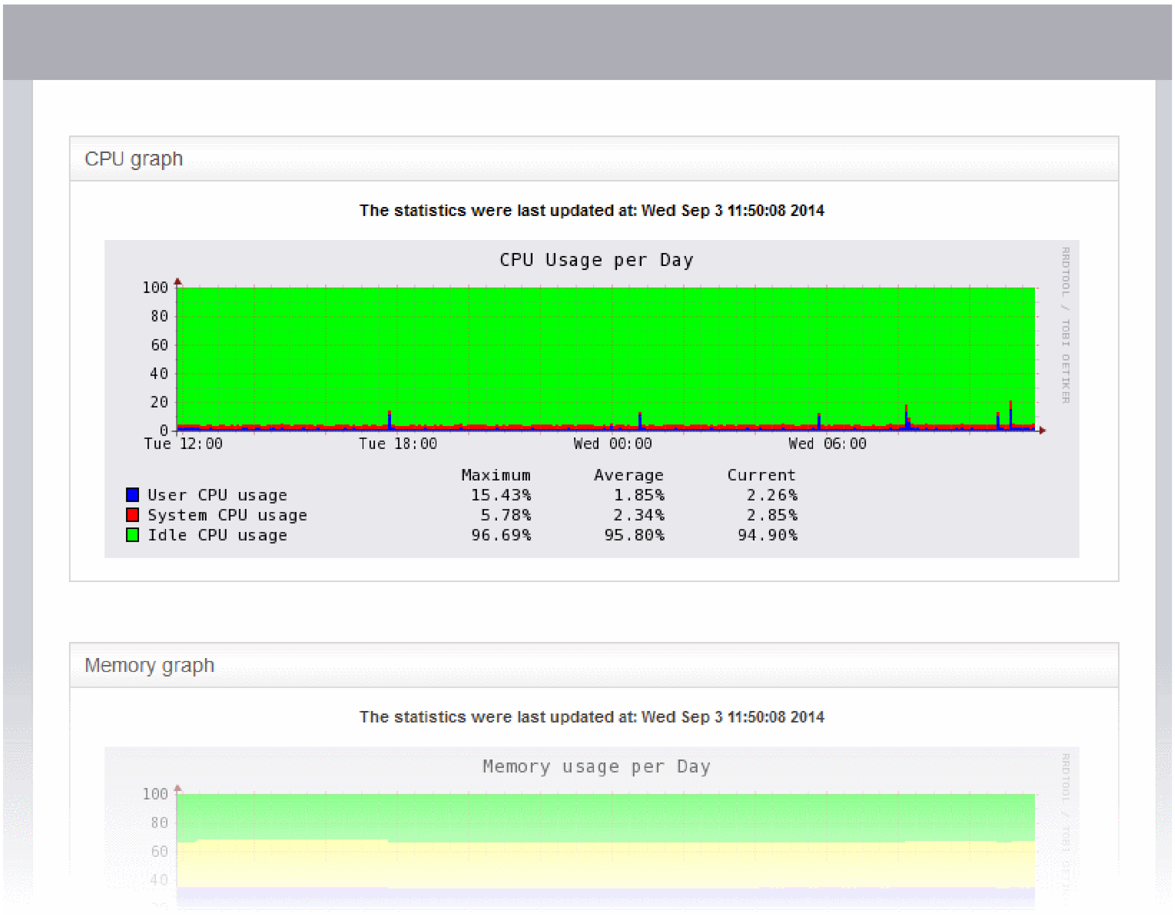
ARP table entries

```
     Address          HWtype          HWaddress     Flags_Mask     Iface
 10.100.49.5           ether  08:81:f4:cf:3c:08              C     PORT2
```

ARP Entries - Column Descriptions	
Column	**Description**
Address	The IP address of the host destination network or the host or other hardware device
HWtype	The type of the hardware device
HWaddress	The MAC address of the hardware device
Flags_Mask	Displays the flags indicating the status of the device. The possible values are: • C - Complete • P - Published • M - Permanent
Iface	The interface to which the packets are to be sent.

5.3 System Usage Summaries

The System Graphs screen displays the usage history of system resources such as CPU, system memory, swap memory and disk drives for the past 24 hours.



CPU graph

The statistics were last updated at: Wed Sep 3 11:50:08 2014

```
                      Maximum     Average     Current
■ User CPU usage       15.43%       1.85%       2.26%
■ System CPU usage      5.78%       2.34%       2.85%
■ Idle CPU usage       96.69%      95.80%      94.90%
```

Memory graph

The statistics were last updated at: Wed Sep 3 11:50:08 2014

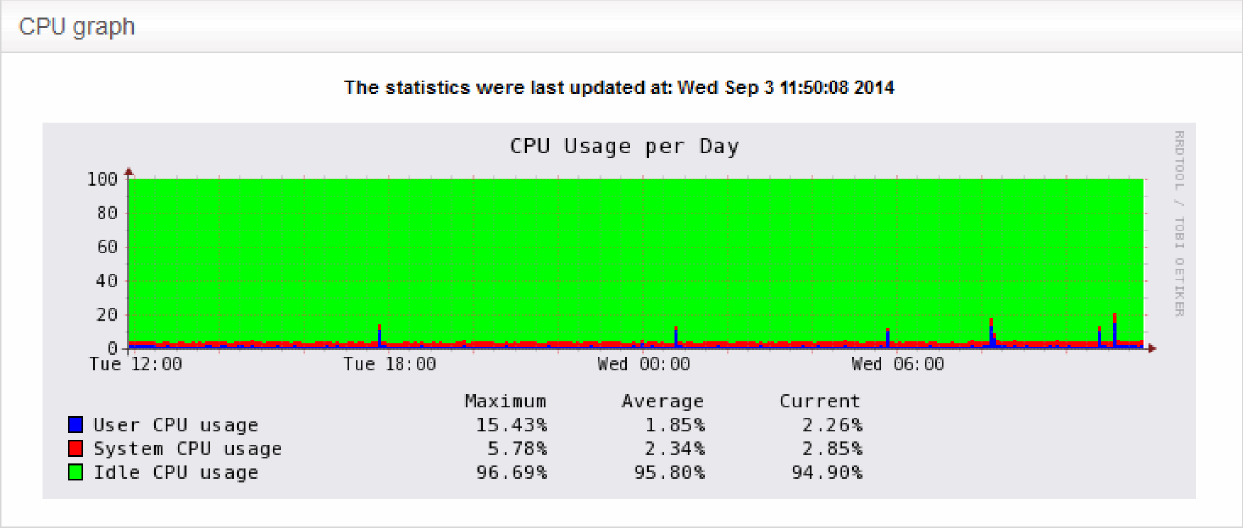
Clicking any graph will open more detailed graphs for that component showing usage history for the past day, week, month and year.

- CPU Graph
- Memory Graph
- Swap Graph
- Disk Graph

CPU Graph

The CPU Graph displays the load on the virtual appliance CPU over the past 24 hours. Processes are indicated with different colors.

- Green - Idle, CPU was not used by any of the processes
- Blue - User initiated processes, run with default priority
- Red - System processes



CPU graph

The statistics were last updated at: Wed Sep 3 11:50:08 2014

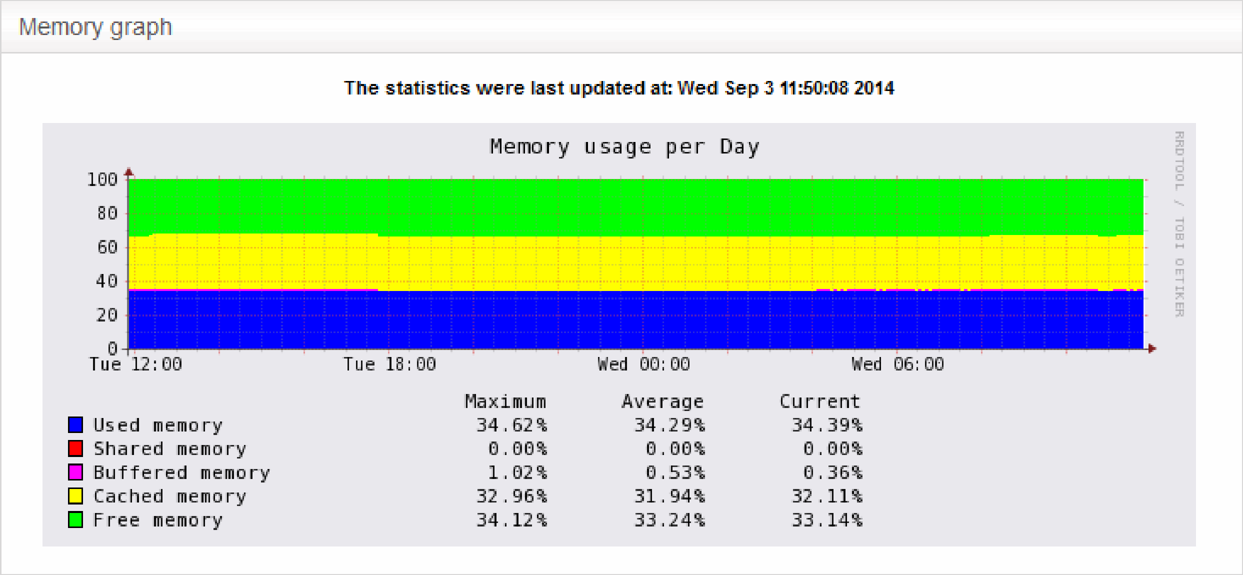
	Maximum	Average	Current
🟦 User CPU usage	15.43%	1.85%	2.26%
🟥 System CPU usage	5.78%	2.34%	2.85%
🟩 Idle CPU usage	96.69%	95.80%	94.90%

The table below the graph shows the maximum, average and current load of the CPU for the past day from various processes. Clicking the graph opens a new page with detailed CPU usage history graphs for the past day, week, month and year.

Memory Graph

The Memory Graph shows memory usage over the past 24 hours. The different types of memory are indicated with different colors.

- Blue - Memory used by running processes
- Red - Memory shared by concurrently running processes
- Pink - Buffered memory space used for temporarily storing data received from or sent to external devices
- Yellow - Cached memory, used for storing recent data used by running processes
- Green - Free, unallocated memory



Memory graph

The statistics were last updated at: Wed Sep 3 11:50:08 2014

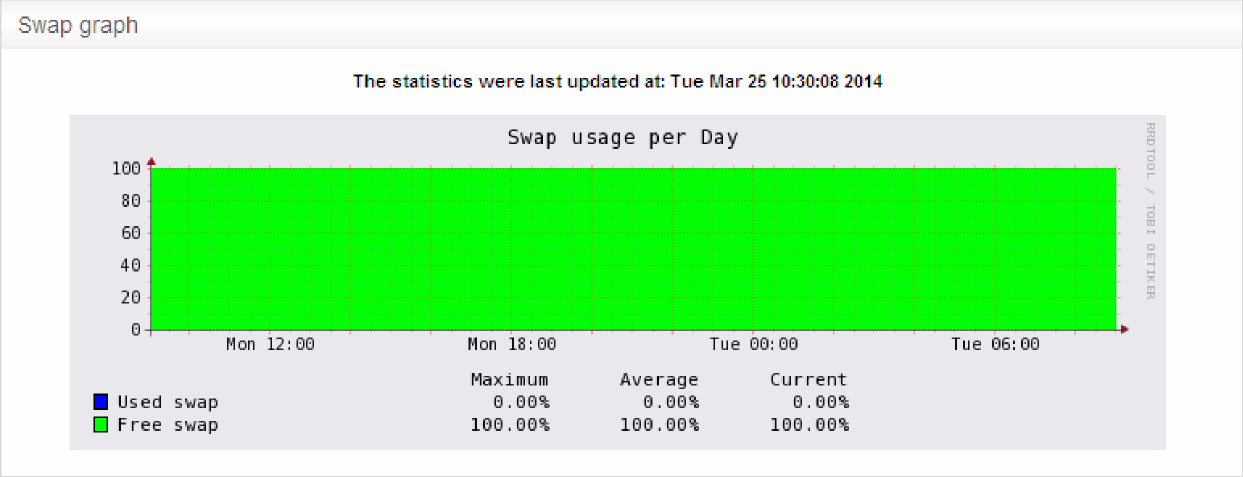
	Maximum	Average	Current
🟦 Used memory	34.62%	34.29%	34.39%
🟥 Shared memory	0.00%	0.00%	0.00%
🟪 Buffered memory	1.02%	0.53%	0.36%
🟨 Cached memory	32.96%	31.94%	32.11%
🟩 Free memory	34.12%	33.24%	33.14%

The table below the graph shows statistics of maximum, average and current usage of system memory for the past day. Clicking the graph opens a new page with detailed memory usage history graphs for the past day, week, month and year.

Swap Graph

The Swap Graph shows the usage of the swap area in the hard disk, used for storing data from inactive processes, from the system memory. Different types of swap spaces are indicated with different colors.

- Blue - Used swap space
- Green - Free swap space



Swap graph

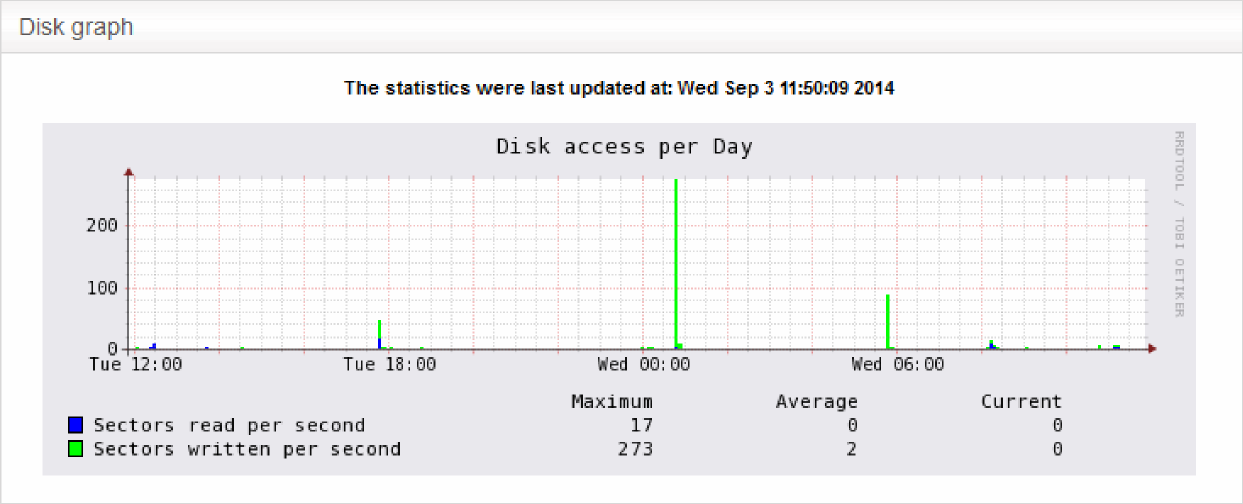
The statistics were last updated at: Tue Mar 25 10:30:08 2014

	Maximum	Average	Current
🟦 Used swap	0.00%	0.00%	0.00%
🟩 Free swap	100.00%	100.00%	100.00%

The table below the graph shows statistics of maximum, average and current usage of swap space for the past day. Clicking the graph opens a new page with detailed usage history graphs for the past day, week, month and year.

Disk Graph

The Disk Graph shows disk access levels over the past two days.



Disk graph

The statistics were last updated at: Wed Sep 3 11:50:09 2014

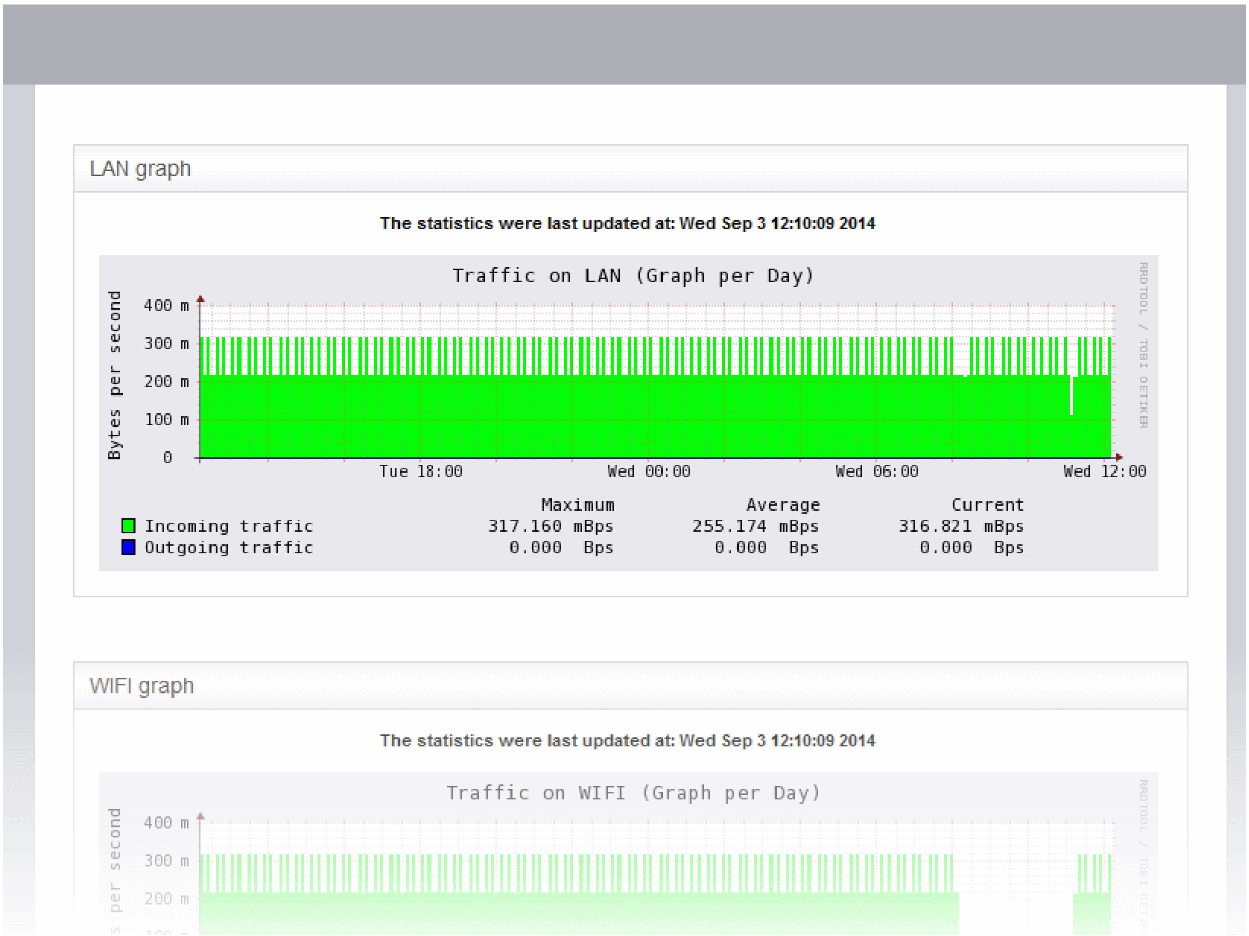
	Maximum	Average	Current
🟦 Sectors read per second	17	0	0
🟩 Sectors written per second	273	2	0

- Green - Percentage of sectors accessed for writing into the disk
- Blue - Percentage of sectors accessed for reading from the disk

The table below the graph shows maximum access, average access and current usage of the disk space over he past two days. Clicking the graph opens a new page with detailed access history graphs for the past day, week, month and year.

5.4 Network Traffic

The Network Traffic Graphs screen shows the amount of data passing through different network zones (LAN, DMZ, Wi-Fi and external network zone). The number of graphs shown on this page depends on number of network zones configured in the DFW virtual appliance.


LAN graph
The statistics were last updated at: Wed Sep 3 12:10:09 2014
Traffic on LAN (Graph per Day)
Bytes per second
400 m
300 m
200 m
100 m
0
Tue 18:00
Wed 00:00
Wed 06:00
Wed 12:00
RRDTOOL / TOBI OETIKER
Maximum
Average
Current
🟩 Incoming traffic 317.160 mBps 255.174 mBps 316.821 mBps
🟦 Outgoing traffic 0.000 Bps 0.000 Bps 0.000 Bps
WIFI graph
The statistics were last updated at: Wed Sep 3 12:10:09 2014
Traffic on WIFI (Graph per Day)
per second
400 m
300 m
200 m
RRDTOOL / TOBI OETIKER

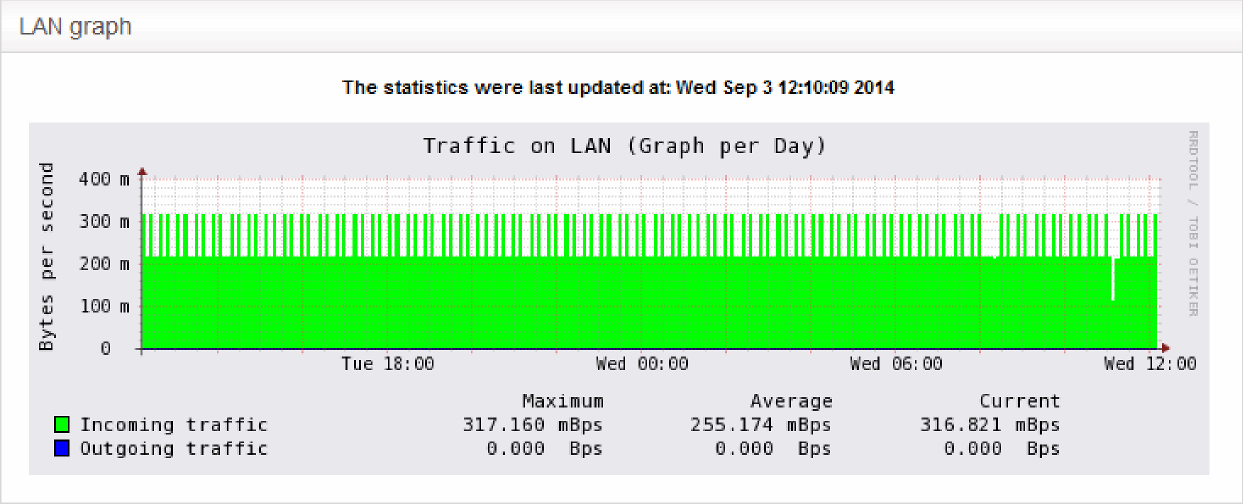
Selecting a graph opens a new page with more detailed graphs showing the data traffic for the past day, week, month and year.

- LAN Graph
- WIFI Graph
- DMZ Graph
- Uplink Graphs

LAN Graph

The LAN Graph shows the data traffic passing through the Local Area Network (LAN). The oncoming and outgoing traffic are indicated with different colors.

- Green - Incoming traffic
- Blue - Outgoing traffic



LAN graph

The statistics were last updated at: Wed Sep 3 12:10:09 2014

	Maximum	Average	Current
🟩 Incoming traffic	317.160 mBps	255.174 mBps	316.821 mBps
🟦 Outgoing traffic	0.000 Bps	0.000 Bps	0.000 Bps

The table below the graph shows statistics of maximum, average and current data traffic through the local network for the past day. Clicking the graph opens a new page with detailed traffic statistics for the past day, week, month and year.

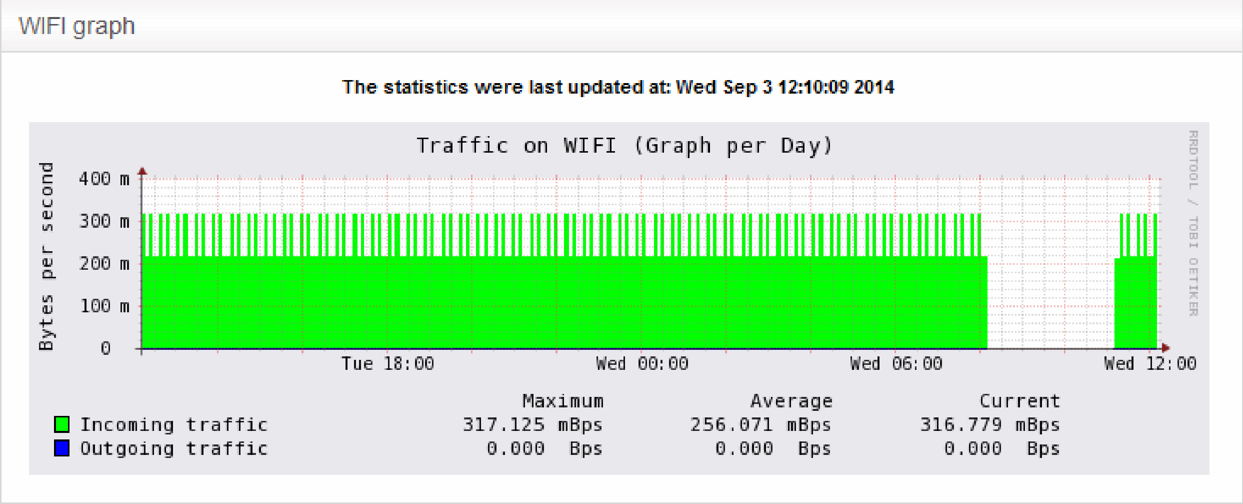
WIFI Graph

The WiFi Graph shows the data traffic through the Wi-Fi network zone defined in your network.

Note: The WiFi Graph will be displayed only if you have a WiFi network zone configured in your network.

The oncoming and outgoing traffic are indicated with different colors.

- Green - Incoming traffic
- Blue - Outgoing traffic



WIFI graph

The statistics were last updated at: Wed Sep 3 12:10:09 2014

	Maximum	Average	Current
🟩 Incoming traffic	317.125 mBps	256.071 mBps	316.779 mBps
🟦 Outgoing traffic	0.000 Bps	0.000 Bps	0.000 Bps

The table below the graph shows statistics about the maximum, average and current data traffic through the WiFi network zone for the past day. Clicking the graph opens a new page with detailed traffic statistics for the past day, week, month and year.

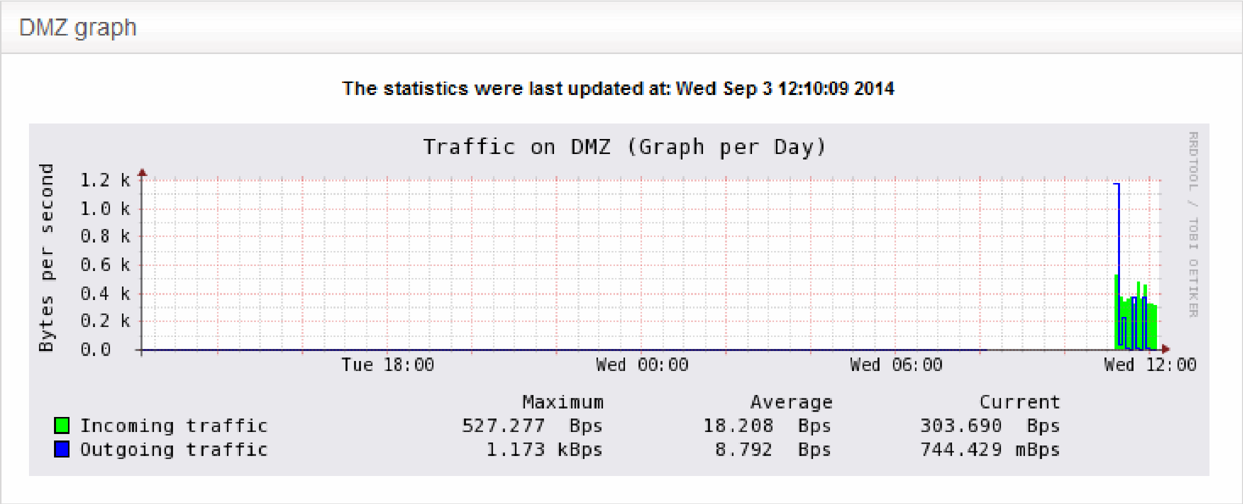
DMZ Graph

The DMZ Graph shows the data traffic through the DMZ network zone defined in your network.

Note: The DMZ Graph will be displayed only if you have a DMZ network zone configured in your network.

The oncoming and outgoing traffic are indicated with different colors.

- Green - Incoming traffic
- Blue - Outgoing traffic



DMZ graph

The statistics were last updated at: Wed Sep 3 12:10:09 2014

Traffic on DMZ (Graph per Day)

	Maximum	Average	Current
🟩 Incoming traffic	527.277 Bps	18.208 Bps	303.690 Bps
🟦 Outgoing traffic	1.173 kBps	8.792 Bps	744.429 mBps

The table below the graph shows statistics for maximum, average and current data traffic through the DMZ network zone for the past day. Clicking the graph opens a new page with detailed data traffic statistics graphs for the past day, week, month and year.

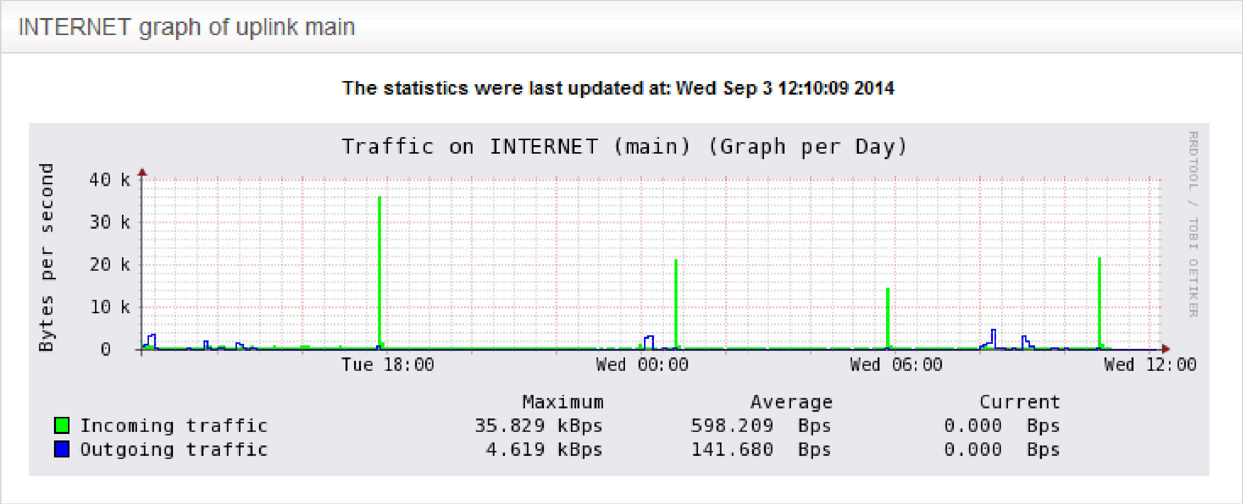
Uplink Graphs

The Uplink Graph(s) show the traffic through external network zones, such as WANs, which are connected to the internet.

Note: If you have more than one uplinks configured for your network, separate graphs will be displayed for each uplink.

Incoming and outgoing traffic are indicated with different colors.

- Green - Incoming traffic
- Blue - Outgoing traffic



INTERNET graph of uplink main

The statistics were last updated at: Wed Sep 3 12:10:09 2014

Traffic on INTERNET (main) (Graph per Day)

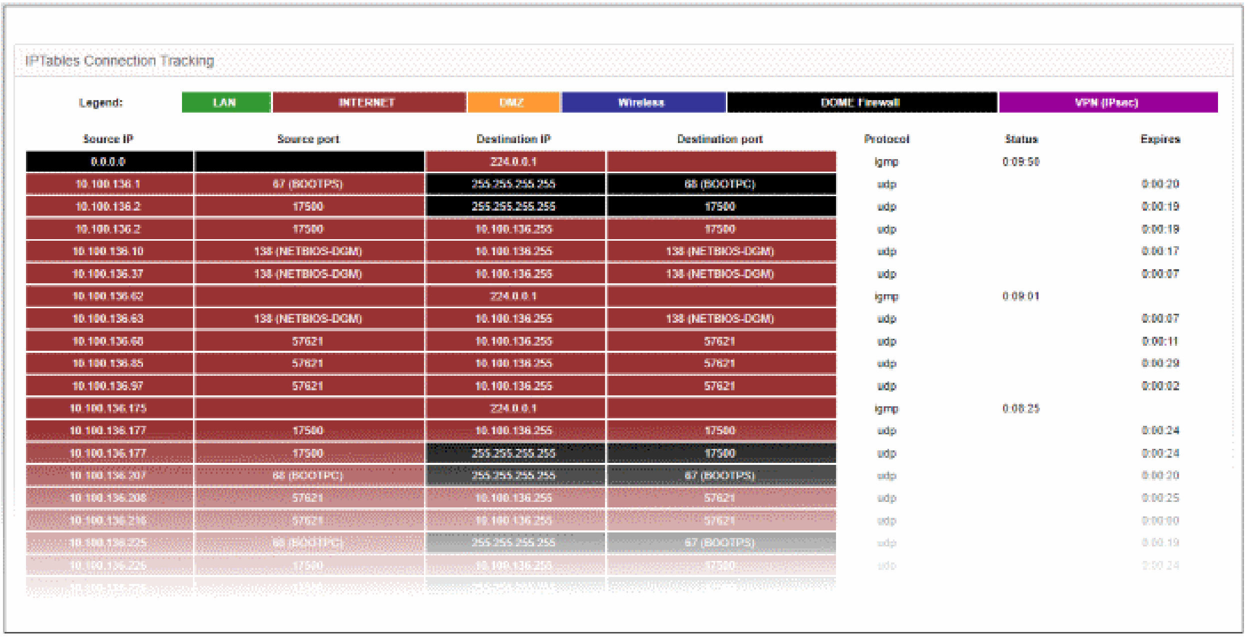
	Maximum	Average	Current
🟩 Incoming traffic	35.829 kBps	598.209 Bps	0.000 Bps
🟦 Outgoing traffic	4.619 kBps	141.680 Bps	0.000 Bps

The table below the graph shows statistics for maximum, average and current data traffic through the zone for the past day. Clicking the graph opens a new page with detailed traffic graphs for the past day, week, month and year.

5.5 Network Connections

The Connections interface displays a list of current network connections to, from and through the DFW virtual appliance with their source, destination, protocol and status. The background colors in the cells of the table depict the source and destination of the connection.

- Green - Indicates LAN connections
- Red - Indicates internet connections
- Orange - Indicates DMZ connections
- Blue - Wireless connections
- Black - Indicates firewall connections, including daemons and services such as SSH or web access
- Purple - Indicates VPN or IPsec connections



IPTables Connection Tracking

Legend: LAN | INTERNET | DMZ | Wireless | DOME Firewall | VPN (IPsec)

Source IP	Source port	Destination IP	Destination port	Protocol	Status	Expires
0.0.0.0		224.0.0.1		igmp	0:09:50	
10.100.136.1	67 (BOOTPS)	255.255.255.255	68 (BOOTPC)	udp		0:00:20
10.100.136.2	17500	255.255.255.255	17500	udp		0:00:19
10.100.136.2	17500	10.100.136.255	17500	udp		0:00:19
10.100.136.10	138 (NETBIOS-DGM)	10.100.136.255	138 (NETBIOS-DGM)	udp		0:00:17
10.100.136.37	138 (NETBIOS-DGM)	10.100.136.255	138 (NETBIOS-DGM)	udp		0:00:07
10.100.136.62		224.0.0.1		igmp	0:09:01	
10.100.136.63	138 (NETBIOS-DGM)	10.100.136.255	138 (NETBIOS-DGM)	udp		0:00:07
10.100.136.60	57621	10.100.136.255	57621	udp		0:00:11
10.100.136.85	57621	10.100.136.255	57621	udp		0:00:29
10.100.136.97	57621	10.100.136.255	57621	udp		0:00:02
10.100.136.175		224.0.0.1		igmp	0:08:25	
10.100.136.177	17500	10.100.136.255	17500	udp		0:00:24
10.100.136.177	17500	255.255.255.255	17500	udp		0:00:24
10.100.136.207	68 (BOOTPC)	255.255.255.255	67 (BOOTPS)	udp		0:00:20
10.100.136.208	57621	10.100.136.255	57621	udp		0:00:25
10.100.136.216	57621	10.100.136.255	57621	udp		0:00:00
10.100.136.225	68 (BOOTPC)	255.255.255.255	67 (BOOTPS)	udp		0:00:19
10.100.136.226	17500	10.100.136.255	17500	udp		0:00:24

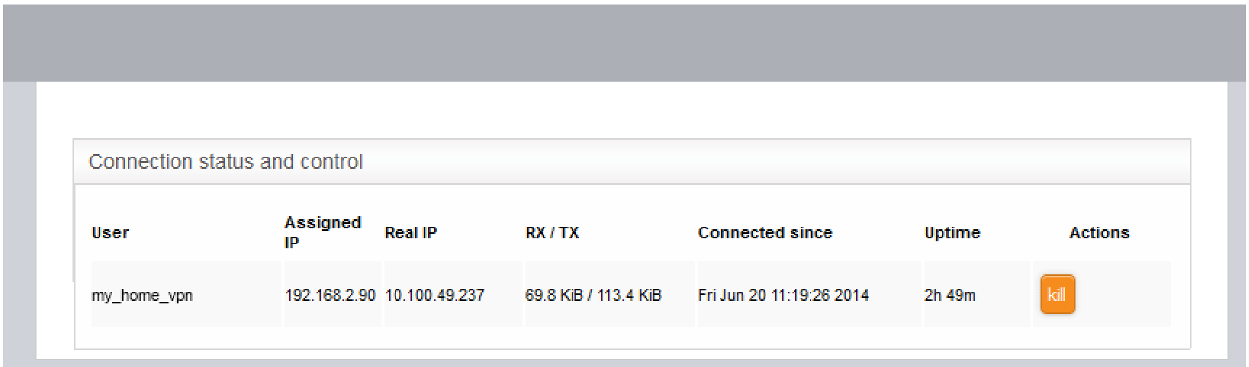
IP Table Connections - Column Descriptions	
Column	**Description**
Source IP	IP from which the connection originated.
Source Port	Port number from which the connection originated.
Destination IP	IP address of the device to which packets are being sent
Destination Port	Port number used to connect to the device at the destination IP
Protocol	Type of connection. Typically either TCP or UDP.
Status	Indicates the current status of the connection (only for TCP). The status will be either Established (active connection) and Closed (connection closed).
Expires	Indicates the time the connection will remain in the same status.

- Clicking an IP address will provide 'WHOIS' data
- Clicking a port number will lead to 'Internet Storm Center' webpage providing details of the port activity such as which services used that port including any exploits and the number of attacks received.

5.6 SSLVPN Connections

Administrators can configure the DFW virtual appliance to allow OpenVPN clients in external networks to connect to internal network zones, and as an OpenVPN client for gateway to gateway connections to external OpenVPN servers. For more details on configuring OpenVPN connections and user accounts, see '**Configuring Virtual Private Network Settings**' for more details.

The SSLVPN connections screen displays a list of active connections from external clients that are connected to the OpenVPN server configured in the DFW virtual appliance. The interface also provides other details such as since when the connections is established, how long the connection is up and more. Administrators can also terminate unwanted VPN connections.



Connection status and control

User	Assigned IP	Real IP	RX / TX	Connected since	Uptime	Actions
my_home_vpn	192.168.2.90	10.100.49.237	69.8 KiB / 113.4 KiB	Fri Jun 20 11:19:26 2014	2h 49m	kill

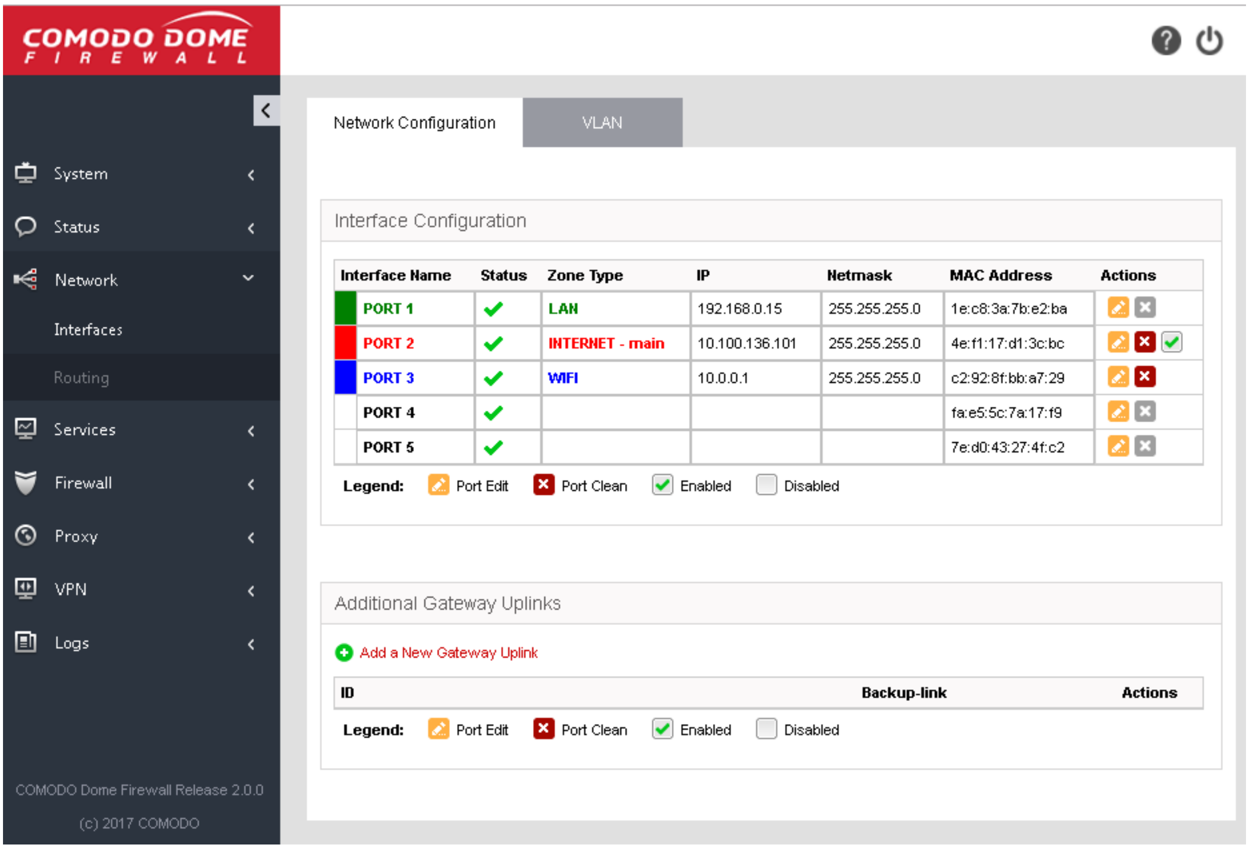
Open VPN Server Connection status and control table - Column Descriptions	
Column	**Description**
User	The user name of the account with which the client has logged-in to the server
Assigned IP	The IP address dynamically assigned to the client from Dome FW.
Real IP	The original externally facing IP address of the client
RX / TX	Displays data transmitted and received by Dome FW to / from the client during the current session.
Connected since	The date and time that the connection was established.
Uptime	The length of time the current session has been active.
Actions	Displays control buttons for terminating the session. kill - Enables to stop the connection.

6 Network Configuration

Depending on the configuration, the DFW virtual appliance has a minimum of four ports to connect devices in different network zones to external networks like the internet. You can connect different interface devices to the ports in desired order.

Once you have connected the interface devices and logged-in to the management interface, you need to complete an initial network configuration to successfully deploy the virtual appliance to the network. Dome Firewall has a built-in wizard which assists you to do this. The Network Setup Wizard can be accessed by clicking Network > Interfaces from the left hand side navigation.

- Click 'Network' in the left-hand menu to open the network module



Interface Configuration

Interface Name	Status	Zone Type	IP	Netmask	MAC Address	Actions
PORT 1	✓	LAN	192.168.0.15	255.255.255.0	1e:c8:3a:7b:e2:ba	✎ ☒
PORT 2	✓	INTERNET - main	10.100.136.101	255.255.255.0	4e:f1:17:d1:3c:bc	✎ ☒ ☑
PORT 3	✓	WIFI	10.0.0.1	255.255.255.0	c2:92:8f:bb:a7:29	✎ ☒
PORT 4	✓				fa:e5:5c:7a:17:f9	✎ ☒
PORT 5	✓				7e:d0:43:27:4f:c2	✎ ☒

Legend: ✎ Port Edit ☒ Port Clean ☑ Enabled □ Disabled

Additional Gateway Uplinks

Add a New Gateway Uplink

ID	Backup-link	Actions

Legend: ✎ Port Edit ☒ Port Clean ☑ Enabled □ Disabled

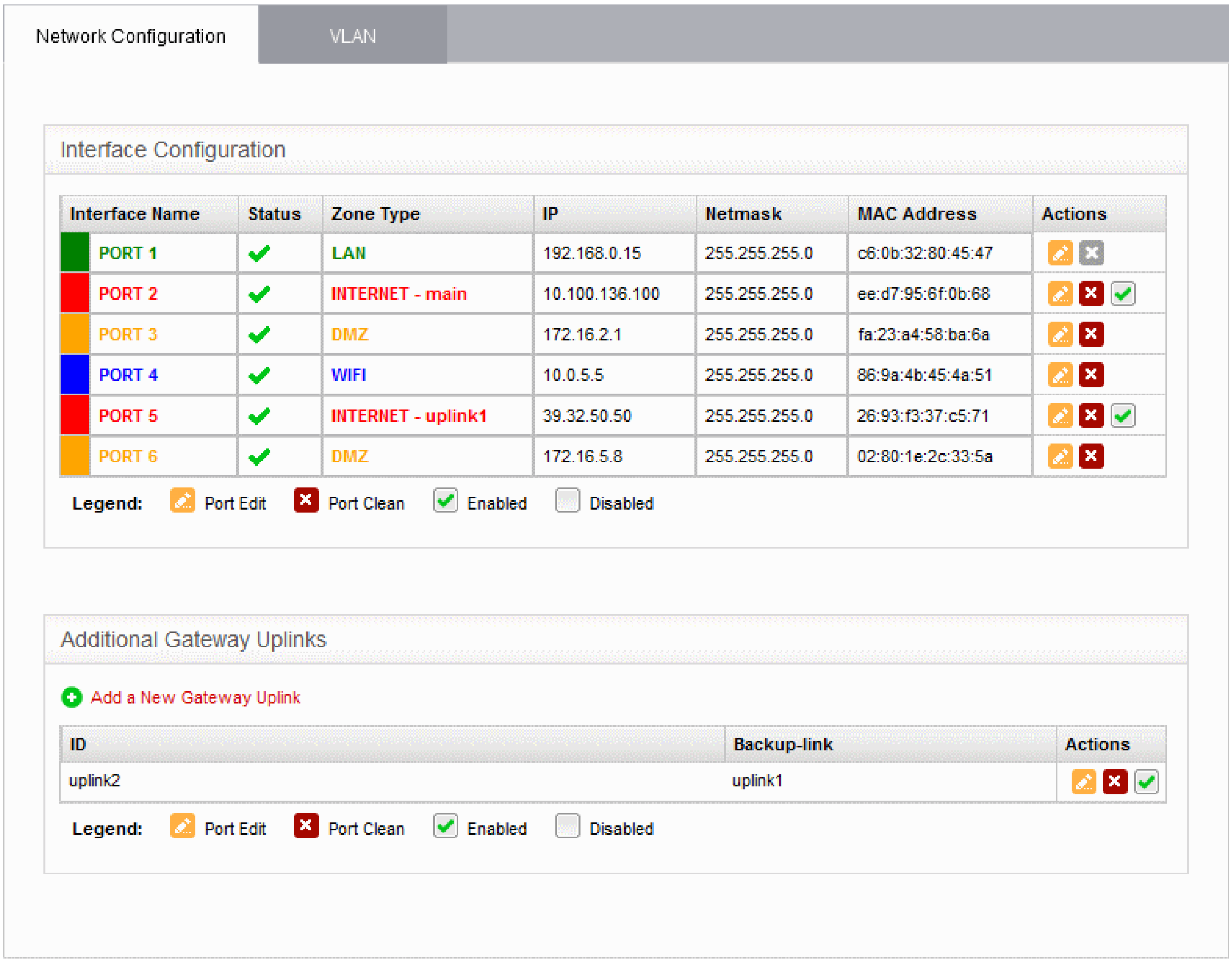
The module has the following areas:

- **Interfaces** - Carry out basic configuration on network interfaces. Add uplinks to the virtual appliance for fail-over. Configure Virtual LANs (VLANs). See **Configuring Interface Devices, Uplinks and VLANs** for more details.
- **Routing** - Create custom routes for the firewall to connect to networks through devices like external routers or VPN tunnels. See **Routes** for more details.

6.1 Configure Interface Devices, Uplinks and VLANs

The 'Interfaces' screen allows you to add and edit interface devices which connect to network zones, add fail-over uplinks and to configure Virtual LANs (VLANs).

- Click 'Network' > 'Interfaces' to open the network and VLAN configuration screens:



Interface Configuration

Interface Name	Status	Zone Type	IP	Netmask	MAC Address	Actions
🟩 PORT 1	✓	LAN	192.168.0.15	255.255.255.0	c6:0b:32:80:45:47	✎ ✖
🟥 PORT 2	✓	INTERNET - main	10.100.136.100	255.255.255.0	ee:d7:95:6f:0b:68	✎ ✖ ☑
🟧 PORT 3	✓	DMZ	172.16.2.1	255.255.255.0	fa:23:a4:58:ba:6a	✎ ✖
🟦 PORT 4	✓	WIFI	10.0.5.5	255.255.255.0	86:9a:4b:45:4a:51	✎ ✖
🟥 PORT 5	✓	INTERNET - uplink1	39.32.50.50	255.255.255.0	26:93:f3:37:c5:71	✎ ✖ ☑
🟧 PORT 6	✓	DMZ	172.16.5.8	255.255.255.0	02:80:1e:2c:33:5a	✎ ✖

Legend: ✎ Port Edit ✖ Port Clean ☑ Enabled □ Disabled

Additional Gateway Uplinks

Add a New Gateway Uplink

ID	Backup-link	Actions
uplink2	uplink1	✎ ✖ ☑

Legend: ✎ Port Edit ✖ Port Clean ☑ Enabled □ Disabled

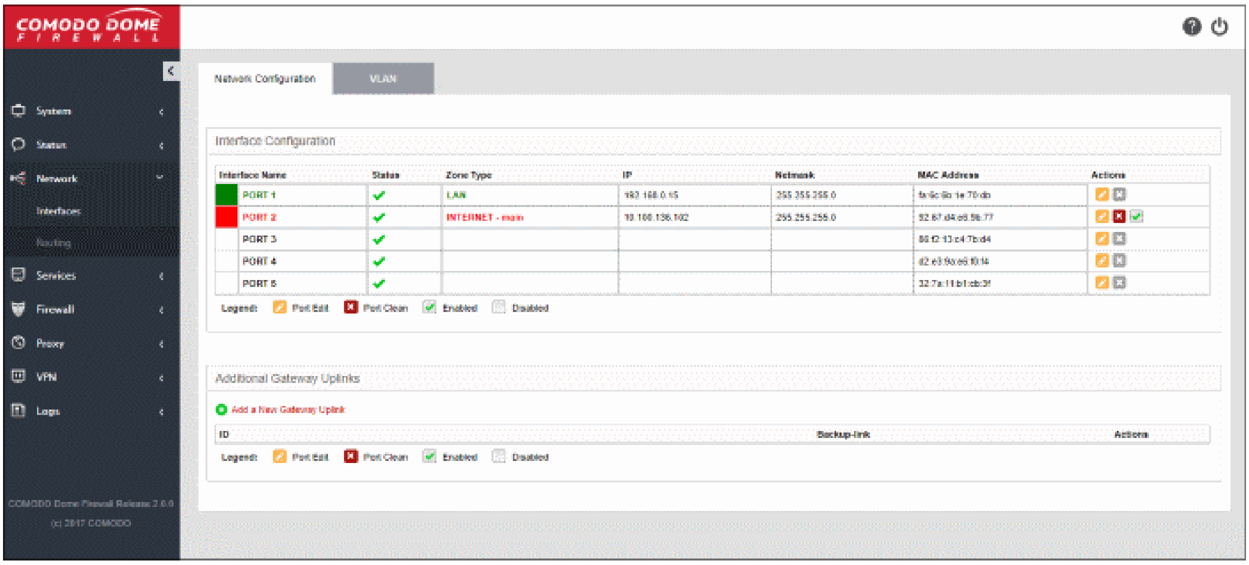
The interface contains two tabs:

- **Network Configuration** - Shows interface devices configured for the virtual appliance along with their connection status. Admins can configure interfaces after connecting the virtual appliance to the network. See **Configuring Interface Devices** for more details. The interface also allows the administrator to configure additional gateway uplink interface devices for fail over. See **Adding and Managing Gateway Uplink Devices** for more details.
- **VLANs** - Add VLANs to be associated with network zone(s). See **Creating VLANs** for more details.

6.1.1 Configuring Interface Devices

The network configuration tab allows you to view and configure appliances which connect to your network.

- Click 'Network' > 'Interfaces' to open the network and VLAN configuration screens:



Interface Configuration

Interface Name	Status	Zone Type	IP	Netmask	MAC Address	Actions
🟩 PORT 1	✓	LAN	192.168.0.15	255.255.255.0	fa:6c:6b:1e:70:db	
🟥 PORT 2	✓	INTERNET - main	10.100.136.102	255.255.255.0	92:67:d4:e6:9b:77	
PORT 3	✓				86:f2:13:c4:7b:d4	
PORT 4	✓				d2:e3:9a:e6:f0:f4	
PORT 5	✓				32:7a:11:b1:cb:3f	

Legend: Port Edit ☒ Port Clean ☑ Enabled □ Disabled

Additional Gateway Uplinks

Add a New Gateway Uplink

ID	Backup-link	Actions

Legend: Port Edit ☒ Port Clean ☑ Enabled □ Disabled

The network configuration screen has two panes:

- **Interface Configuration** - Shows interface devices connected to the ports of the virtual appliance along with their configuration and connection status. Allows you to add and manage network zone interfaces. This section explains about how to configure the interface devices.
- **Additional Gateway Uplinks** - Shows nodes in your internal network zones configured as gateway devices for the DFW virtual appliance to connect to internet. Allows you to add and manage gateway devices. See next section **Adding and Managing Gateway Uplink Devices** for more details.

Interface Configuration

The interface configuration table shows port configuration details for your interface devices. You can add new interface connections and enable/disable existing connections from this interface.

Interface Configuration Table - Column Descriptions	
Column Header	**Description**
Interface Name	Name of the Dome Firewall port. The font color indicates the type of network zone to which the port is connected. Red - External networks, like WAN, for internet connection Yellow - DMZ zone Green - Local Area Network to which workstations are connected Blue - Wi-Fi network
Status	Link status of the interface device. The status can be one of the following: Green Tick - Link is active Red Cross - The link is not active Question Mark - No information about the link from the device driver
Zone Type	The network zone type of the interface. The network zone can be one of the following: • Internet • LAN • Wi-Fi • DMZ

Interface Configuration Table - Column Descriptions	
Column Header	**Description**
IP	The IP address of the interface device connected to the port.
Netmask	The netmask of the network zone connected through the interface
MAC Address	The Media Access Control (MAC) address of the interface
Actions	Displays control buttons for editing and deleting the port entries ✎ - Opens connection settings and allows you to edit the parameters of the interface. ☒ - Disconnects the interface and clears the port. ☑ - Indicates whether the port is enabled or disabled. The checkbox also allows the administrator to switch the port between enabled and disabled states.

The following sections explain how to configure the network zone interfaces:

- **Configuring untrusted external network zones like WAN for connecting to the Internet**
- **Configuring trusted internal network zones like LAN**
- **Configuring the DMZ interface**
- **Configuring the Wi-Fi interface**

Configuring untrusted external network zones like WAN for connecting to the Internet

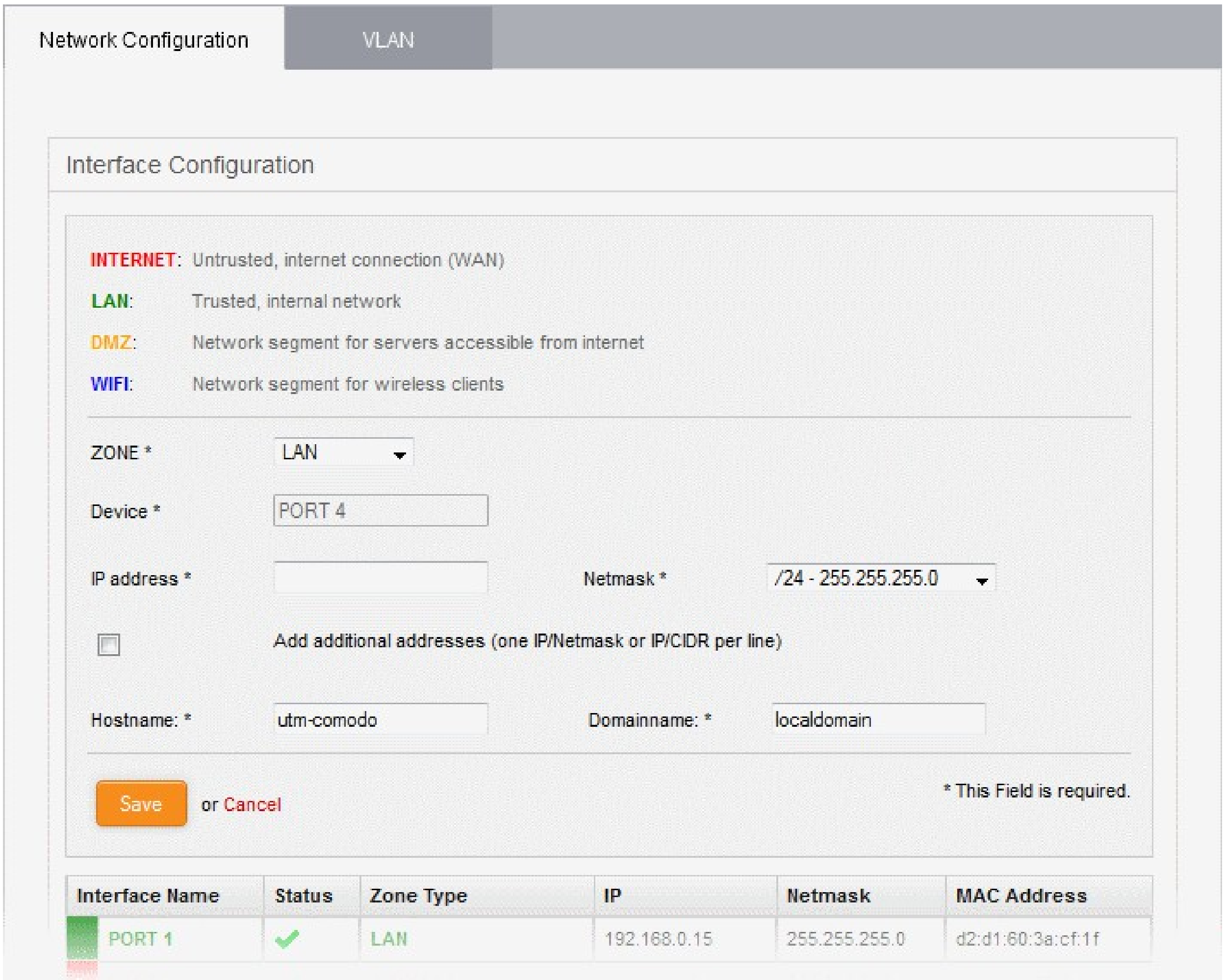
The setup for external networks involves choosing the physical port to which the interface device for main uplink is connected and then configuring network parameters and preferences.

Tip: You can add more uplinks for fail-over and load sharing to different ports at a later time from the 'Network' > 'Interfaces' > 'Network Configuration' screen using the same procedure. Also you can add nodes among your internal network and connected to internet as gateway uplink devices to the virtual appliance through the same interface. See **Adding and Managing Gateway Uplink Devices** for more details.

To configure the external network zone

- Click on the edit icon ✎ in the row of the port to which the interface device for connecting to external network/internet is plugged-in.

The pane for configuring the interface device will open, with the row of the selected port highlighted.



Interface Configuration

INTERNET: Untrusted, internet connection (WAN)

LAN: Trusted, internal network

DMZ: Network segment for servers accessible from internet

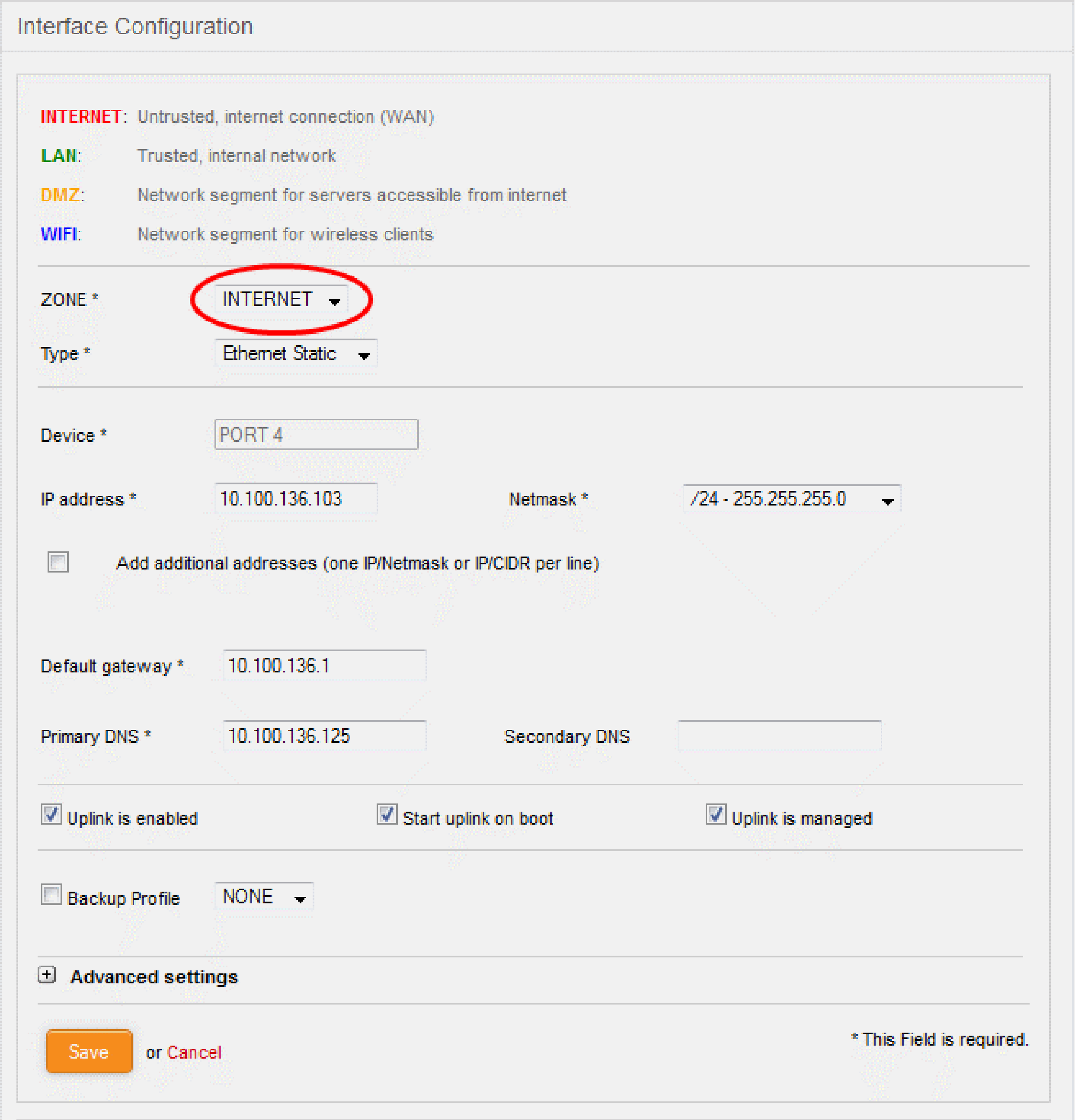
WIFI: Network segment for wireless clients

ZONE *	LAN		
Device *	PORT 4		
IP address *		Netmask *	/24 - 255.255.255.0
□	Add additional addresses (one IP/Netmask or IP/CIDR per line)		
Hostname: *	utm-comodo	Domainname: *	localdomain

* This Field is required.

Interface Name	Status	Zone Type	IP	Netmask	MAC Address
PORT 1	✓	LAN	192.168.0.15	255.255.255.0	d2:d1:60:3a:cf:1f

- Zone - Select 'Internet' from the drop-down. The configuration options for external network interface devices will appear:



Interface Configuration

INTERNET: Untrusted, internet connection (WAN)

LAN: Trusted, internal network

DMZ: Network segment for servers accessible from internet

WIFI: Network segment for wireless clients

ZONE * INTERNET

Type * Ethernet Static

Device * PORT 4

IP address * 10.100.136.103 Netmask * /24 - 255.255.255.0

☐ Add additional addresses (one IP/Netmask or IP/CIDR per line)

Default gateway * 10.100.136.1

Primary DNS * 10.100.136.125 Secondary DNS

☑ Uplink is enabled ☑ Start uplink on boot ☑ Uplink is managed

☐ Backup Profile NONE

- Type - Choose the interface type through which the virtual appliance is connected to the internet. The available options are:
  - ETHERNET STATIC - The external network interface is in a LAN and has a fixed IP address and netmask. An example is a router in which the DFW virtual appliance is assigned a fixed IP address.
  - ETHERNET DHCP - The external network interface receives its network configuration through dynamic host control protocol (DHCP) from a local server, router, or modem.
  - PPPoE - The external interface is connected to an ADSL modem through an Ethernet cable. Select this option only if the modem uses the Point-to-Point Protocol over Ethernet (PPPoE) protocol to connect to the service provider.

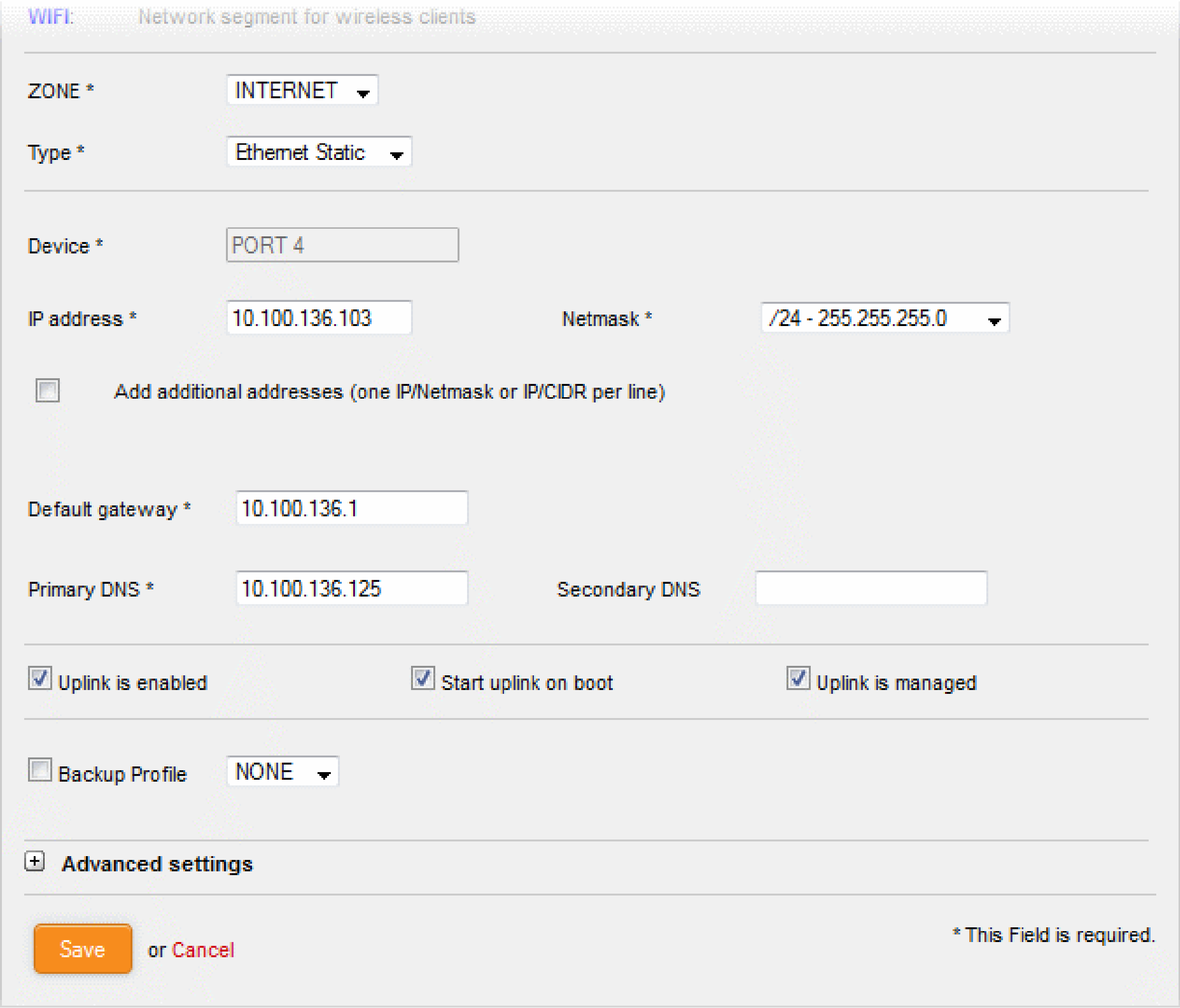
The following sections explain configuration parameters for each interface type:

- ETHERNET STATIC
- ETHERNET DHCP

- **PPPoE**

ETHERNET STATIC

- Configure the following for the external network zone



WIFI: Network segment for wireless clients

ZONE *	INTERNET		
Type *	Ethernet Static		
Device *	PORT 4		
IP address *	10.100.136.103	Netmask *	/24 - 255.255.255.0
□	Add additional addresses (one IP/Netmask or IP/CIDR per line)		
Default gateway *	10.100.136.1		
Primary DNS *	10.100.136.125	Secondary DNS	
☑ Uplink is enabled	☑ Start uplink on boot	☑ Uplink is managed	
□ Backup Profile	NONE		

⊞ **Advanced settings**

Save or Cancel

* This Field is required.

Device Settings

- Device - The port to which the interface device is connected. The port is pre-selected.
- IP Address - Enter the IP address of the interface device
- Netmask - Choose the network mask containing the possible masks from the drop-down (e.g. /24 - 255.255.255.0)
- Add additional addresses - If additional IP address(es)/netmask(s) are to be added to the interface, select the 'Add additional addresses' checkbox and enter the additional IP address(es)/netmask(s) of different subnets one by one per line.
- Default gateway - Enter the IP address of the default gateway through which the virtual appliance connects to internet in the 'Default Gateway' text box
- DNS Settings - Enter the IP addresses/hostnames of the primary and secondary DNS servers to be used in the respective fields.

Uplink Settings

- Uplink is Enabled - The uplink will be activated immediately after it is created. Deselect this if you don't want to enable the uplink device at this time. You can enable the uplink later in two ways:
  - Interface configuration screen - Enable the port in the **Interface Configuration screen**
  - Dashboard - Enable the 'Active' checkbox beside the uplink in the 'Uplinks' box. See the

section explaining the Uplinks box in the '**Dashboard**' for more details.

- Start uplink on boot - The uplink will start automatically on every restart of the DFW virtual appliance. Deselect this checkbox if you want to manually start the uplink only when required.
- Uplink is managed - The uplink will be managed by Dome Firewall and its details will be displayed in the Dashboard. Deselect this option if you do not want the uplink details to be displayed in the Dashboard. You can switch the uplink to managed state at any time by selecting the 'Managed' checkbox beside the uplink in the Dashboard. See **section explaining the Uplinks box** in the '**Dashboard**' chapter for more details.
- Backup Profile - Select this checkbox if you want to specify an alternative uplink connection to be activated in the event this uplink fails and choose the alternative uplink device from the drop-down.
- Additional Link check hosts - The uplink reconnects automatically after a time period set by your ISP, in the event of a connection failure. If you want the virtual appliance to check whether the uplink has connected successfully, you can try to ping known hosts in an external network. Enabling this option will reveal a text field where you should enter a list of one or more perpetually reachable IP addresses or hostnames. One of the hosts could be your ISP's DNS server or gateway.

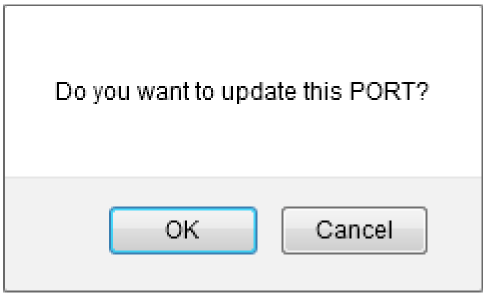
Advanced Settings:

The Advanced Settings pane allows you to specify the MAC address and the Maximum Transmission Unit (MTU) of the data packets for the interface device. These settings are optional. If you need to specify custom values for these fields, click on the '+' sign beside 'Advanced Settings' to expand the 'Advanced Settings' pane.

- Use custom MAC address - The virtual appliance has the capability to automatically detect the MAC address of the device connected to the port specified and populates the same in the MAC address column. If you need to specify a different MAC address to override and replace the default MAC address of the external interface, select the ' Use custom MAC address' checkbox and enter the MAC address in the text box that appears below the checkbox.
- Reconnection timeout - Specify the maximum time period (in seconds) that the uplink should attempt to reconnect in the event of a connection failure. The reconnection timeout period depends on the ISP configuration. If you are unsure, leave this field blank.
- MTU - Enter the Maximum Transmission Unit (MTU) of the data packets that can be sent over the network.

- Click 'Save'.

A confirmation dialog will be displayed.



Do you want to update this PORT?

- Click OK.

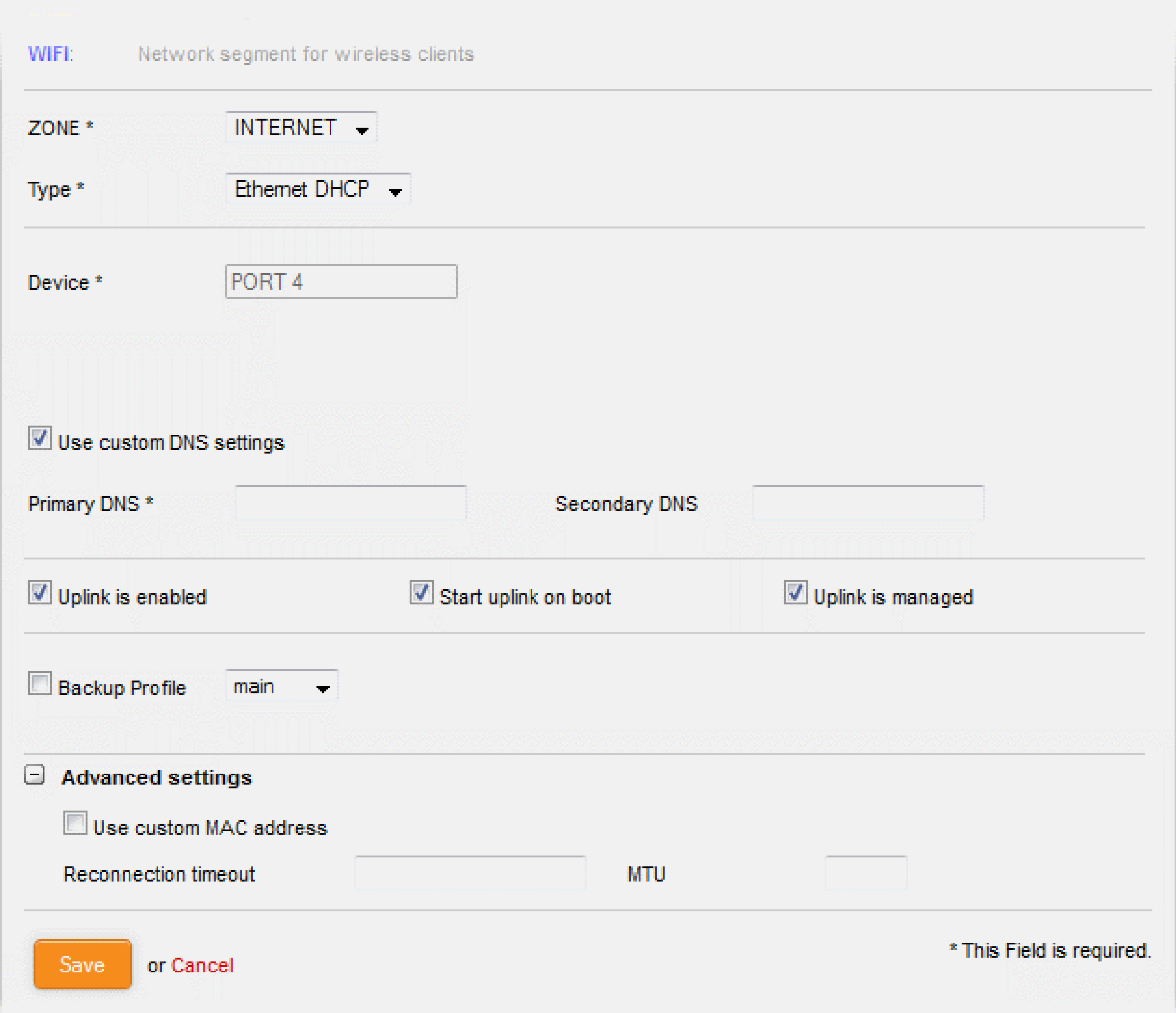
The virtual appliance will restart for your settings to take effect.

- Network configuration activities like date, time, type of event, subject id, component name and the event outcome are logged.

Tip: You can edit the network configuration e.g. for changing selected parameters like hostname or the network range of a zone, at any time depending on changes in your network. Click Network > Interface, click the 'Edit icon' ✎ in the 'Internet' row of the table, make the changes and save the changes.

ETHERNET DHCP

- Configure the following for the external network zone with Ethernet DHCP interface



WIFI: Network segment for wireless clients

ZONE * INTERNET

Type * Ethernet DHCP

Device * PORT 4

☑ Use custom DNS settings

Primary DNS * Secondary DNS

☑ Uplink is enabled ☑ Start uplink on boot ☑ Uplink is managed

☐ Backup Profile main

⊟ **Advanced settings**

☐ Use custom MAC address

Reconnection timeout MTU

Save or Cancel * This Field is required.

Device Settings

- Device - The port to which the interface device is connected. The port is pre-selected.
- DNS Settings - Select whether the DNS servers are to be automatically or manually assigned. If the latter, select the 'Use Custom DNS Settings' checkbox and enter the IP addresses/hostnames of the your primary and secondary DNS servers.

Uplink Settings

- Uplink is Enabled - The uplink will be activated immediately after it is created. Deselect this if you don't want to enable the uplink device at this time. You can enable the uplink later in two ways:
  - Interface configuration screen - Enable the port in the **Interface Configuration screen**
  - Dashboard - Enable the 'Active' checkbox beside the uplink in the 'Uplinks' box. See the **section explaining the Uplinks box** in the '**Dashboard**' for more details.
- Start uplink on boot - The uplink will start automatically on every restart of the DFW virtual appliance. Deselect this checkbox if you want to manually start the uplink when required.
- Uplink is managed - The uplink will be managed by Dome Firewall and its details displayed in the dashboard. Deselect this option if you do not want the uplink to be listed in the dashboard. You can switch the uplink to managed state at any time by selecting the 'Managed' checkbox beside the uplink in the dashboard. See **section explaining the Uplinks box** in the '**Dashboard**' chapter for

more details.

- Backup Profile - Select if you want to specify an alternative uplink connection which is activated in the event this uplink fails. You need to choose the alternative uplink device from the drop-down.
- Additional Link check hosts - The uplink reconnects automatically after a time period set by your ISP in the event of a connection failure. If you want the virtual appliance to check whether the uplink has connected successfully, you can try to ping known hosts in an external network.

  Enabling this option will reveal a text field where you should enter a list of one or more perpetually reachable IP addresses or hostnames. One of the hosts could be your ISP's DNS server or gateway.

Advanced Settings:

The 'Advanced Settings' pane allows you to specify the MAC address and the Maximum Transmission Unit (MTU) of the data packets for the interface device. These settings are optional. If you need to specify custom values for these fields, click on the '+' sign beside 'Advanced Settings' to expand the 'Advanced Settings' pane.

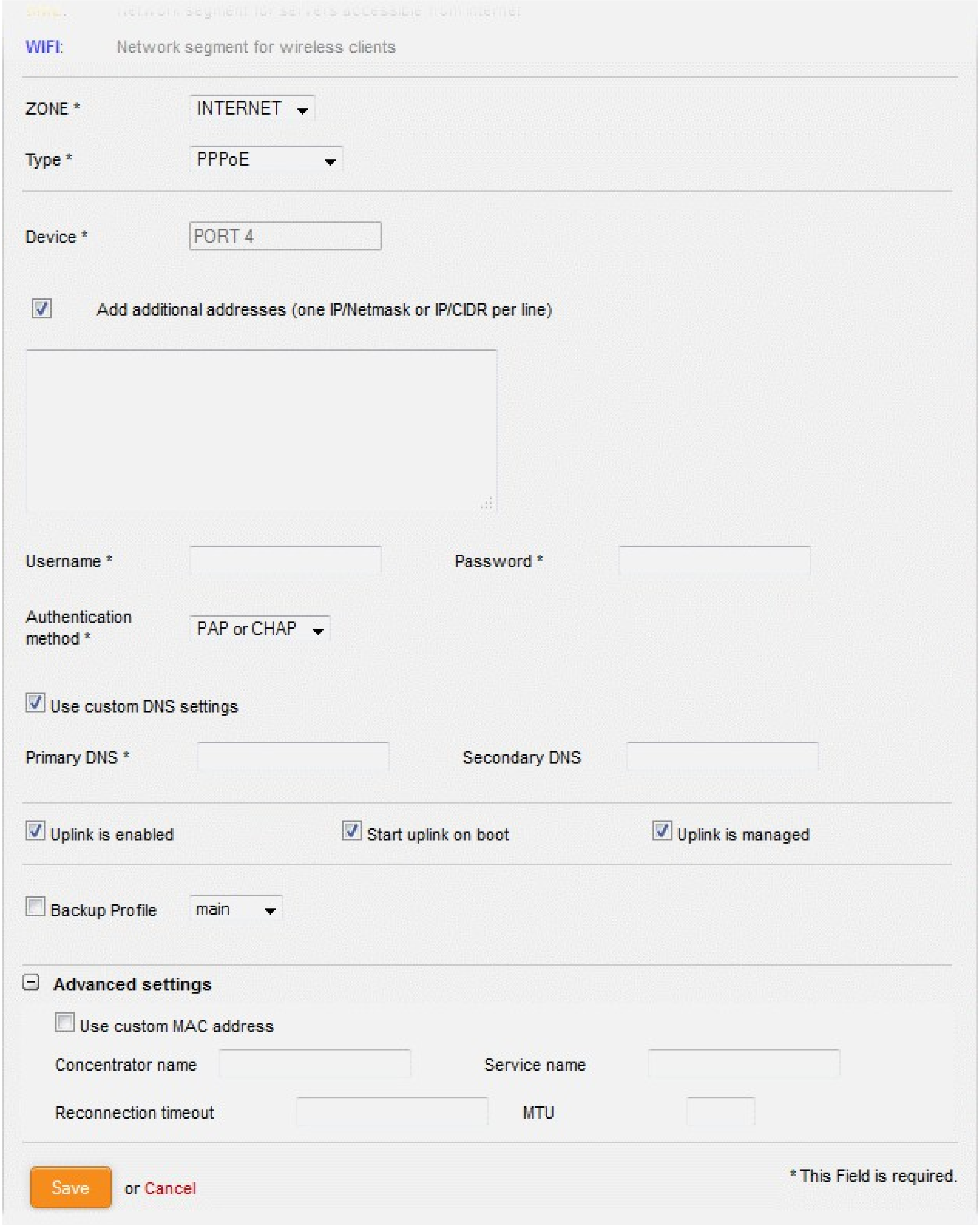
- Use custom MAC address - By default, the virtual appliance automatically detects the MAC address of the device connected to the specified port and populates the MAC address column with this information. If you need to specify a different MAC address (and replace the default MAC address of the external interface), select the ' Use custom MAC address' checkbox and enter the MAC address in the text box that appears below the checkbox.
- Reconnection timeout - Specify the maximum time period (in seconds) that the uplink should attempt to reconnect in the event of a connection failure. The reconnection timeout period depends on the ISP configuration. If you are unsure, leave this field blank.
- MTU - Enter the Maximum Transmission Unit (MTU) of the data packets that can be sent over the network.

- Click 'Save'.
- Network configuration activities like date, time, type of event, subject id, component name and the event outcome are logged.

Tip: You can edit the network configuration e.g. for changing selected parameters like hostname or the network range of a zone, at any time depending on changes in your network. Click Network > Interface, click the 'Edit icon' ✎ in the 'Internet' row of the table, make the changes and save the changes.

PPPoE

- Configure the following for external network zones with PPPoP interface



DMZ: Network segment for servers accessible from internet

WIFI: Network segment for wireless clients

ZONE * INTERNET

Type * PPPoE

Device * PORT 4

☑ Add additional addresses (one IP/Netmask or IP/CIDR per line)

Username * Password *

Authentication method * PAP or CHAP

☑ Use custom DNS settings

Primary DNS * Secondary DNS

☑ Uplink is enabled ☑ Start uplink on boot ☑ Uplink is managed

☐ Backup Profile main

⊟ **Advanced settings**

☐ Use custom MAC address

Concentrator name Service name

Reconnection timeout MTU

Save or Cancel

* This Field is required.

Device Settings

- Device - The port to which the interface device is connected. The port is pre-selected.
- Add additional addresses - If additional IP address(es)/netmask(s) are to be added to the interface, select the 'Add additional addresses' checkbox and enter the additional IP address(es)/netmask(s) of different subnets one by one per line.
- Username - Enter the login username for internet connection as provided by your Internet Service Provider (ISP)
- Password - Enter the login password as provided by your ISP for internet connection

- Authentication Method - Enter the method of authentication used by your ISP for your device to connect to internet from the drop-down. The options available are: Password Authentication Protocol (PAP); Challenge Handshake Authentication Protocol (CHAP); or both. If you are not sure about the authentication method, choose PAP or CHAP (Default).
- DNS Settings - Select whether the DNS servers are to be automatically assigned or manually assigned. If the later, select the Use 'Custom DNS Settings' checkbox and enter the IP addresses/hostnames of the primary and secondary DNS servers to be used.

Uplink Settings

- Uplink is Enabled - The uplink will be activated immediately after it is created. Deselect this if you don't want to enable the uplink device at this time. You can enable the uplink later in two ways:
  - Interface configuration screen - Enable the port in the **Interface Configuration screen**
  - Dashboard - Enable the 'Active' checkbox beside the uplink in the 'Uplinks' box. See the **section explaining the Uplinks box** in the '**Dashboard**' for more details.
- Start uplink on boot - The uplink will start automatically on every restart of the DFW virtual appliance. Deselect this checkbox if you want to manually start the uplink only when required.
- Uplink is managed - The uplink will be managed by Dome Firewall and its details will be displayed in the Dashboard. Deselect this option if you do not want the uplink details to be displayed in the Dashboard. You can switch the uplink to managed state at any time by selecting the 'Managed' checkbox beside the uplink in the Dashboard. See **section explaining the Uplinks box** in the '**Dashboard**' chapter for more details.
- Backup Profile - Select this checkbox if you want to specify an alternative uplink connection to be activated in the event this uplink fails and choose the alternative uplink device from the drop-down.
- Additional Link check hosts - The uplink reconnects automatically after a time period set by your ISP, in the event of a connection failure. If you want the virtual appliance to check whether the uplink has connected successfully, you can try to ping known hosts in an external network. Enabling this option will reveal a text field where you should enter a list of one or more perpetually reachable IP addresses or hostnames. One of the hosts could be your ISP's DNS server or gateway.

Advanced Settings:

The Advanced Settings pane allows you to specify the MAC address and the Maximum Transmission Unit (MTU) of the data packets for the interface device. These settings are optional. If you need to specify custom values for these fields, click on the '+' sign beside 'Advanced Settings' to expand the 'Advanced Settings' pane.

- Use custom MAC address - The virtual appliance has the capability to automatically detect the MAC address of the device connected to the port specified and populates the same in the MAC address column. If you need to specify a different MAC address to override and replace the default MAC address of the external interface, select the ' Use custom MAC address' checkbox and enter the MAC address in the text box that appears below the checkbox.
- Concentrator name - Enter the identifier of the remote access concentrator setup by your service provider (Optional, usually not needed).
- Service Name - Enter the name of your ISP (Optional, usually not needed).
- Reconnection timeout - Specify the maximum time period (in seconds) that the uplink should attempt to reconnect in the event of a connection failure. The reconnection timeout period depends on the ISP configuration. If you are unsure, leave this field blank.
- MTU - Enter the Maximum Transmission Unit (MTU) of the data packets that can be sent over the network.

- Click 'Save'.
- Network configuration activities like date, time, type of event, subject id, component name and the event outcome are logged.

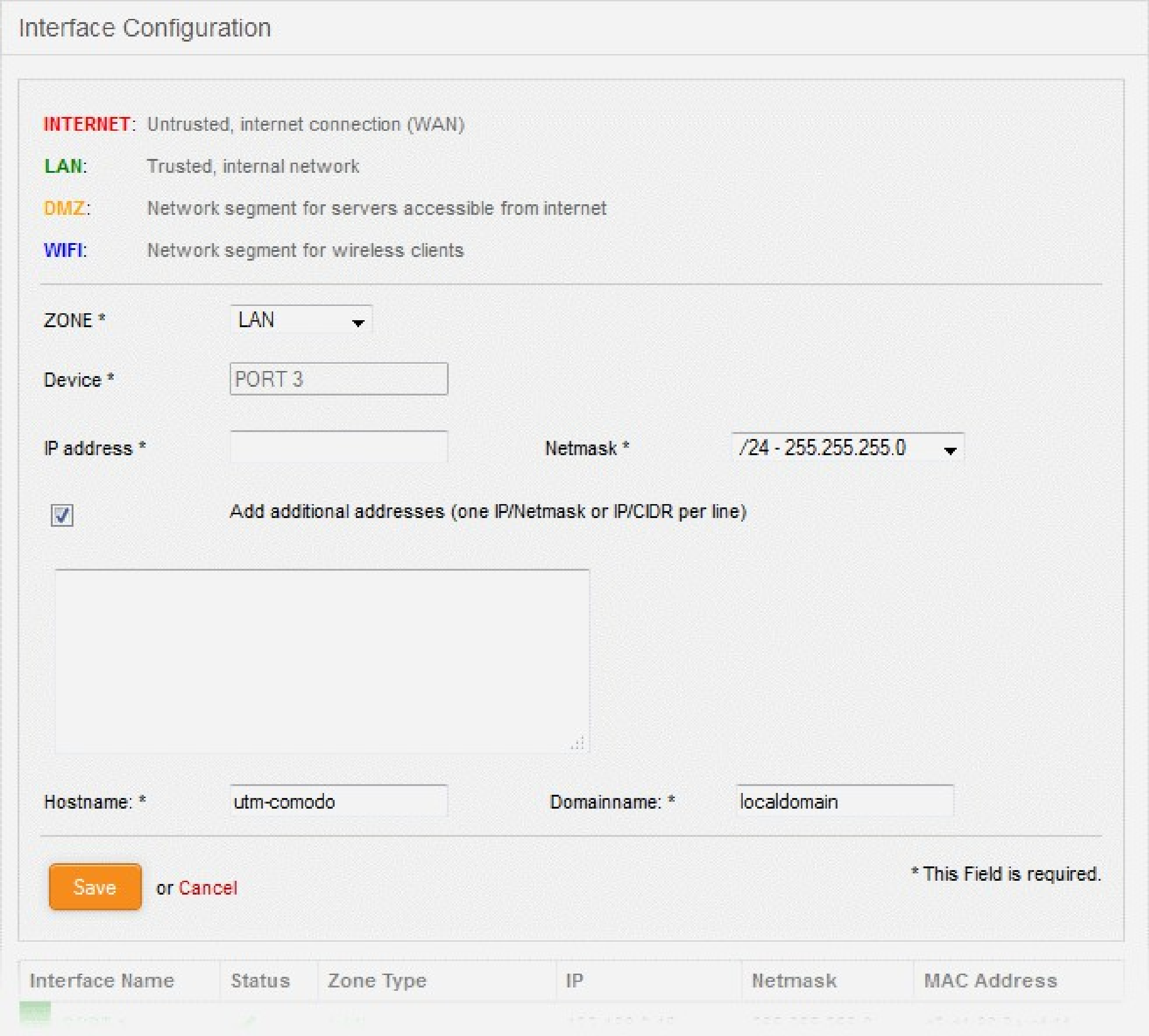
Tip: You can edit the network configuration e.g. for changing selected parameters like hostname or the network range of a zone, at any time depending on changes in your network. Click Network > Interface, click the 'Edit icon' ✎ in the 'Internet' row of the table, make the changes and save the changes.

Configuring a trusted internal network zone (e.g. LAN)

The setup for internal network zone involves choosing the physical port to which the interface device for LAN is connected and then configuring network parameters and preferences for the same.

To configure the internal network zone

- Click on the edit icon ✎ in the row of the port to which the interface device for connecting to the LAN zone is plugged-in.



Interface Configuration

INTERNET: Untrusted, internet connection (WAN)

LAN: Trusted, internal network

DMZ: Network segment for servers accessible from internet

WIFI: Network segment for wireless clients

ZONE * LAN

Device * PORT 3

IP address *

Netmask * /24 - 255.255.255.0

☑ Add additional addresses (one IP/Netmask or IP/CIDR per line)

Hostname: * utm-comodo

Domainname: * localdomain

* This Field is required.

Interface Name	Status	Zone Type	IP	Netmask	MAC Address

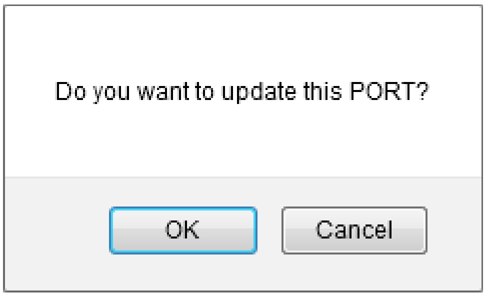
- Zone - Select 'LAN' from the drop-down. The configuration options for the internal network interface device will appear:
- Device - The port to which the interface device is connected. The port is pre-selected.
- IP Address - Enter the IP address of the interface device, as pre-configured in the network
- Netmask - Choose the network mask containing the possible masks from the drop-down (e.g. /24 - 255.255.255.0)
- Add additional addresses - If additional IP address(es)/netmask(s) are to be added to the interface, select the 'Add additional addresses' checkbox and enter the additional IP address(es)/netmask(s)

of different subnets one by one.

- Hostname and Domainname - Enter the host name of your network server and the domain name of your network in the respective text fields

- Click 'Save'.

A confirmation dialog will be displayed.



Do you want to update this PORT?

- Click OK.

The virtual appliance will restart for your settings to take effect.

- Network configuration activities like date, time, type of event, subject id, component name and the event outcome are logged.

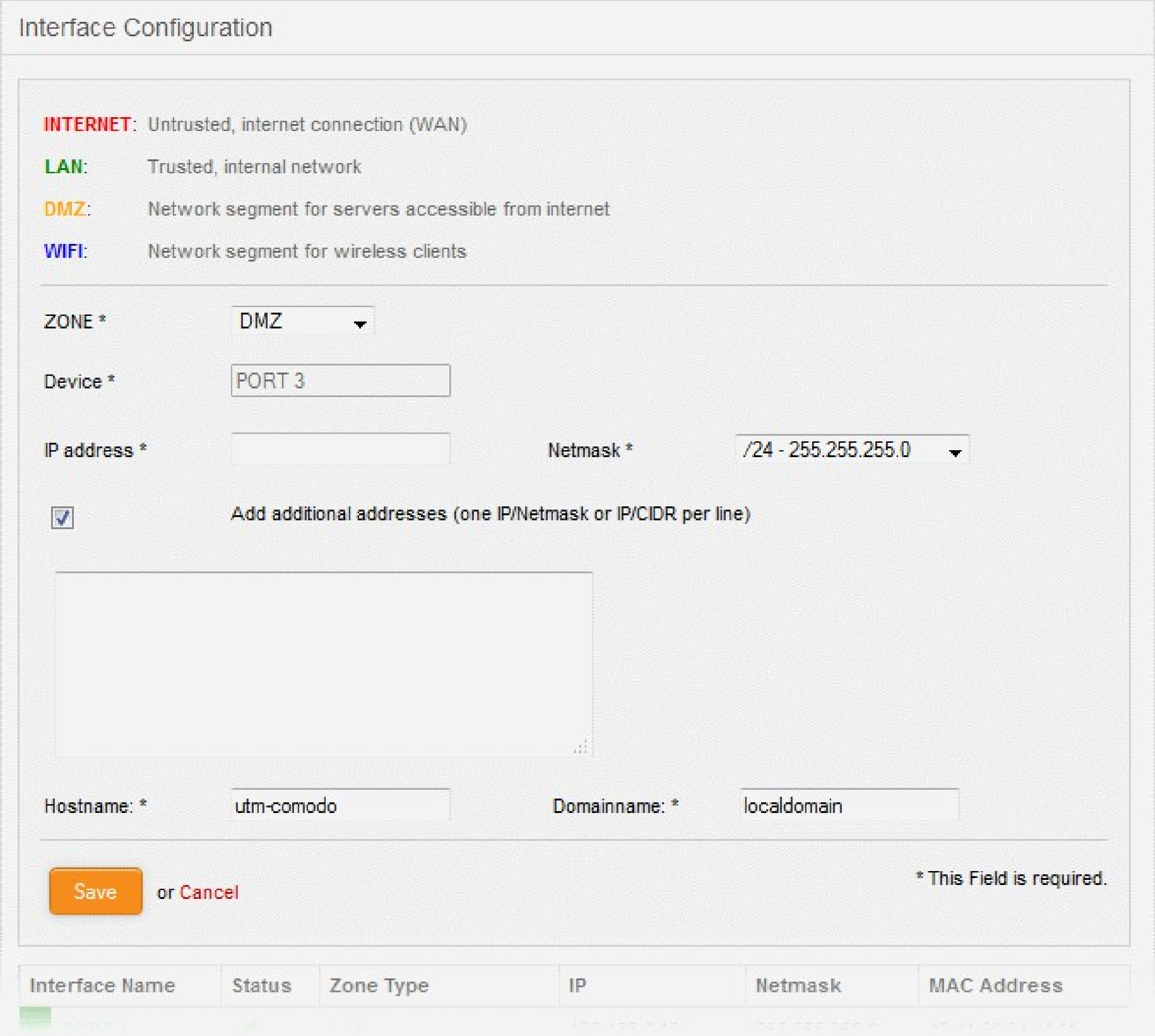
Tip: You can edit the network configuration e.g. for changing selected parameters like hostname or the network range of a zone, at any time depending on changes in your network. Click Network > Interface, click the 'Edit icon' in the 'LAN' row of the table, make the changes and save the changes.

Configuring the DMZ interface

DMZ setup involves choosing the port to which the DMZ device is connected then configuring network parameters and preferences.

To configure the DMZ network zone

- Click the edit icon in the row of the port used by the DMZ device



Interface Configuration

INTERNET: Untrusted, internet connection (WAN)

LAN: Trusted, internal network

DMZ: Network segment for servers accessible from internet

WIFI: Network segment for wireless clients

ZONE *	DMZ		
Device *	PORT 3		
IP address *		Netmask *	/24 - 255.255.255.0

☑ Add additional addresses (one IP/Netmask or IP/CIDR per line)

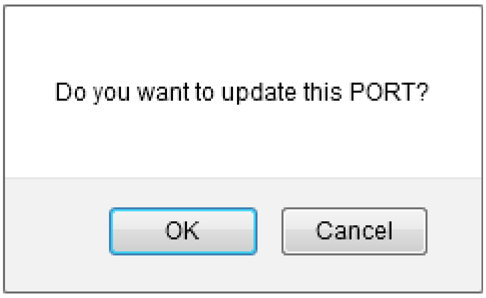
Hostname: *	utm-comodo	Domainname: *	localdomain

Interface Name	Status	Zone Type	IP	Netmask	MAC Address

- Zone - Select 'DMZ' from the drop-down. The configuration options for the DMZ network interface device will appear:
- Device - The port to which the interface device is connected. The port is pre-selected.
- IP Address - Enter the IP address of the interface device, as pre-configured in the network
- Netmask - Choose the network mask containing the possible masks from the drop-down (e.g. /24 - 255.255.255.0)
- Add additional addresses - If additional IP address(es)/netmask(s) are to be added to the interface, select the 'Add additional addresses' checkbox and enter the additional IP address(es)/netmask(s) of different subnets one by one.
- Hostname and Domainname - Enter the host name of your network server and the domain name of your network in the respective text fields

- Click 'Save'.

A confirmation dialog will be displayed.



Do you want to update this PORT?

- Click OK.

The virtual appliance will restart for your settings to take effect.

- Network configuration activities like date, time, type of event, subject id, component name and the event outcome are logged.

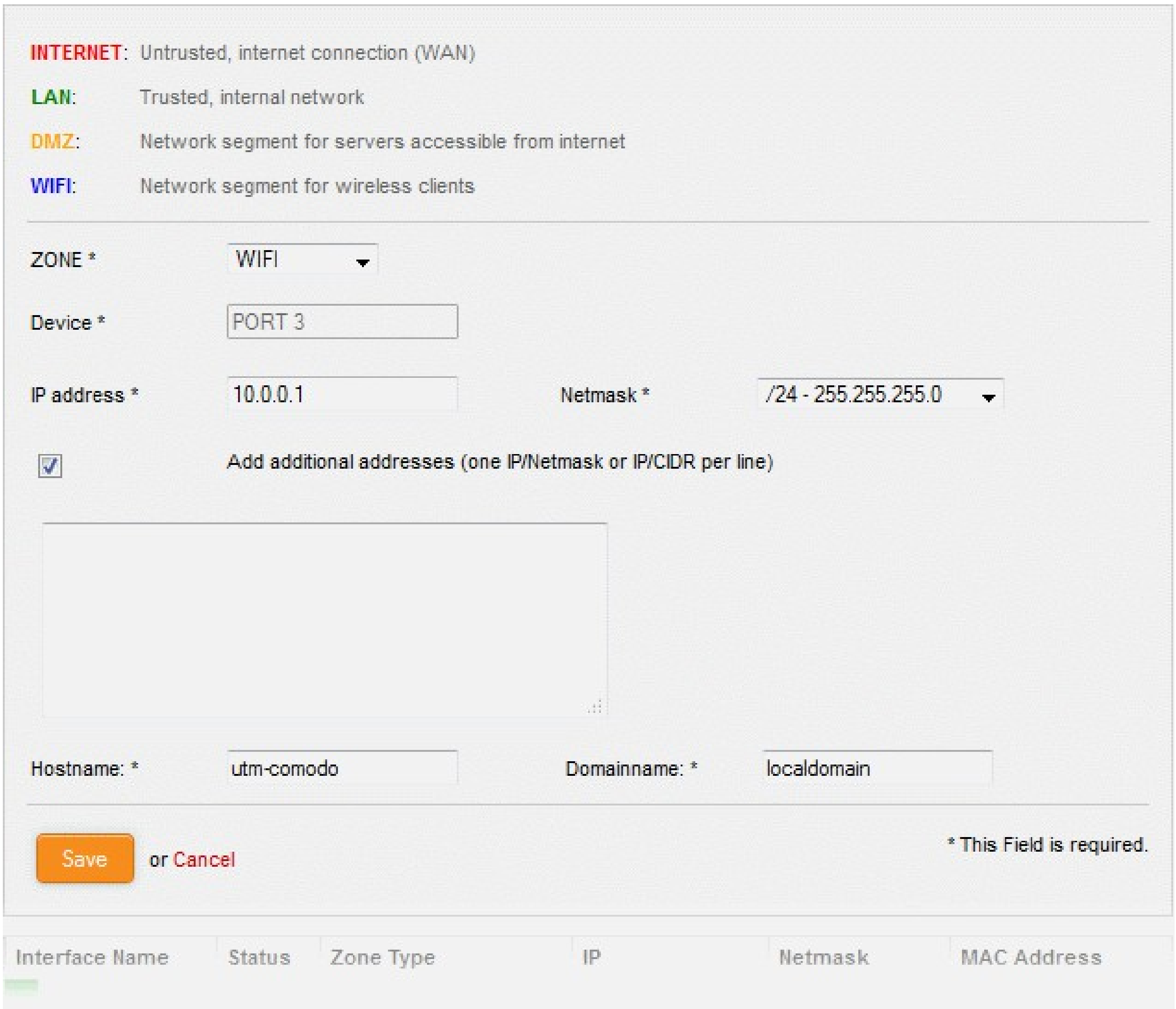
Tip: You can edit the network configuration at any time. To do so, click Network > Interface, click the 'Edit icon' in the 'DMZ' row of the table

Configuring the Wi-Fi interface

The setup for the WiFi zone involves choosing the physical port to which the interface device for Wi-Fi is connected and then configuring network parameters and preferences for the same.

To configure the Wi-Fi network zone

- Click on the edit icon in the row of the port to which the interface device for connecting to the Wi-Fi zone is plugged-in.



INTERNET: Untrusted, internet connection (WAN)

LAN: Trusted, internal network

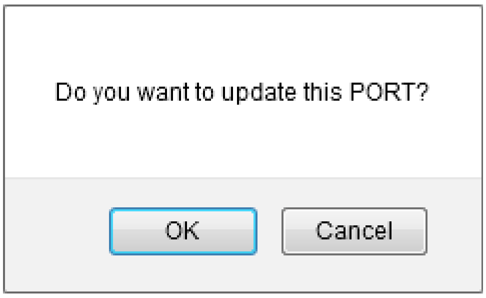
DMZ: Network segment for servers accessible from internet

WIFI: Network segment for wireless clients

ZONE *	WIFI		
Device *	PORT 3		
IP address *	10.0.0.1	Netmask *	/24 - 255.255.255.0
☑	Add additional addresses (one IP/Netmask or IP/CIDR per line)		
Hostname: *	utm-comodo	Domainname: *	localdomain

- Zone - Select 'Wi-Fi' from the drop-down. The configuration options for the Wi-Fi network interface device will appear:
- Device - The port to which the interface device is connected. The port is pre-selected.
- IP Address - Enter the IP address of the interface device, as pre-configured in the network
- Netmask - Choose the network mask containing the possible masks from the drop-down (e.g. /24 - 255.255.255.0)
- Add additional addresses - If additional IP address(es)/netmask(s) are to be added to the interface, select the 'Add additional addresses' checkbox and enter the additional IP address(es)/netmask(s) of different subnets one by one.
- Hostname and Domainname - Enter the host name of your network server and the domain name of your network in the respective text fields

- Click 'Save'. A confirmation dialog will be displayed.


Do you want to update this PORT?

- Click OK.

The virtual appliance will restart for your settings to take effect.

- Network configuration activities like date, time, type of event, subject id, component name and the event outcome are logged.

Tip: You can edit the network configuration e.g. for changing selected parameters like hostname or the network range of a zone, at any time depending on changes in your network. Click Network > Interface, click the 'Edit icon' ✎ in the 'Wi-Fi' row of the table, make the changes and save the changes.

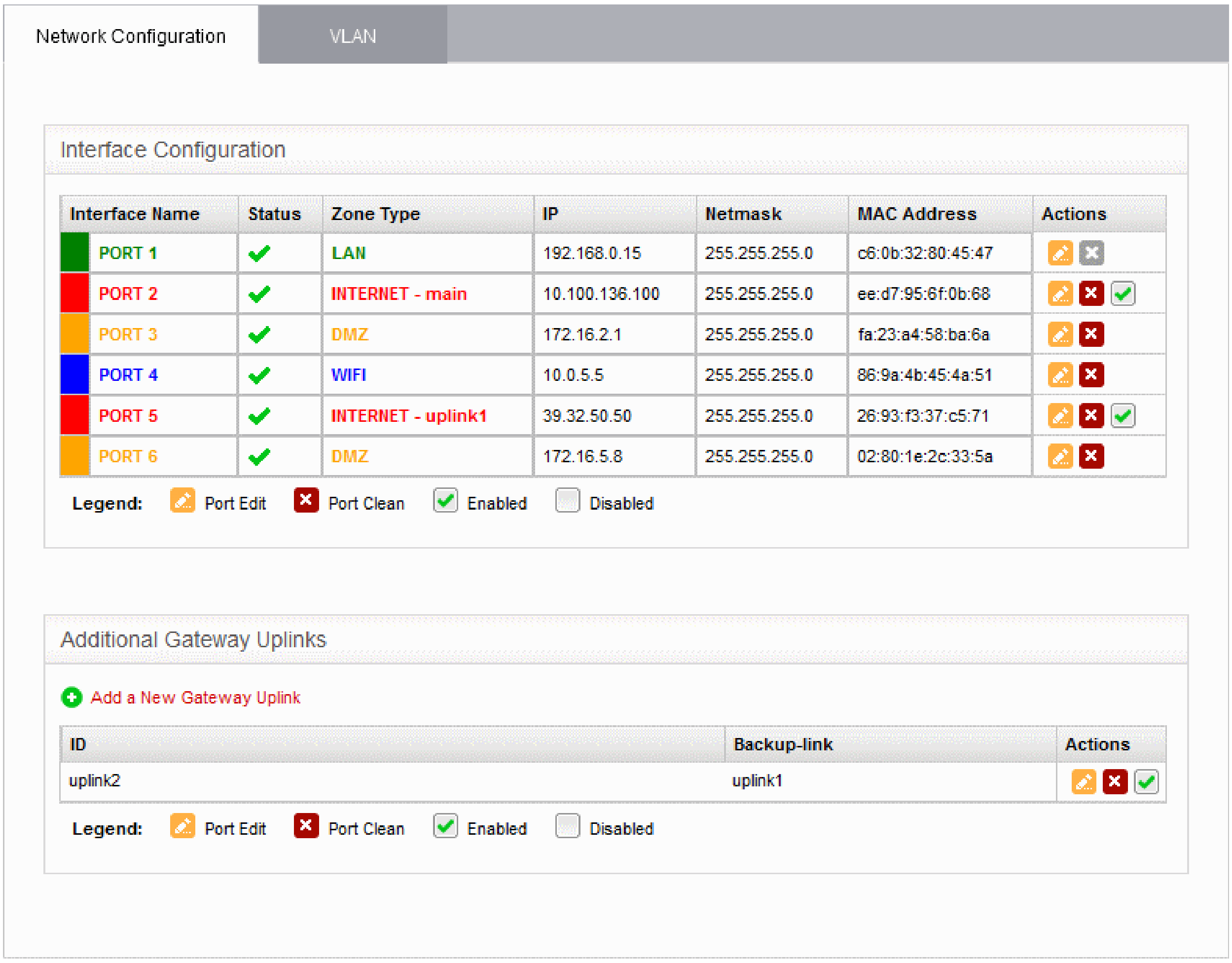
6.1.2 Adding and Managing Gateway Uplink Devices

The main uplink device connected to the virtual appliance (configured during initial network configuration) connects the virtual appliance to the internet and allows network zones like the local area network and DMZ to access the internet. As a standby, the administrator can connect more than one gateway uplink devices to the virtual appliance. The additional gateway uplink device(s) can be configured and used for fail-over in case the main uplink fails.

The 'Additional Gateway Uplinks' pane of the 'Network Configuration' screen displays a list of currently configured gateway uplinks and allows the administrator to add new gateway uplinks.

To add and manage gateway uplink devices

- Click 'Network' > 'Interfaces' from the left hand side navigation
- Click the 'Network Configuration' tab.



Interface Configuration

	Interface Name	Status	Zone Type	IP	Netmask	MAC Address	Actions
🟩	PORT 1	✓	LAN	192.168.0.15	255.255.255.0	c6:0b:32:80:45:47	✎ ☒
🟥	PORT 2	✓	INTERNET - main	10.100.136.100	255.255.255.0	ee:d7:95:6f:0b:68	✎ ☒ ☑
🟧	PORT 3	✓	DMZ	172.16.2.1	255.255.255.0	fa:23:a4:58:ba:6a	✎ ☒
🟦	PORT 4	✓	WIFI	10.0.5.5	255.255.255.0	86:9a:4b:45:4a:51	✎ ☒
🟥	PORT 5	✓	INTERNET - uplink1	39.32.50.50	255.255.255.0	26:93:f3:37:c5:71	✎ ☒ ☑
🟧	PORT 6	✓	DMZ	172.16.5.8	255.255.255.0	02:80:1e:2c:33:5a	✎ ☒

Legend: ✎ Port Edit ☒ Port Clean ☑ Enabled □ Disabled

Additional Gateway Uplinks

⊕ Add a New Gateway Uplink

ID	Backup-link	Actions
uplink2	uplink1	✎ ☒ ☑

Legend: ✎ Port Edit ☒ Port Clean ☑ Enabled □ Disabled

The 'Additional Gateway Uplinks' pane displays the currently connected gateway uplink devices.

Uplink Editor Table - Column Descriptions	
Column	**Description**
ID	The identity of the gateway uplink device, as assigned automatically by the DFW virtual appliance.
Backup-link	The alternative uplink connection that will be activated in the event of failure of this gateway uplink

Actions	Displays control buttons for enabling/disabling and editing the uplink. ✓ - Allows the administrator to enable or disable the uplink. A tick in the checkbox indicates that the uplink is enabled. ✎ - Opens the interface to edit the gateway uplink device configuration parameters. The 'Edit' interface is similar to interface adding a new device. Refer to the section **Adding a Gateway Uplink Device** for more details ☒ - Removes the uplink

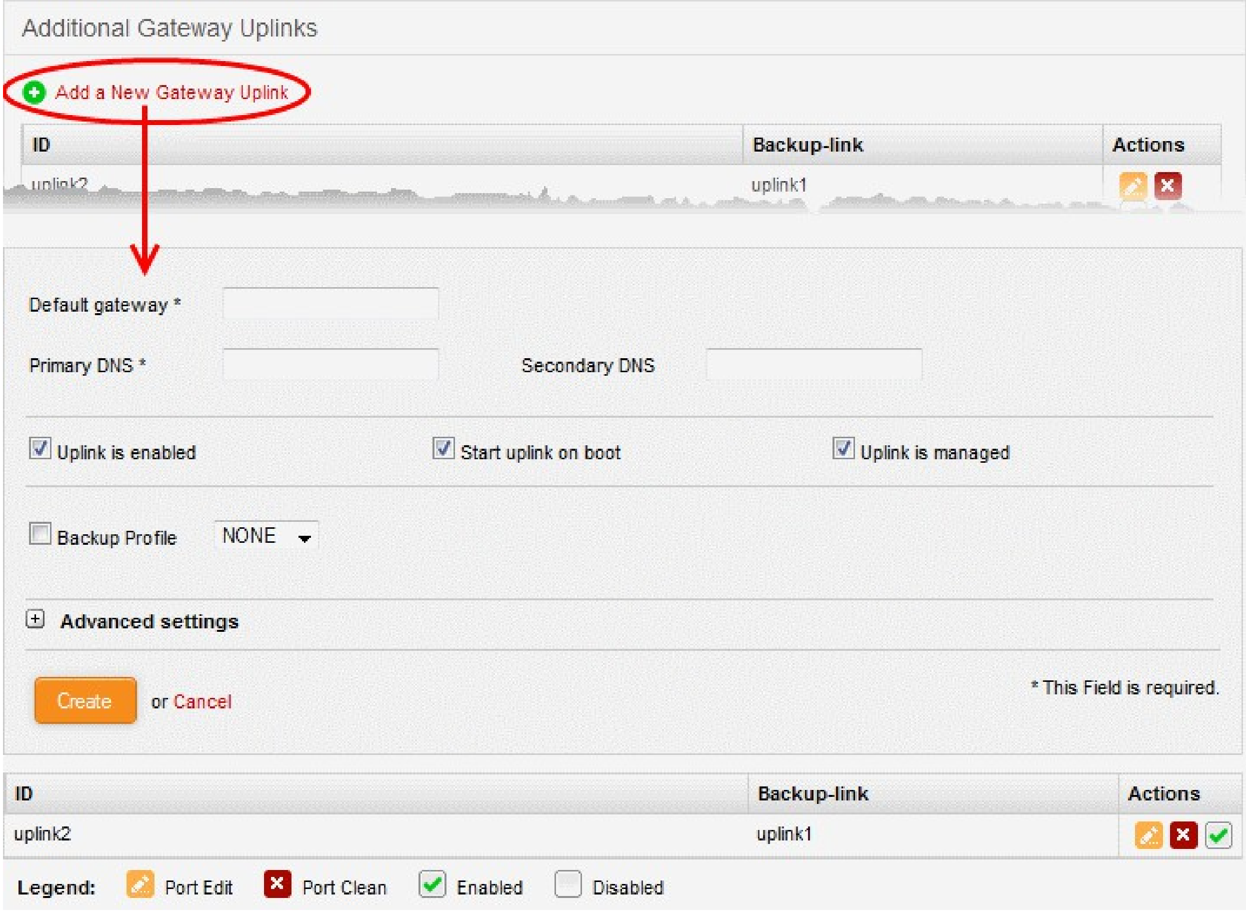
Adding a Gateway Uplink Device

Any node among your internal network zones, individually connected to internet can be configured as additional gateway uplink device for the virtual appliance.

> **Note**: Before configuring a new uplink, ensure that you have connected the uplink device to the DFW virtual appliance.

To add a new gateway uplink device

- Click the 'Add a New Gateway Uplink' link at the top left of the 'Additional Gateway Uplinks' pane. The 'interface for adding a new gateway uplink device will open.



Additional Gateway Uplinks

Add a New Gateway Uplink

ID	Backup-link	Actions
uplink2	uplink1	✎ ☒

Default gateway *

Primary DNS * Secondary DNS

☑ Uplink is enabled ☑ Start uplink on boot ☑ Uplink is managed

□ Backup Profile NONE

⊞ Advanced settings

* This Field is required.

ID	Backup-link	Actions
uplink2	uplink1	✎ ☒ ✓

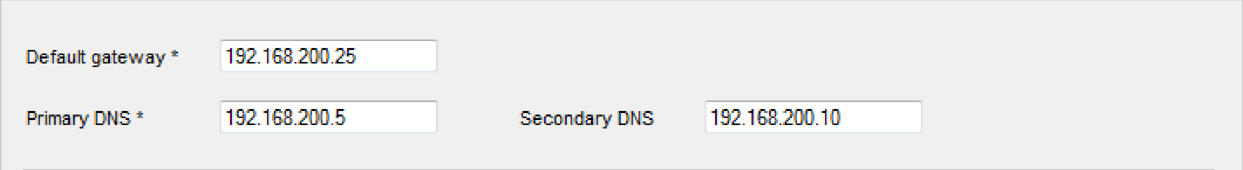
Legend: ✎ Port Edit ☒ Port Clean ✓ Enabled □ Disabled

The 'Uplink Editor' interface is divided into four areas:

- **Device Settings** - Enter IP address and DNS servers for the gateway device
- **Uplink Settings** - Specify power and fail-over options for the uplink

- **Advanced Settings** - Specify connection timeout period for the uplink

Device Settings



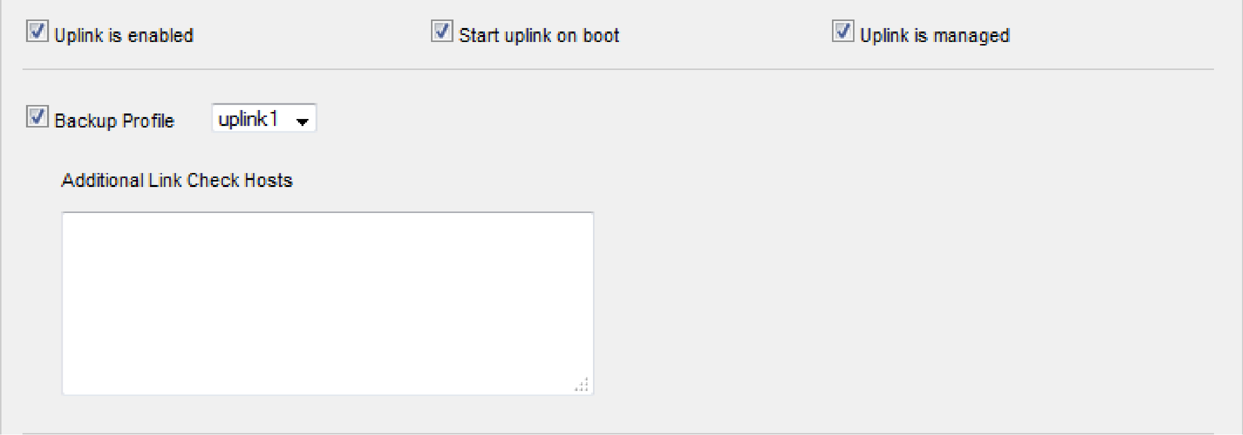
Default gateway * 192.168.200.25

Primary DNS * 192.168.200.5

Secondary DNS 192.168.200.10

- Default Gateway - Enter the IP address or hostname of the default gateway device for this uplink in the 'Default Gateway' text box
- Primary DNS and Secondary DNS - Enter the IP addresses/hostnames of the primary and secondary DNS servers to be used.

Uplink Settings



☑ Uplink is enabled ☑ Start uplink on boot ☑ Uplink is managed

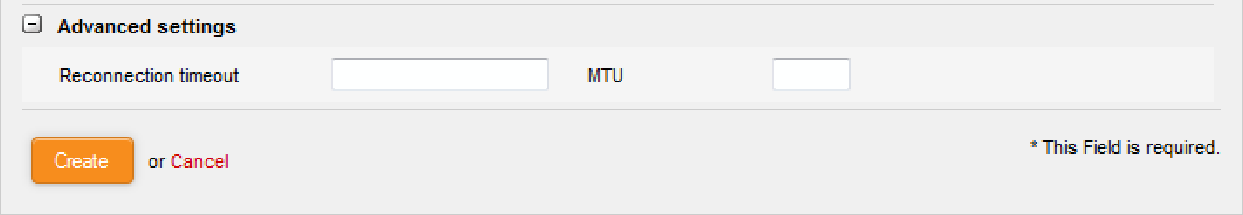
☑ Backup Profile uplink1

Additional Link Check Hosts

- Uplink is Enabled - The uplink will be activated immediately after it is created. Deselect this if you don't want to enable the uplink device at this time. You can enable the uplink later in two ways:
  - Interface configuration screen - Enable the port in the **Interface Configuration screen**
  - Dashboard - Enable the 'Active' checkbox beside the uplink in the 'Uplinks' box. See the **section explaining the Uplinks box** in the '**Dashboard**' for more details.
- Start uplink on boot - The uplink will start automatically on every restart of the DFW virtual appliance. Deselect this checkbox if you want to manually start the uplink only when required.
- Uplink is managed - The uplink will be managed by Dome Firewall and its details will be displayed in the Dashboard. Deselect this option if you do not want the uplink details to be displayed in the Dashboard. You can switch the uplink to managed state at any time by selecting the 'Managed' checkbox beside the uplink in the Dashboard. See the **section explaining the Uplinks box** in the '**Dashboard**' for more details.
- Backup Profile - Select this checkbox if you want to specify an alternative uplink connection to be activated in the event this uplink fails and choose the alternative uplink device from the drop-down.

Advanced Settings

The Advanced Settings pane allows administrators to configure the reconnection time out period. These settings are only for advanced users, hence the pane is not displayed by default. To open this panel, click the '+' button next to 'Advanced Settings'.



   - **Reconnection timeout** - Specify the maximum time period (in seconds) that the uplink should attempt to reconnect in the event of a connection failure. The reconnection timeout period depends on the ISP configuration. If you are unsure, leave this field blank.
   - **MTU** - Enter the Maximum Transmission Unit (MTU) of the data packets that can be sent over the network. (Optional)
- Click 'Create' after configuring the parameters. The uplink will be added to the **Additional Gateway Uplinks interface**. You can enable/disable the uplink at any time from this interface.

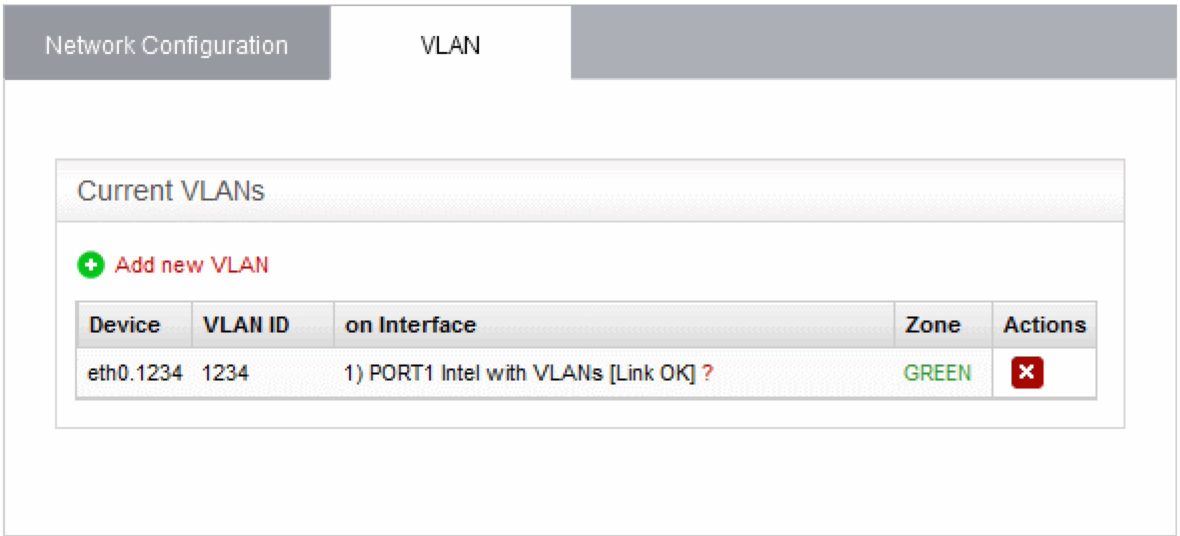
6.1.3 Creating VLANs

Comodo Dome Firewall allows administrators to create Virtual LAN interface devices associated with network zone(s). The devices can be associated with arbitrary VLAN IDs. VLAN interface devices provide an additional layer of separation from other network devices. They enable clients from different locations to be connected to a single LAN, separated from local network zones.

The 'VLAN' tab displays a list of current VLAN interface devices and allows the administrator to add or remove devices.

To access the VLAN manager interface

- Click 'Network' > 'Interfaces' from the left hand side navigation
- Click the 'VLAN' tab.



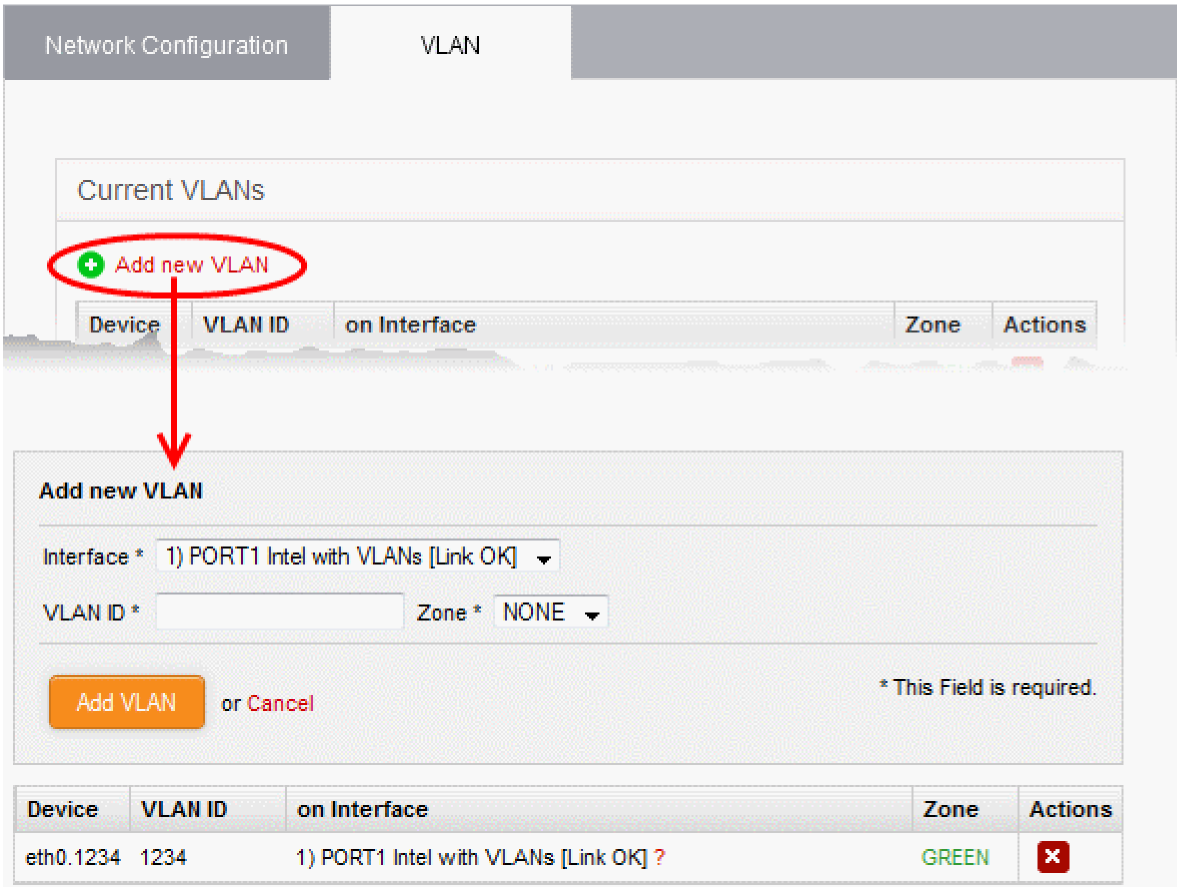
Device	VLAN ID	on Interface	Zone	Actions
eth0.1234	1234	1) PORT1 Intel with VLANs [Link OK] ?	GREEN	✖

VLANs Table - Column Descriptions	
Column	**Description**
Device	The identity of the VLAN interface device. The device ID is of the format ethX.y, where 'X' is the identification number of the physical interface to which the VLAN interface is associated and 'y' is the VLAN ID.

VLAN ID	The identification number of the VLAN
On Interface	The physical interface to which the VLAN is associated
Zone	Indicates the network zone to which the VLAN interface is associated Green - Local network zone (for example, a LAN) Orange - DMZ Blue - Wi-Fi network zone
Actions	Displays control buttons for deleting the VLAN interface device. ☒ - Removes the VLAN.

To add a new VLAN interface device

- Click the 'Add new VLAN' link from the top left of the VLAN manager interface. The 'Add new VLAN' pane will open.



Interface * 1) PORT1 Intel with VLANs [Link OK]

VLAN ID * Zone * NONE

* This Field is required.

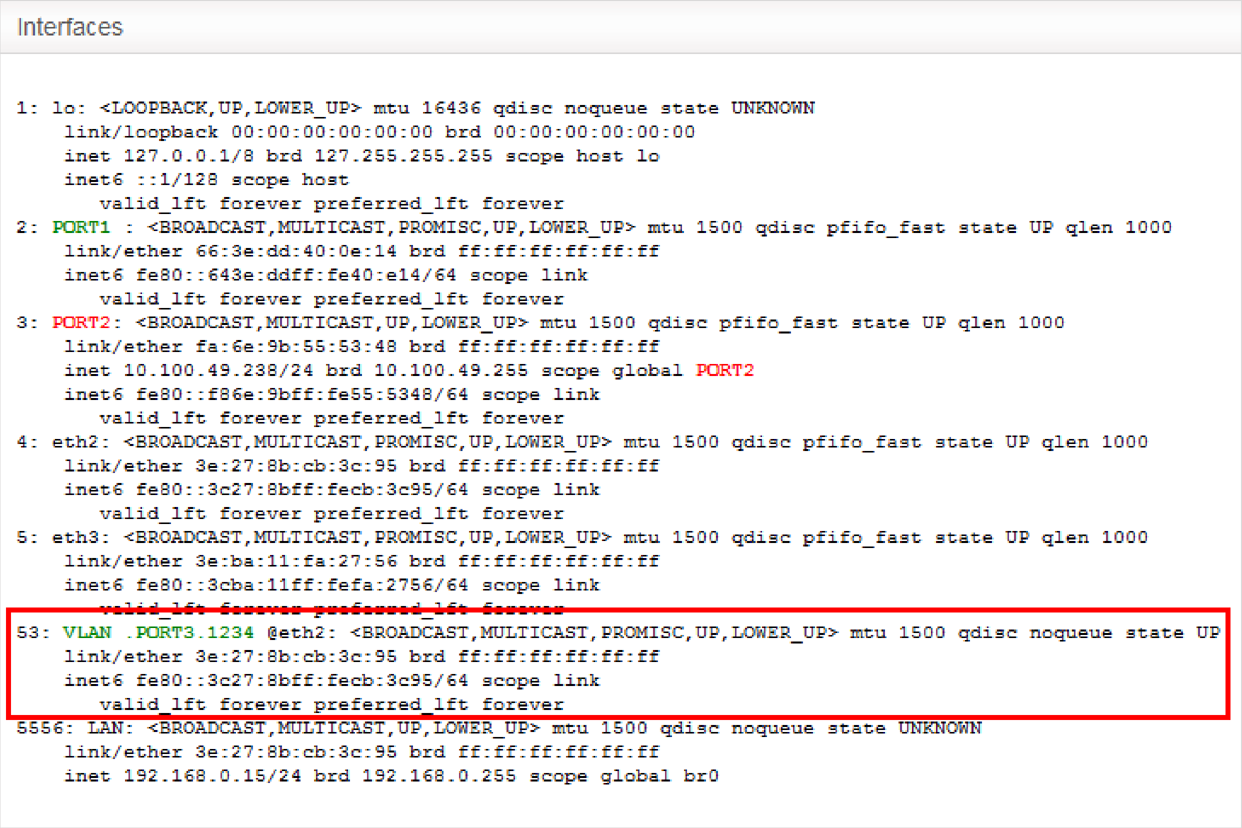
Device	VLAN ID	on Interface	Zone	Actions
eth0.1234	1234	1) PORT1 Intel with VLANs [Link OK] ?	GREEN	☒

- Enter the parameters as given below:
  - **Interface** - The drop-down displays all configured interfaces connected to the DFW virtual appliance, with their link status. Choose the interface to which the VLAN interface device should be connected.
  - **VLAN ID** - Assign an ID for the VLAN. The ID can be from '0' to '4095'
  - **Zone** - The drop-down displays the network zones that were enabled in the Network > Interfaces interface. Select the network zone to which the VLAN should be associated.

Note: You can create a VLAN associated to a zone and connected to the interface that already serves the same zone. It is not possible to associate a VLAN to a zone and connect it to an interface that serves a different zone. For example, if eth0 serves Green LAN zone, you cannot associate a VLAN to blue Wi-Fi zone and connect it to eth0.

- Click 'Add VLAN' to create the VLAN.

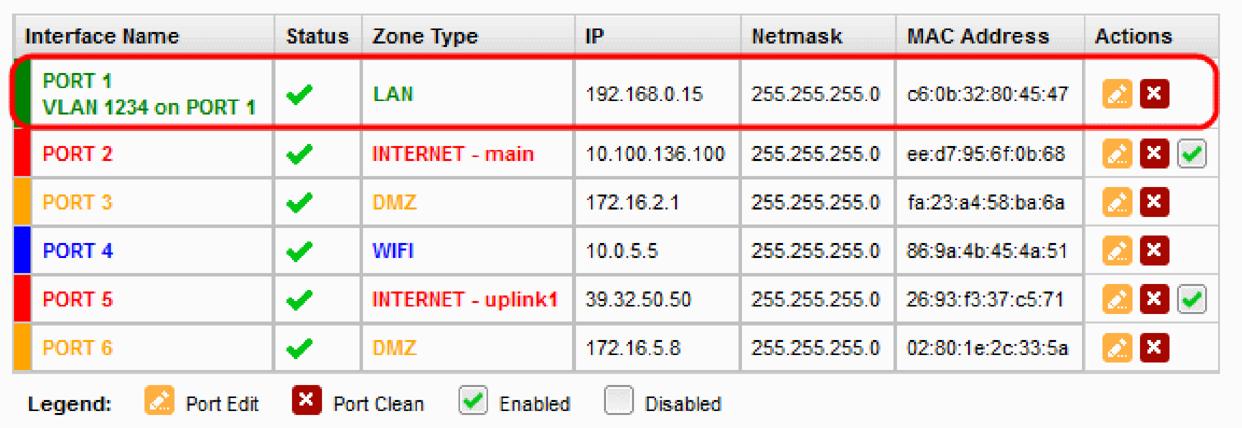
Once created, the VLAN interface device will be displayed as a interface device in the list of VLANs. It will also be shown in other areas of the administrative console like Status > Network Status, with the extension of the VLAN ID in the interface ID.



Interfaces

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: PORT1 : <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 66:3e:dd:40:0e:14 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::643e:ddff:fe40:e14/64 scope link
       valid_lft forever preferred_lft forever
3: PORT2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether fa:6e:9b:55:53:48 brd ff:ff:ff:ff:ff:ff
    inet 10.100.49.238/24 brd 10.100.49.255 scope global PORT2
    inet6 fe80::f86e:9bff:fe55:5348/64 scope link
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 3e:27:8b:cb:3c:95 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::3c27:8bff:fecb:3c95/64 scope link
       valid_lft forever preferred_lft forever
5: eth3: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 3e:ba:11:fa:27:56 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::3cba:11ff:fefa:2756/64 scope link
       valid_lft forever preferred_lft forever
53: VLAN .PORT3.1234 @eth2: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 3e:27:8b:cb:3c:95 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::3c27:8bff:fecb:3c95/64 scope link
       valid_lft forever preferred_lft forever
5556: LAN: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 3e:27:8b:cb:3c:95 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.15/24 brd 192.168.0.255 scope global br0
```

The device can be assigned to new network zones in the 'Network' > 'Interfaces' interface.



Interface Name	Status	Zone Type	IP	Netmask	MAC Address	Actions
PORT 1 VLAN 1234 on PORT 1	✓	LAN	192.168.0.15	255.255.255.0	c6:0b:32:80:45:47	✎ ☒
PORT 2	✓	INTERNET - main	10.100.136.100	255.255.255.0	ee:d7:95:6f:0b:68	✎ ☒ ☑
PORT 3	✓	DMZ	172.16.2.1	255.255.255.0	fa:23:a4:58:ba:6a	✎ ☒
PORT 4	✓	WIFI	10.0.5.5	255.255.255.0	86:9a:4b:45:4a:51	✎ ☒
PORT 5	✓	INTERNET - uplink1	39.32.50.50	255.255.255.0	26:93:f3:37:c5:71	✎ ☒ ☑
PORT 6	✓	DMZ	172.16.5.8	255.255.255.0	02:80:1e:2c:33:5a	✎ ☒

Legend: ✎ Port Edit ☒ Port Clean ☑ Enabled □ Disabled

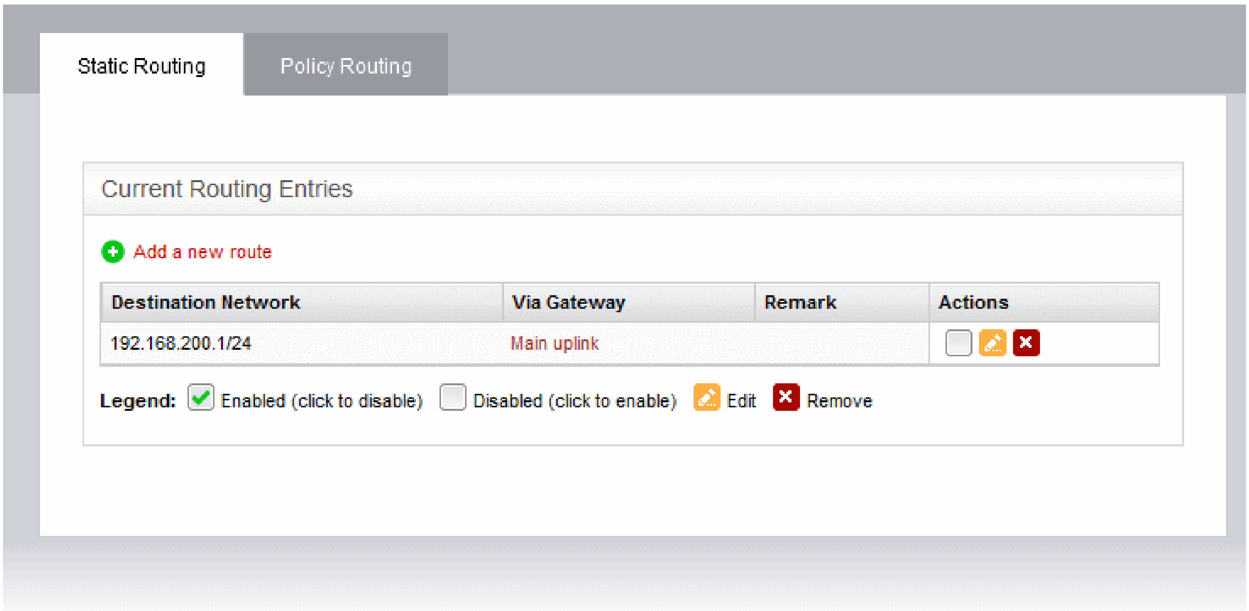
6.2 Routes

The DFW virtual appliance maintains a default routing table for routing traffic between different network zones as per the network configuration. The default routing table can be viewed from the 'Network status Information' interface accessible by clicking Status > Network status. In addition to the default routing table, the administrator can create custom routes to connect to other networks through other devices like external routers or VPN tunnels.

Two types of custom routes can be created:

- Static Routes - The static route defines a custom route between a specific source network and a specific destination network through a specific gateway or uplink.
- Policy Routes - A rule that defines the route between specific network addresses, zones, or services (expressed as port and protocol) and a specific uplink.

Custom routes can be added and managed through the 'Routes' interface ('Network' > 'Routing'):



Destination Network	Via Gateway	Remark	Actions
192.168.200.1/24	Main uplink		

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) Edit ☒ Remove

The interface contains two tabs:

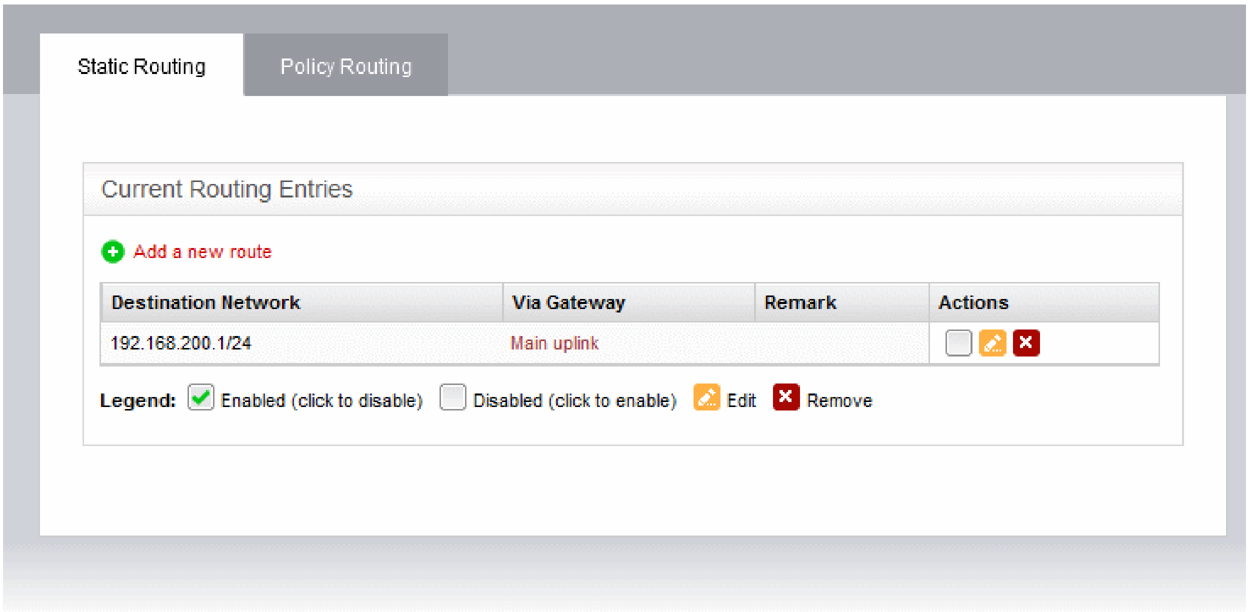
- **Static Routing** - Displays a list of existing static routes and allows administrators to add new static routes. See **Adding and Managing Static Routes** for more details.
- **Policy Routing** - Displays a list of existing policy routing rules and allows administrators to add new rules. See **Adding and Managing Policy Routing Rules** for more details.

6.2.1 Adding and Managing Static Routes

The 'Static Routing' interface displays a list of existing static routes to any source network to specific destination networks. New rules can be added by clicking the 'Add a new route' link. Existing rules can be enabled, disabled, edited or removed by using the controls in the 'Actions' column.

To open the 'Static Routing' interface

- Click 'Network' > 'Routing' from the left hand side navigation.
- Click the 'Static Routing' tab


Static Routing
Policy Routing
Current Routing Entries
Add a new route

Destination Network	Via Gateway	Remark	Actions
192.168.200.1/24	Main uplink		□ ✎ ☒

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

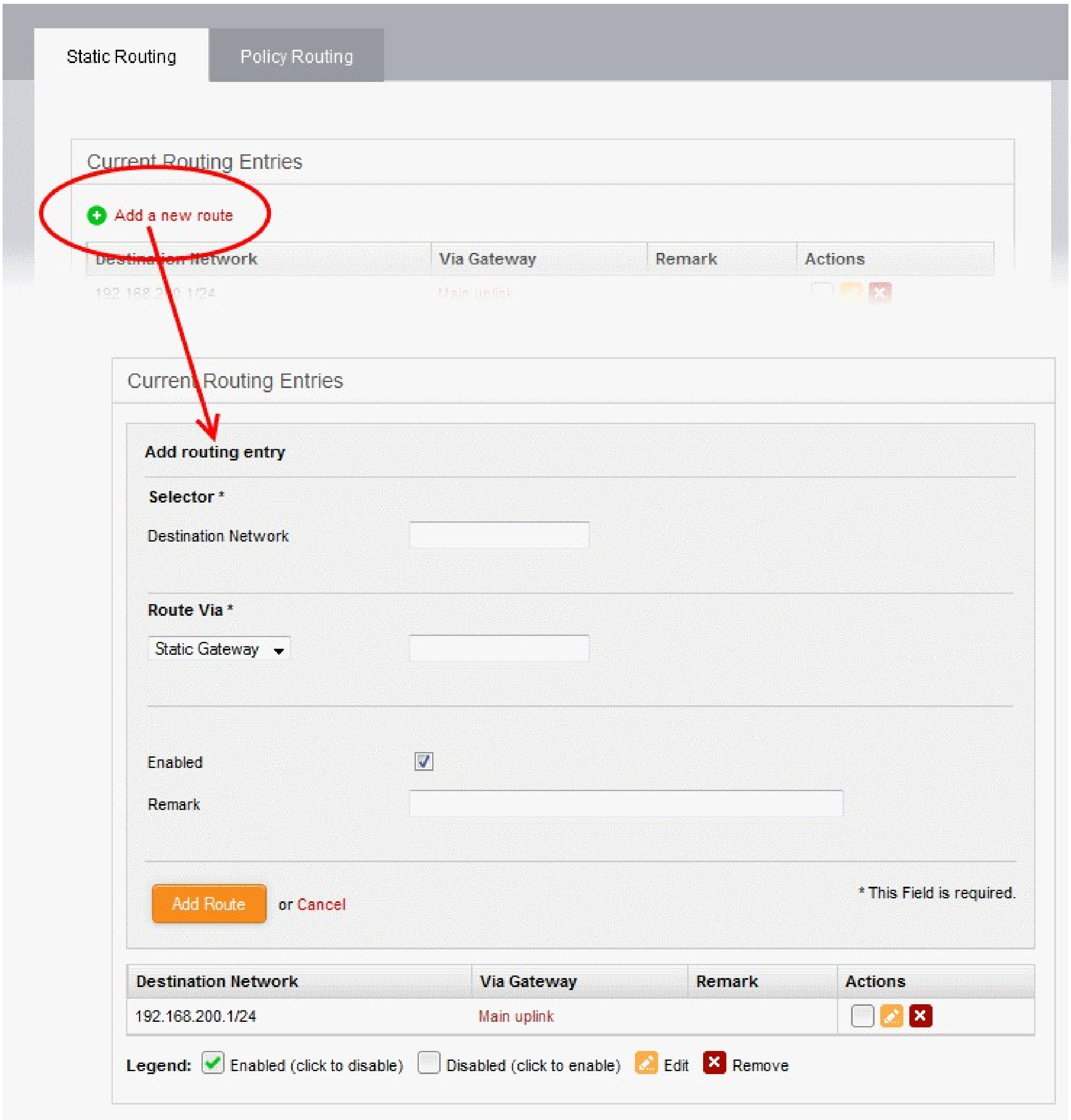
Static Routing Table - Column Descriptions	
Column	**Description**
Destination Network	The traffic destination network defined for the route. This can be an external network or an internal network zone.
Via Gateway	The traffic between the defined source and destination networks will be passed through the gateway specified here. This can be a static gateway, an uplink connected to the virtual appliance or an SSL VPN user.
Remark	A shot description of the route as entered by the administrator during creation.
Actions	Displays control buttons for enabling/disabling and editing the route. ☑ - Allows administrators to enable or disable the route. A tick in the checkbox indicates that the route is enabled. ✎ - Edit the route entry. ☒ - Removes the route. **Note**: On clicking the 'Remove' button, the route entry will be immediately deleted without requesting confirmation. This is action is irreversible so if you accidentally delete an entry, you need to manually re-add it.

The following sections provide detailed guidance on:

- **Adding a new static route entry**
- **Editing an existing static route entry**

To add a new static route entry

- Click the 'Add a new route' link from the top left of the 'Static Routing' interface. The 'Adding Routing entry' pane will open.



Current Routing Entries

Add routing entry

Selector *

Destination Network

Route Via *

Static Gateway ▾

Enabled ☑

Remark

* This Field is required.

Destination Network	Via Gateway	Remark	Actions
192.168.200.1/24	Main uplink		□ ✎ ✕

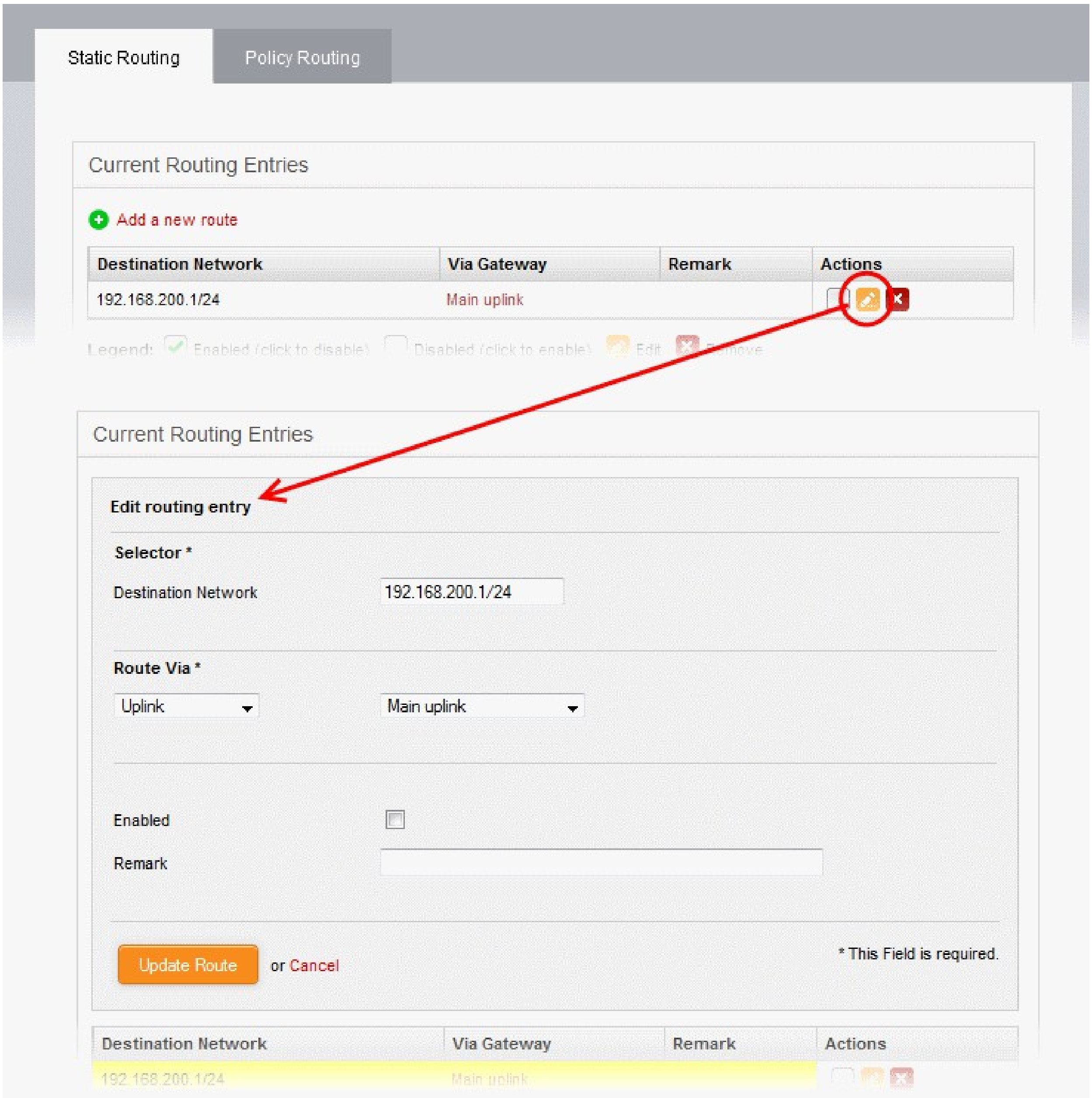
Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ✕ Remove

- - **Destination Network** - Specify the network range of the destination network in CIDR notation, e.g. 192.168.200.01/24. To specify the source network as any network, leave the field blank.
  - **Route Via** - Choose the route gateway for traffic between the source and destination networks. Available options are:
    - Static Gateway - Specify the IP address of the router in the text box on the right.
    - Uplink - Choose the uplink to be used, from the uplink interfaces connected to the virtual appliance, from the drop-down at the right.
    - SSL VPN User - Choose the SSL VPN client to be used from the drop-down on the right
  - **Enabled** - Deselect if you do not want the route to be enabled after you click the 'Add Route' button. The route can be enabled/disabled at anytime from the Static Routing Editor interface.
  - **Remark** - Enter a short description for the route. The description will appear in the 'Remark' column in the list of routes.
- Click 'Add Route' to save your changes.

Example: If you want the virtual appliance to connect to an external network, which in turn is connected to a router in the local area network, then enter the IP address range of the external network in the Destination field, select Static Gateway for 'Route Via' and enter the IP address of the router as assigned in the LAN in the 'Static Gateway' field.

To edit a static route entry

- Click the Edit button ✎ in the row of the route entry to be edited.



Current Routing Entries

Add a new route

Destination Network	Via Gateway	Remark	Actions
192.168.200.1/24	Main uplink		□ ✎ ✕

Legend: ✓ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ✕ Remove

Current Routing Entries

Edit routing entry

Selector *

Destination Network: 192.168.200.1/24

Route Via *

Uplink ▾ Main uplink ▾

Enabled □

Remark

* This Field is required.

Destination Network	Via Gateway	Remark	Actions
192.168.200.1/24	Main uplink		□ ✎ ✕

- The Edit interface is similar to 'Add Routing Entry' interface. Edit the details as required and click 'Update Route'. Refer to the **section above** for more details

The new details will be saved and activated on the next restart of the service.

6.2.2 Adding and Managing Policy Routing Rules

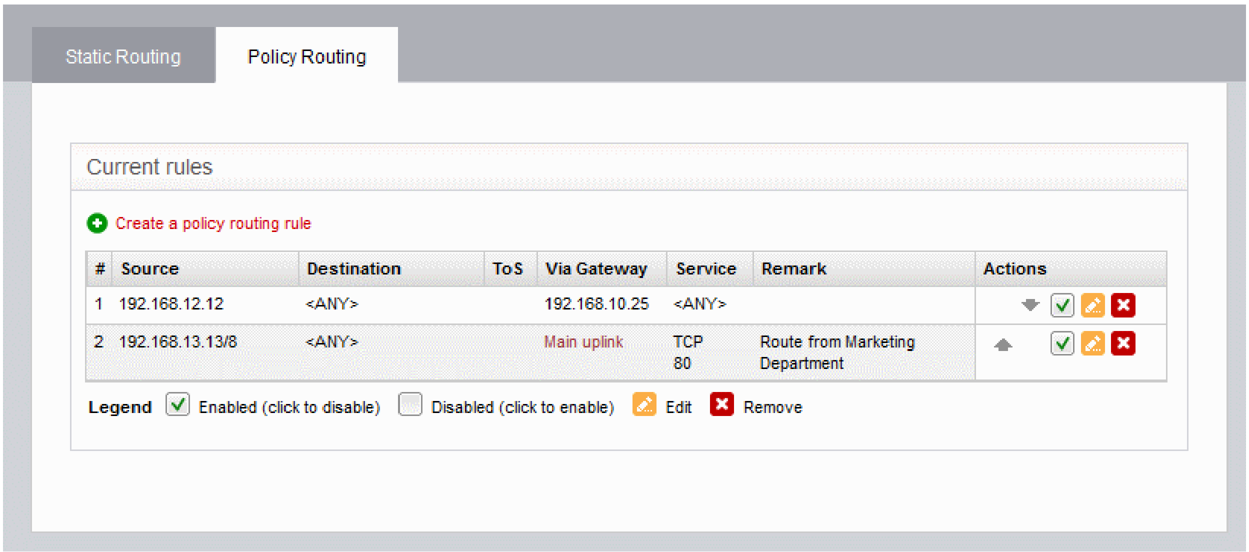
The 'Policy Routing' interface displays a list of all pre-configured static routes and policy routing rules with their configuration parameters.

Policy routing rules can be added to route traffic from specified external networks, zones, interfaces, VPN users or clients to specified network zones or VPN users, for specific services/protocols. Rules can be precisely configured for passing packets with specific Type of Service parameter.

The administrator can create new policy routing rules by defining source and destination networks, gateway, services and type of services and edit existing rules. You can covert static routes (those with only source and destination) into a routing rule by adding parameters like Type of Service (TOS) and Service/Port in this interface.

To open the 'Policy Routing' interface

- Click 'Network' > 'Routing' from the left hand side navigation.
- Click the 'Policy Routing' tab.



Current rules

Create a policy routing rule

#	Source	Destination	ToS	Via Gateway	Service	Remark	Actions
1	192.168.12.12	<ANY>		192.168.10.25	<ANY>		▼ ☑ ✎ ☒
2	192.168.13.13/8	<ANY>		Main uplink	TCP 80	Route from Marketing Department	▲ ☑ ✎ ☒

Legend ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Policy Routing Editor Table - Column Descriptions	
Column	**Description**
Source	The network from which traffic will originate for this rule. This can be an internal network zone or an external network.
Destination	The network to which traffic covered by this rule will be sent. This can be an external network or an internal network zone.
ToS	The Type of Service parameter defined for the route to filter the filter to pass through. See the section '**Note on TOS**' below the table for more details.
Via Gateway	The traffic between the defined source and destination networks will be passed through the gateway specified here. This can be a static gateway, an uplink connected to the virtual appliance or an SSL VPN user.
Service	The network service, protocol and the destination port defined for the rule
Remark	A shot description of the route as entered by the administrator during creation.
Actions	Displays control buttons for enabling/disabling and editing the rule. ▲ / ▼ - The arrows allow the administrator to move the rule up or down to change its priority. ☑ - Allows the administrator to enable or disable the rule. A tick in the checkbox indicates that the rule is enabled. ✎ - Edit the rule. ☒ - Removes the rule. Note: On clicking the 'Remove' button, the route entry will be immediately deleted without requesting confirmation. This is action is irreversible so if you accidentally delete an entry, you need to manually re-add it.

Note on ToS - The Type of Service (ToS) is a eight bit field in the header of an IPv4 packet for managing the routing of the datagram packet between its source and the destination depending on is priority, latency, throughput and reliability. The ToS value can be from:

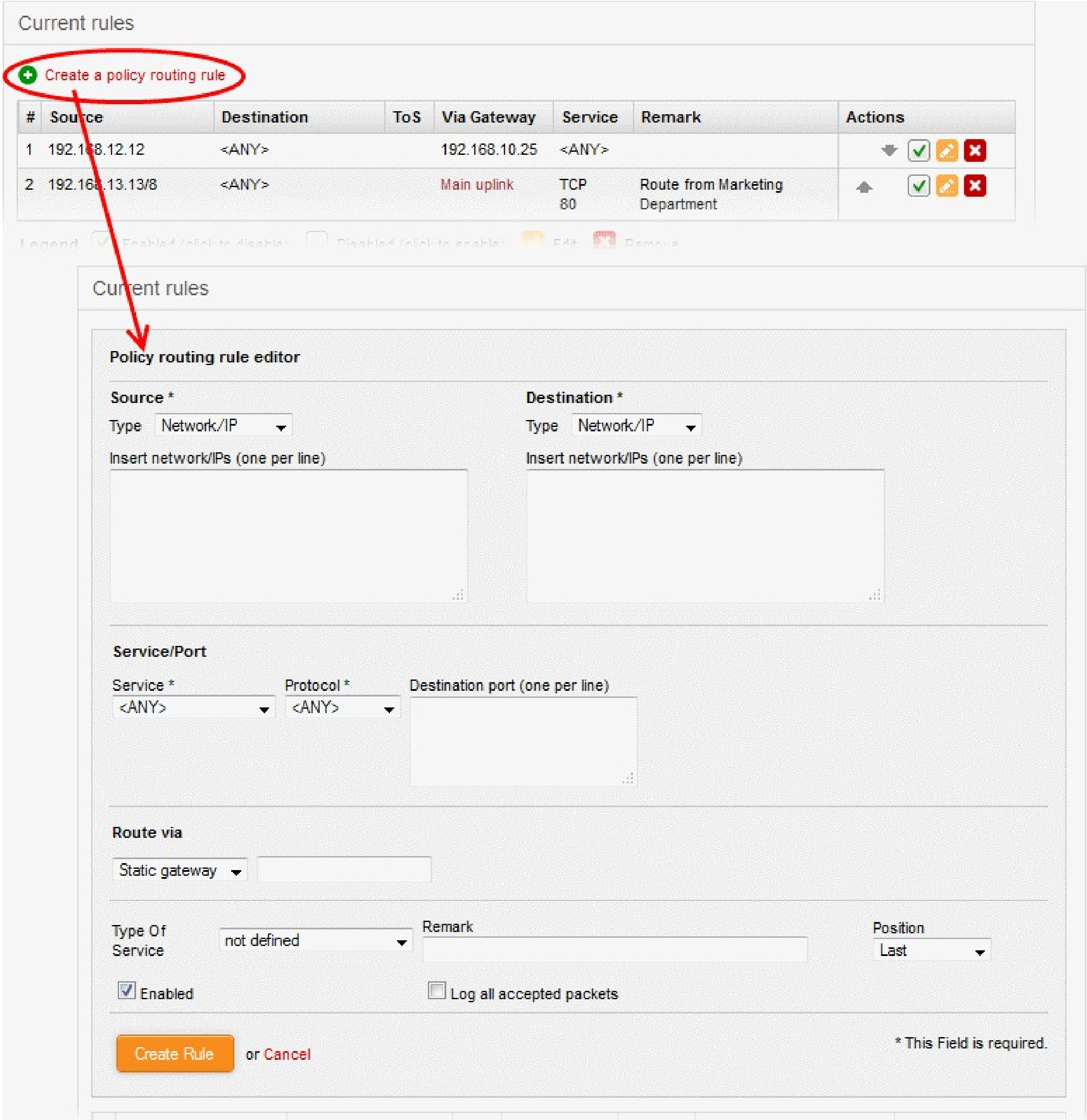
- Eight priority values for Class Selectors (CS0-7), which denote backward compatibility with the TOS field. In other words, these are 'true' TOS values.
- Twelve latency values for Assured Forwarding (AF*xy*, where x being a class from 1 to 4 and y being a 'drop precedence' from 1 to 3 - low, medium, high) that provide low packet loss with minimum guarantees about latency.
- One reliability value for Expedited Forwarding (EF PHB), defined in RFC 3246 and used to give the highest priority to packets. It is useful for services requiring low delay, low latency, and low rate of losses, like e.g., VoIP or video streaming.

The following sections provide detailed guidance on:

- **Adding a new policy routing rule**
- **Editing an existing static route entry** or policy routing rule

To add a new policy routing rule

- Click the 'Create a policy routing rule' link from the top left of the 'Policy Routing' interface. The 'Policy routing rule editor' pane will open.



Current rules

Create a policy routing rule

#	Source	Destination	ToS	Via Gateway	Service	Remark	Actions
1	192.168.12.12	<ANY>		192.168.10.25	<ANY>		▼ ✓ ✎ ✖
2	192.168.13.13/8	<ANY>		Main uplink	TCP 80	Route from Marketing Department	▲ ✓ ✎ ✖

Legend: ✓ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ✖ Remove

Current rules

Policy routing rule editor

Source *
Type: Network/IP
Insert network/IPs (one per line)

Destination *
Type: Network/IP
Insert network/IPs (one per line)

Service/Port
Service * <ANY>
Protocol * <ANY>
Destination port (one per line)

Route via
Static gateway

Type Of Service: not defined
Remark
Position: Last

☑ Enabled
□ Log all accepted packets

Create Rule or Cancel

* This Field is required.

- The following parameters can be configured:
    - **Source** - Select the type of source from the 'Type' drop-down and specify the source in the text box below it. The options available are:
        - Any - The rule will be applied to traffic from any source
        - Zone/Interface - Select this option if the source is a network zone or an Interface connected to the virtual appliance. Choose the network zone and/or the interface from the options listed in the text box. Press and hold the Ctrl key in the keyboard to choose multiple zones/interfaces.
        - SSL VPN User - Select this option if the rule is to be applied to traffic from VPN user(s) added to the network. Choose user(s) from the list of pre-registered users displayed in the textbox. Press and hold the Ctrl key in the keyboard to choose VPN users.
        - Network/IP - Select this option if the rule is to be applied to traffic from an external network or from a specific IP address. Enter the IP address of the network(s) in CIDR notation or the specific IP address(es) in the text box, as one entry per line.
        - MAC - Select this option if the rule is to be applied to traffic from specific clients. Enter the MAC address(es) in the text box, with one entry per line.

- **Destination** - Select the type of destination for the traffic from the 'Type' drop-down and specify the actual destination in the text box below it. The options available are:
    - Any - The rule will be applied to traffic going any destination
    - SSL VPN User - Select this option if the rule is to be applied to traffic to VPN user(s) which have been added to the network. Choose user(s) from the list of pre-registered users displayed in the text-box. Press and hold the Ctrl key in the keyboard to choose VPN users.
    - Network/IP - Select this option if the rule is to be applied to traffic to an external network or to a specific IP address. Enter the IP address of the network(s) in CIDR notation or the specific IP address(es) in the text box, as one entry per line.
- **Service/Port** - Specify the service, protocol and destination port for the rule when the TCP, UDP, or TCP + UDP protocols are selected.
    - Service - Select the service for which the rule to be applied from the drop-down.
    - Protocol - Select the protocol for the service. Usually this field will be auto selected based on the service selected.
    - Destination port - Select the destination port for the service. Usually this field will be auto selected based on the service selected.

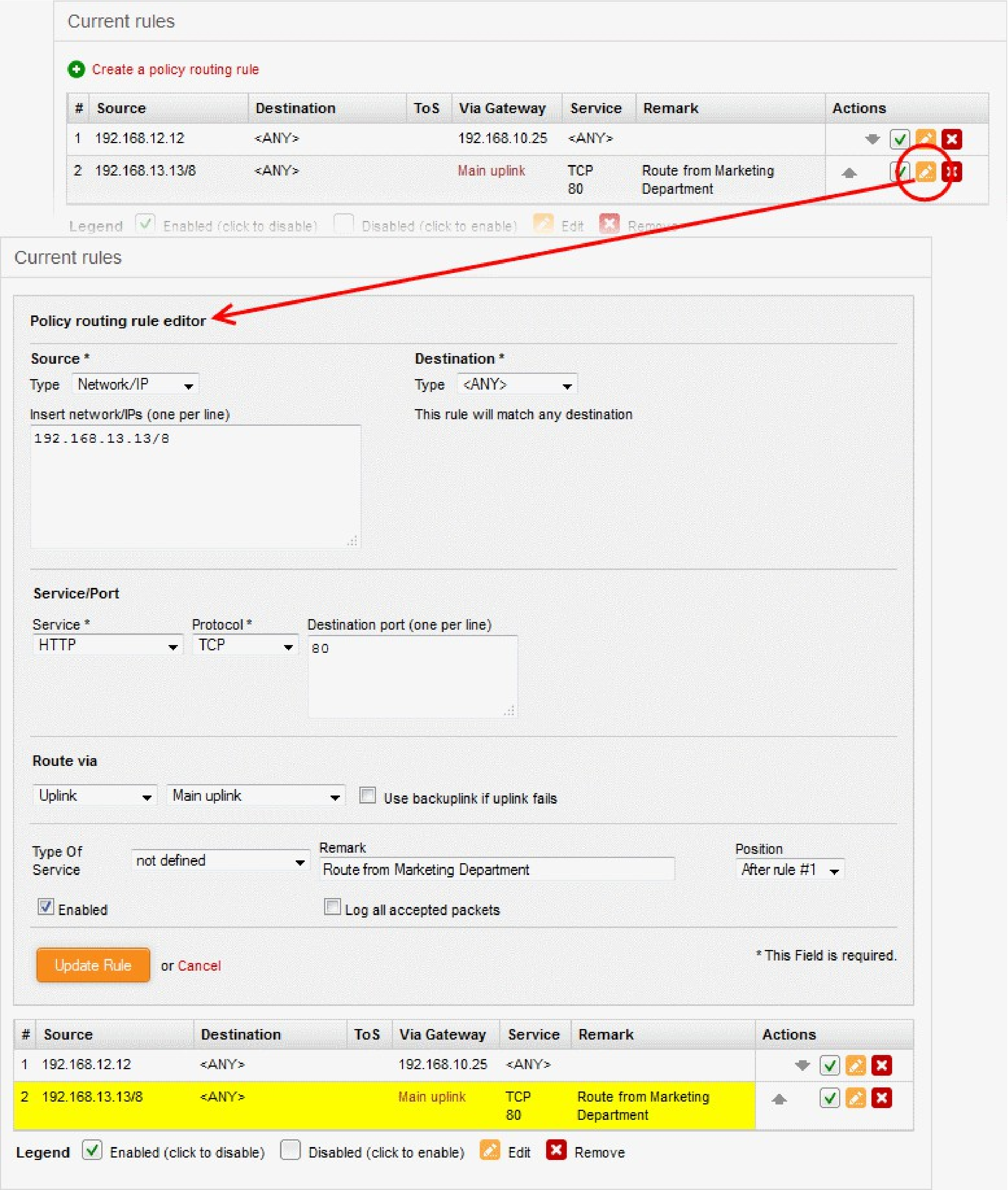
Tip: The virtual appliance is loaded with predefined combinations of service/protocol/port, like HTTP/TCP/80, <ALL>/TCP+UDP/0:65535, or <ANY>, which is a shortcut for all services, protocols, and ports. If you want to specify custom protocol/port combination, then select 'User Defined' from the service. This useful for the services run on ports different from the standard ones.

- **Route Via** - Choose the route gate way for the traffic between the source and destination from the drop-down. The options available are:
    - Static Gateway - Specify the IP address of the router in the text box at the right.
    - Uplink - Choose the uplink to be used, from the uplink interfaces connected to the virtual appliance, through the drop-down at the right.
    - SSL VPN User - Choose the SSL VPN client to be used from the drop-down at the right
- **Type of Service** - Choose the ToS parameter for the rule. For more details on ToS, refer to the note above.
- **Remark** - Enter a short description for the rule. The description will appear in the Remark column in the list of rules.
- **Position** - Select the priority of the rule from the drop-down.
- **Enabled** - Deselect if you do not want the rule to be enabled upon creation. The rule can be enabled/disabled at anytime from the Policy Routing Editor interface.
- **Log all accepted packets** - Select the checkbox if you want all the packets passed through the routing rule.

- Click 'Create Rule' to add your new rule to the virtual appliance.

To edit a policy routing rule

- Click the Edit button ✎ in the row of the rule you want to edit. The 'Policy routing rule editor' pane will open.



Current rules

Create a policy routing rule

#	Source	Destination	ToS	Via Gateway	Service	Remark	Actions
1	192.168.12.12	<ANY>		192.168.10.25	<ANY>		↓ ☑ ✎ ☒
2	192.168.13.13/8	<ANY>		Main uplink	TCP 80	Route from Marketing Department	↑ ☑ ✎ ☒

Legend ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Current rules

Policy routing rule editor

Source *

Type: Network/IP

Insert network/IPs (one per line)

192.168.13.13/8

Destination *

Type: <ANY>

This rule will match any destination

Service/Port

Service *: HTTP

Protocol *: TCP

Destination port (one per line): 80

Route via

Uplink: Main uplink □ Use backuplink if uplink fails

Type Of Service: not defined

Remark: Route from Marketing Department

Position: After rule #1

☑ Enabled

□ Log all accepted packets

Update Rule or Cancel

* This Field is required.

#	Source	Destination	ToS	Via Gateway	Service	Remark	Actions
1	192.168.12.12	<ANY>		192.168.10.25	<ANY>		↓ ☑ ✎ ☒
2	192.168.13.13/8	<ANY>		Main uplink	TCP 80	Route from Marketing Department	↑ ☑ ✎ ☒

Legend ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

- Edit the details as required and click 'Update Rule'. Refer to the **section above** for more details

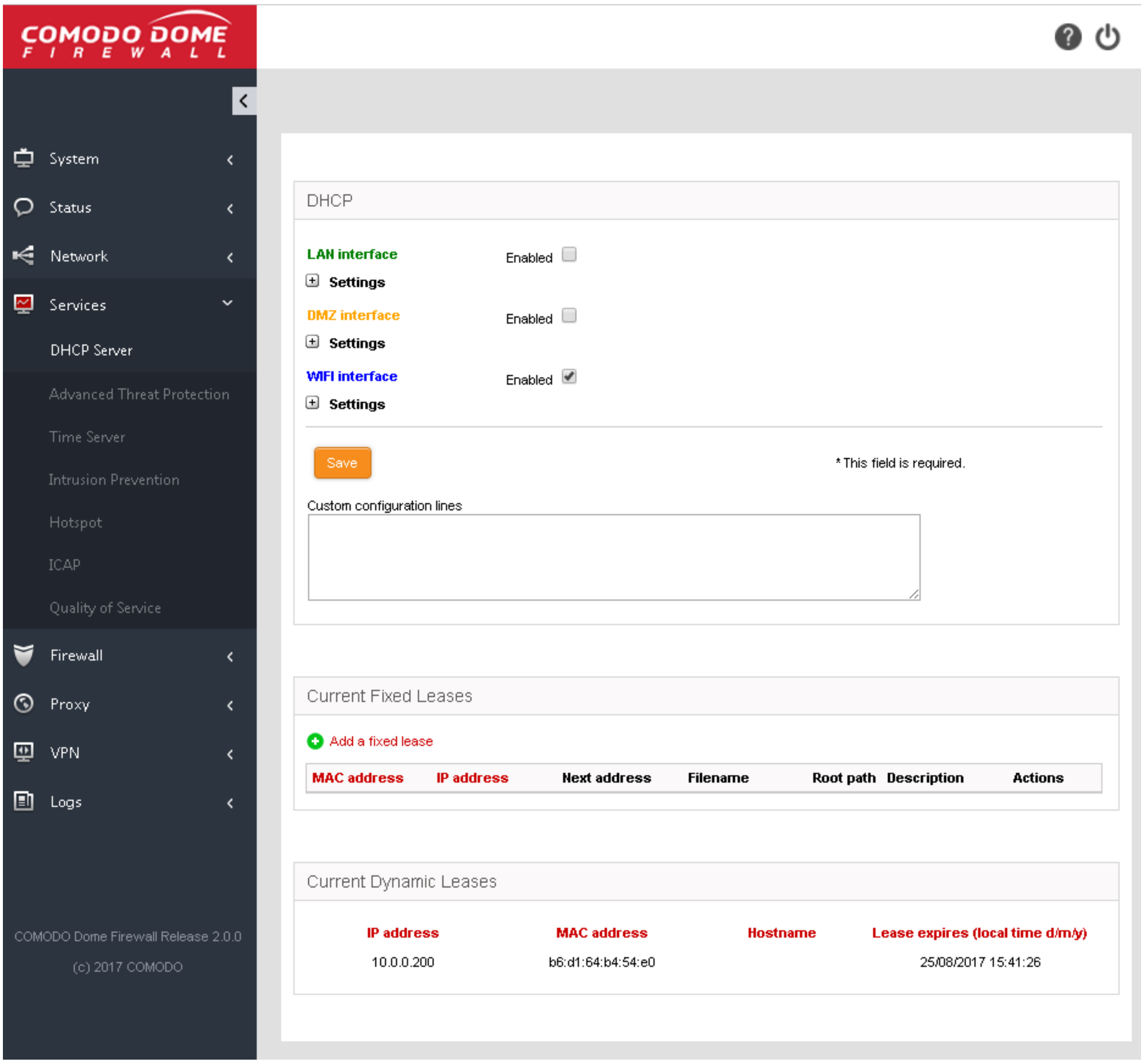
The new details will be saved and activated on the next restart of the service.

7 Configuring DFW Virtual Appliance Services and Protection Settings

- Click 'Services' in the left-hand menu to open a configure all Dome Firewall services.

The 'Services' menu contains a range of basic and advanced services to prevent threats, monitor network zones and help you manage and control your network. Click the following links to find out more about each:

- **DHCP Server** - Configure a Dynamic Host Control Protocol (DHCP) server to assign dynamic or static IP addresses to clients connected to your network zones.
- **Advanced Threat Protection** - Define threat profiles, application containment settings, manage security software at remote endpoints, configure the AV engine and schedule AV scans
- **Time server** - Specify a network time server (NTS) and manually adjust/update time.
- **Intrusion Prevention System** - Configure Snort rules for use by the intrusion prevention system (IPS).
- **Hotspot** - Built-in Captive Portal Service for governing Wi-Fi hotspots on your network
- **ICAP** - Configure the ICAP protocol, which is designed to adapt content while traversing between internet and individual nodes via Dome Firewall.
- **Quality of Service** - Set priority for IP traffic used by different services. Allocate bandwidth to different services.



DHCP

LAN interface Enabled ☐
⊞ Settings

DMZ interface Enabled ☐
⊞ Settings

WIFI interface Enabled ☑
⊞ Settings

Save

* This field is required.

Custom configuration lines

Current Fixed Leases

Add a fixed lease

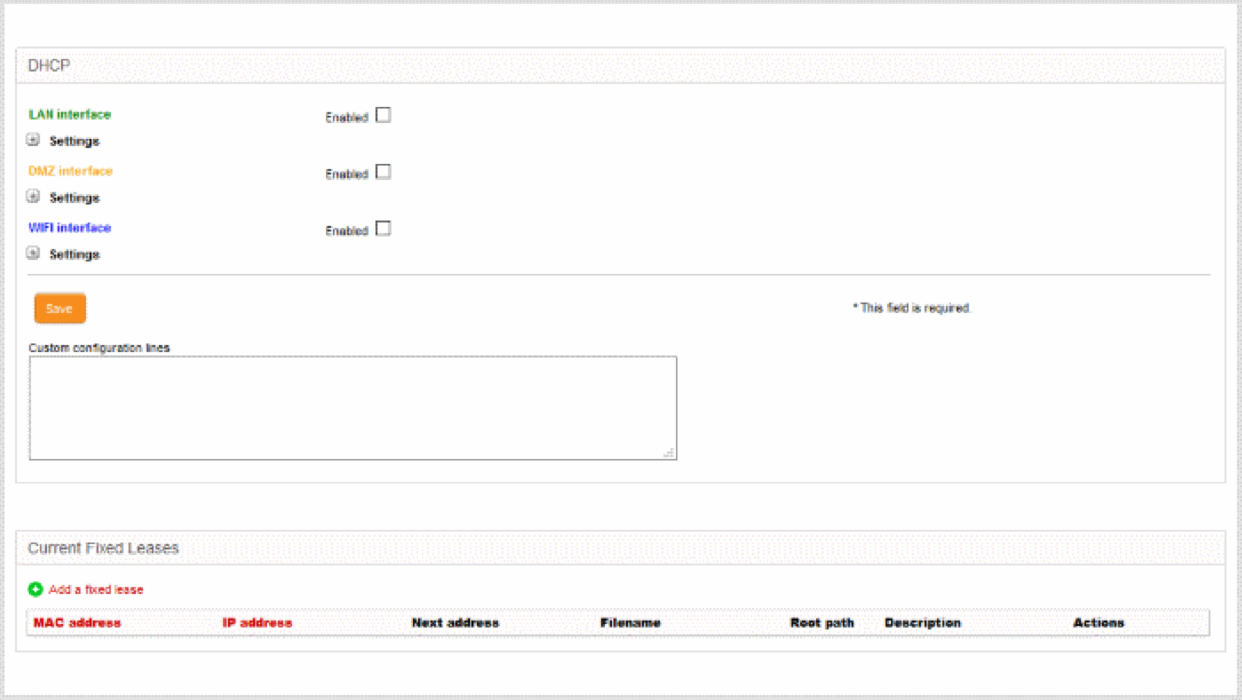
MAC address	IP address	Next address	Filename	Root path	Description	Actions

Current Dynamic Leases

IP address	MAC address	Hostname	Lease expires (local time d/m/y)
10.0.0.200	b6:d1:64:b4:54:e0		25/08/2017 15:41:26

7.1 DHCP Server

- Click 'Services' > 'DHCP Server' in the left-hand menu to open the DHCP Server interface
- The firewall has the ability assign fixed and dynamic IP addresses to workstations connected to different network zones.
- The DHCP Server area lets you configure the start and end IP addresses for each network zone and specify clients to which you want to assign addresses.
- The interface also allows granular configuration of DNS servers, NTP servers and WNS servers for each network zone.



DHCP

LAN interface Enabled □
⊞ Settings
DMZ interface Enabled □
⊞ Settings
WIFI interface Enabled □
⊞ Settings

* This field is required.

Custom configuration lines

Current Fixed Leases

MAC address	IP address	Next address	Filename	Root path	Description	Actions

The DHCP interface contains two panes:

- **DHCP**
- **Current fixed leases**

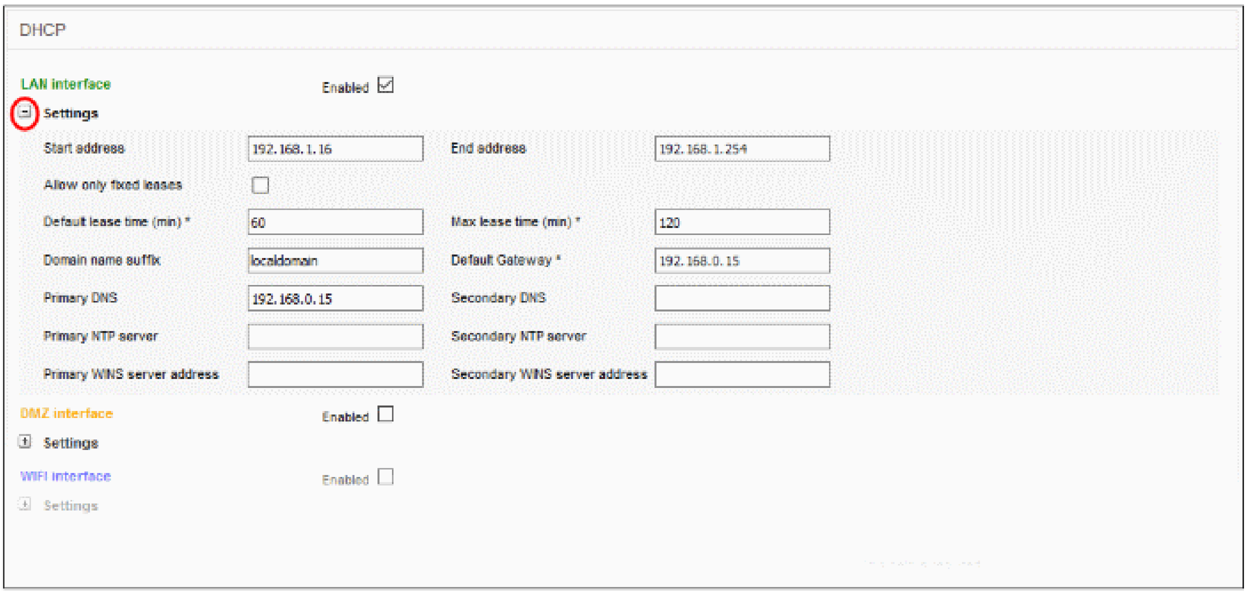
DHCP

The upper pane allows you to enable/disable the DHCP service and to configure DHCP settings for LAN, DMZ and Wi-Fi network zones.

To configure/edit the DHCP settings for a network zone

- Click the '+' button beside **Settings** under the network zone name.

The settings panel will open. The panel shows the start and end IP addresses of the range you want to dynamically assign to clients and servers in the selected zone.



DHCP

LAN interface Enabled ☑

⊟ Settings

Start address	192.168.1.16	End address	192.168.1.254
Allow only fixed leases	☐		
Default lease time (min) *	60	Max lease time (min) *	120
Domain name suffix	localdomain	Default Gateway *	192.168.0.15
Primary DNS	192.168.0.15	Secondary DNS	
Primary NTP server		Secondary NTP server	
Primary WINS server address		Secondary WINS server address	

DMZ interface Enabled ☐

⊞ Settings

WIFI interface Enabled ☐

⊞ Settings

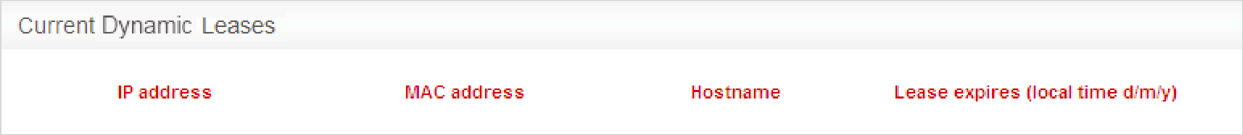
- Start Address and End Address - The first and last IP addresses of the IP address range that can be assigned to the clients connected to that network zone. The address range needs to be within the subnet, that can be assigned to that zone.

Note: Any client like a host, network printer or other network device connected to the selected zone will automatically obtain a valid IP address from the address range specified here, unless it is configured to get a fixed IP address in the lower pane. To enable a client to obtain the address automatically, it should be configured to to use DHCP in its network settings.

- Allow only fixed leases - When selected, no client in the selected zone will be automatically assigned a dynamic IP address. If required, the administrator can assign fixed IP addresses for each client from the lower panel
- Default lease time - The time in minutes for which the assigned IP address should be active on the client
- Max lease time - The maximum time (in minutes) for which the assigned IP address can be active on the client
- Domain name suffix - The domain name suffix to be passed on to the clients for local domain searches
- Default Gateway - The IP address of the default gateway used by the clients in the network zone. If left blank, the clients will use the DFW virtual appliance as the gateway
- Primary DNS and Secondary DNS - The IP addresses of the primary and secondary DNS servers. The defaults value is from the DNS cache of the DFW virtual appliance.
- Primary NTP server and Secondary NTP server - The IP address or the hostname of the Network Time Protocol (NTP) servers to be used by the clients in the network zone for time synchronization.
- Primary WINS server address and Secondary WINS server address - The IP addresses of the Windows Internet Name Service (WINS) servers the clients should use. This is required only for Microsoft Windows networks that use the WINS service.
- Custom Configuration Lines - Allows Advanced Users to add custom configuration lines for DHCP, e.g., custom routes to subnets
- Enabled - The checkbox allows you to enable or disable the DHCP settings for the selected zone.

- Enter/Edit the parameters as required and click 'Save'. The service will restart for your settings to take effect.
- Repeat the process for other network zones as required

Once a client(s) DHCP settings have been enabled and it has been auto-assigned IP addresses, the 'Current dynamic leases' pane will appear below the 'Current Fixed Leases' table. This displays the currently assigned dynamic IP address, the MAC address, the hostname and the expiry time of the address associated with each client.

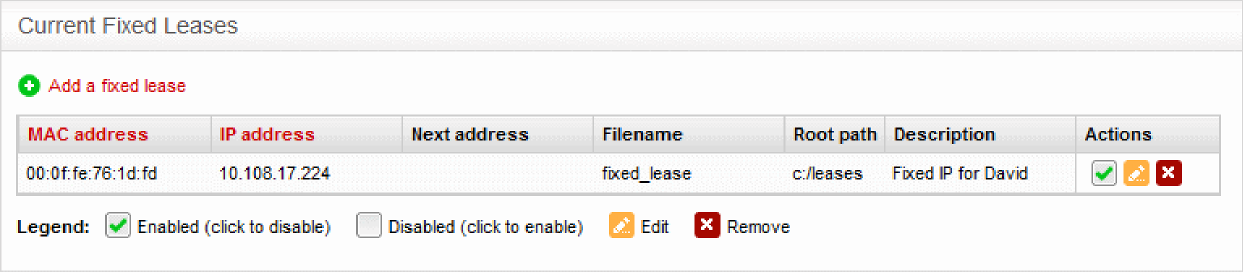


Current Dynamic Leases

IP address	MAC address	Hostname	Lease expires (local time d/m/y)

Current Fixed Leases

The 'Current Fixed Leases' pane displays a list of fixed IP addresses assigned to specific clients and allows you to add new fixed address specifications.



Current Fixed Leases

Add a fixed lease

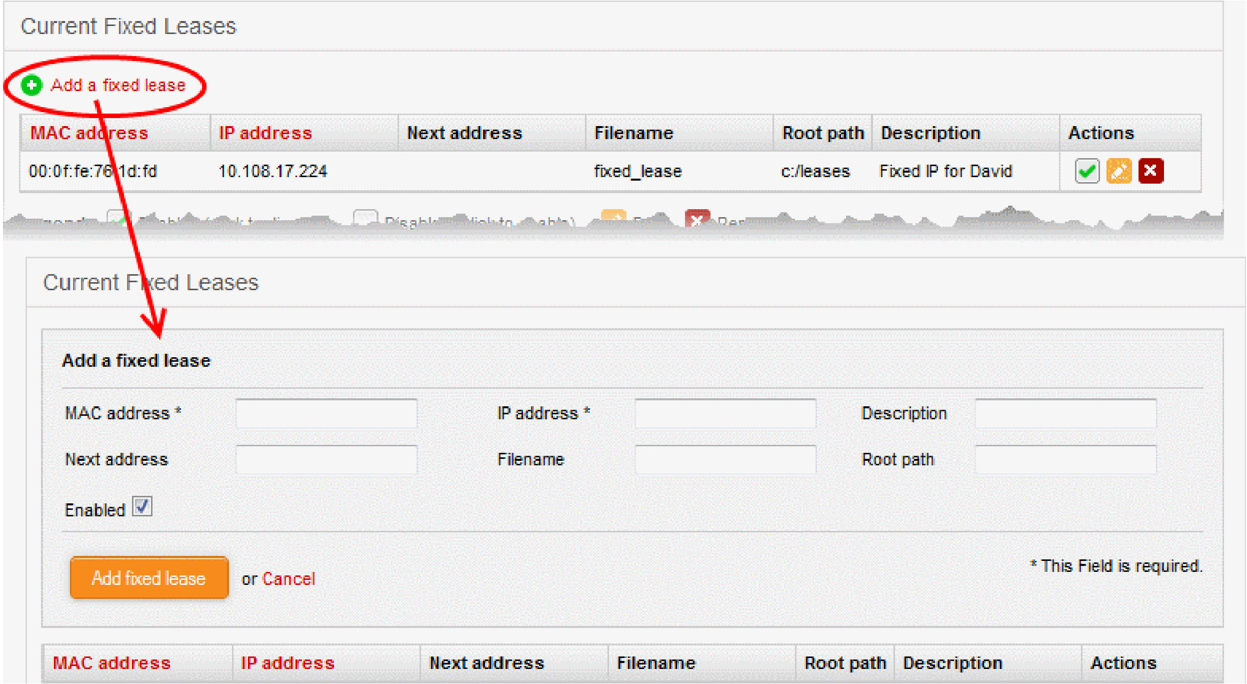
MAC address	IP address	Next address	Filename	Root path	Description	Actions
00:0f:fe:76:1d:fd	10.108.17.224		fixed_lease	c:/leases	Fixed IP for David	☑ ✎ ✖

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ✖ Remove

Current Fixed Leases Table - Column Descriptions	
Column	**Description**
MAC address	The physical MAC address of the client
IP Address	The static IP address assigned to the client
Next address	The address to which the client will be redirected if the client is configured for network boot. The next address may point to the Trivial File Transfer Protocol (TFTP) server that hosts a boot image.
Filename	The boot image file name, if the client is configured for network boot.
Root path	The path of the boot image file, if the client is configured for network boot.
Description	A short description for the device that required the fixed IP address
Actions	Displays control buttons for the fixed lease entry ☑ - Allows administrator to enable or disable the fixed lease entry. ✎dit the entry. ✖emove the entry.

To add a new fixed IP address entry

- Click the 'Add a fixed lease' link at the top left of the interface



Current Fixed Leases

Add a fixed lease

MAC address	IP address	Next address	Filename	Root path	Description	Actions
00:0f:fe:76:1d:fd	10.108.17.224		fixed_lease	c:/leases	Fixed IP for David	✓ ✎ ✗

Current Fixed Leases

Add a fixed lease

MAC address *		IP address *		Description	
Next address		Filename		Root path	
Enabled ☑					

* This Field is required.

MAC address	IP address	Next address	Filename	Root path	Description	Actions

The 'Add a fixed lease' pane will open which contains the following fields and settings:

- MAC Address - The physical MAC address of the client
- IP Address - The static IP address to be assigned to the client
- Description - A short description of the client
- Next Address - The address to which the client to be redirected, if it is in network boot mode. This setting is only for disk-less client or thin client (Optional)
- Filename - The file name of the boot image stored in the server to which the client needs to be redirected for network boot
- Root path - The path of the boot image file stored in the server to which the client needs to be redirected for network boot
- Enabled - The IP address will be assigned and enabled upon creation. If you want the address to be enabled at a later time, deselect this checkbox. You can enable the address when required by selecting the 'Enabled' checkbox under the Actions column in the Current fixed leases table.

Note: To avoid conflicts, make sure that the IP address specified here is *not* included in the IP range specified in DHCP settings for the network zone to which the client is connected and in the range of **OpenVPN address pool**

7.2 Advanced Threat Protection

- Click 'Services' > 'Advanced Threat Protection' in the left-menu to access this interface
- Advanced Threat Protection (ATP) safeguards your network against malware, hack attempts, data breaches and more.
- ATP intercepts files downloaded from websites or email attachments and uses a combination of antivirus scans, behavior analysis and blacklist checks to quickly and accurately threats.
- Application containment protects your endpoints from unknown threats. Unknown threats are those that have not yet been identified as malware by the antivirus industry. If enabled, all files with an 'Unknown' trust rating will be run in an isolated sandbox on your endpoints. This prevents them from modifying other processes, stealing user data or otherwise infecting the local machine.
- The settings you save in the profile section will be applied to all rules in your firewall policy that have 'Advanced Threat Protection' enabled.

ATP uses the following techniques to analyze the files:

- **Comodo Antivirus** - Continuously updated antivirus scanner which provides dependable protection against known malicious files.
- **Comodo Valkyrie** - A cloud based behavior analysis service which improves detection of zero-day threats by rigorously testing the run-time actions of unknown files.

Based on the analysis, files are identified as:

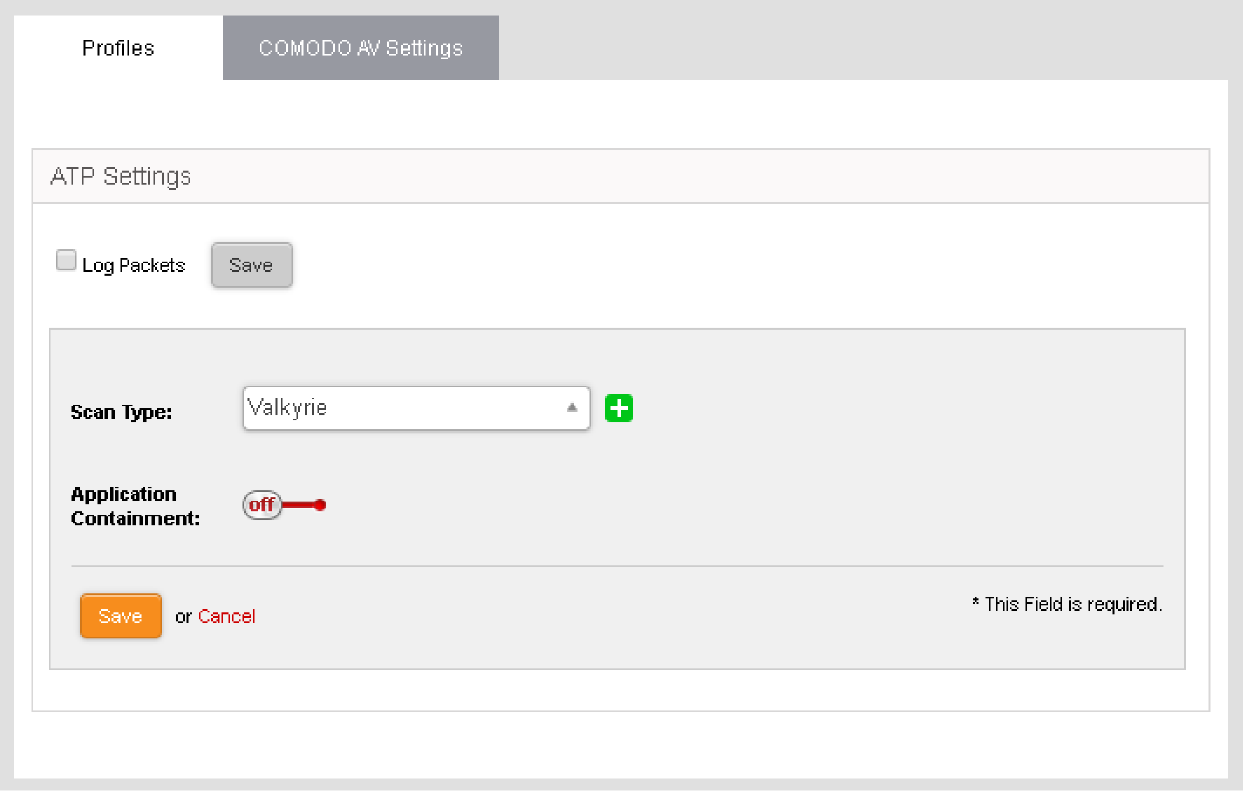
- **Safe** - Files identified as known good files from the whitelist/clean/safe are allowed to be downloaded at the endpoint
- **Threats** - Files identified as known bad from the blacklist/malicious/threats are blocked and a warning is displayed at the endpoint
- **Unknown** - Files that could not be identified are classified as 'Unknown'. These files are subjected to containment technology - meaning the files are wrapped and forwarded to the endpoint. Upon execution, the file is made to run in a isolated sandbox environment at the endpoint, whereby it is not allowed to modify other processes running on the endpoint nor access user data. This ensures the download is secure because it is not possible for the file to infect the endpoint, even if it transpires to be malicious.

Note: Containment for Unknown Applications are only applied to Windows endpoints.

ATP automatically creates whitelist and blacklist of domains based on malware analysis of the files accessed by them and also allows the administrators to manually add domains to these lists.

The Advanced Threat Protection interface allows the administrator to create and manage the profile for ATP which can be applied for web protection Firewall Policy rules. Application containment can only be used with Full License of Dome Firewall Virtual Appliance.

To access the Advanced Threat Protection interface, click 'Services' > 'Advanced Threat Protection' from the left hand side navigation.



The interface contains two tabs:

- **Profiles** - Define the file scan type, application containment settings and domains which should not be monitored by the ATP technologies. The settings you choose here will be applied to all rules in your firewall policy which have 'Advanced Threat Protection' enabled. See **Managing the ATP Profile** for more details.

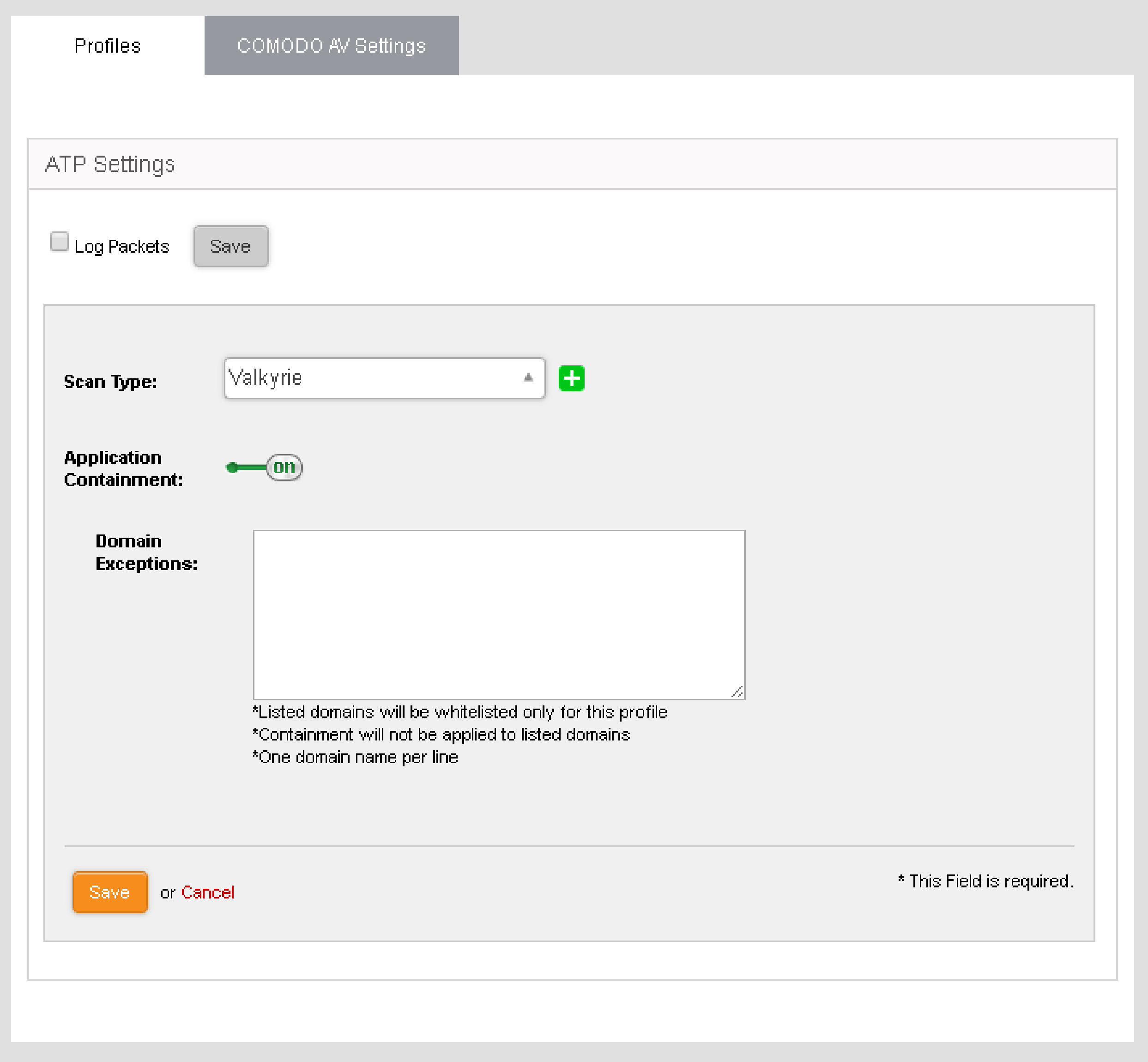
- **Scan Type**- Allows the administrator to view the engine setting for anti-malware analysis. Currently only 'Valkyrie' is available.
- **Comodo AV Settings** - Allows the administrator to configure the AV engine and schedule AV scans. See **Comodo Antivirus** for more details.

7.2.1 Managing the ATP Profile

ATP profile define the scan types to be applied to the files downloaded from websites by the endusers and application of containment technology to the unknown files. The profile can be applied for Web Protection settings while configuring Firewall policies.

To open ATP profiles interface

- Click 'Services' > 'Advanced Threat Protection' from the left hand side navigation
- Click the 'Profiles' tab.



Scan Type: Valkyrie

Application Containment: on

Domain Exceptions:

*Listed domains will be whitelisted only for this profile
*Containment will not be applied to listed domains
*One domain name per line

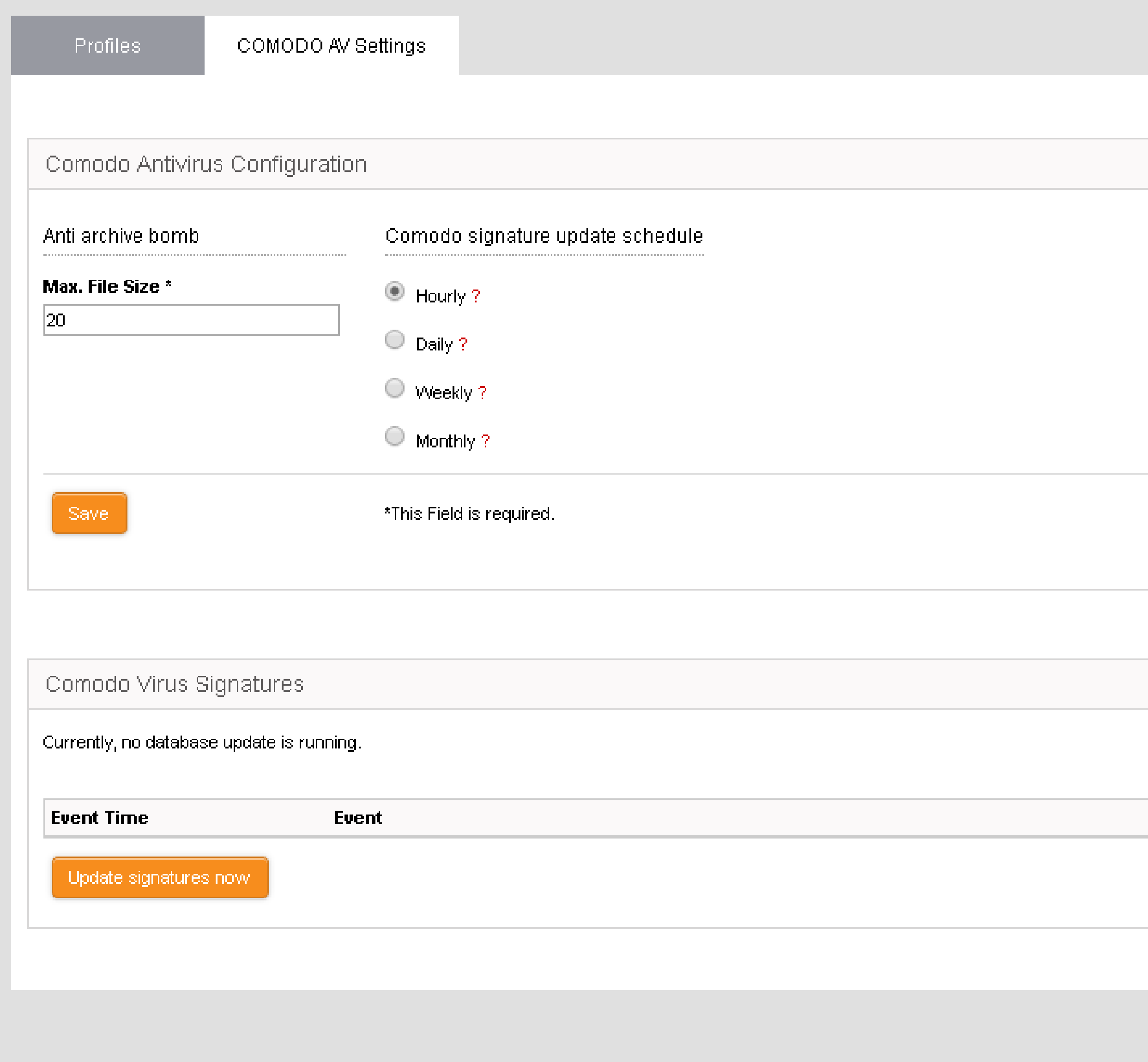
* This Field is required.

The 'Profiles' interface displays the ATP profile added to Comodo Dome Firewall and allows the administrator to edit the profile. Administrator can enable and disable the Application Containment and add domains to be whitelisted:

- **Domain Exceptions** - You can add the domains to be excluded from application containment. The files downloaded from the domains included in the list will be excluded from containment.

7.2.2 Comodo Antivirus

Comodo Dome Firewall boasts a state-of-the-art antivirus engine from Comodo, a leader in Internet Security. The antivirus engine uses constantly updated virus signature database and provides comprehensive protection against malware outbreaks on your network.



Comodo Antivirus Configuration

Anti archive bomb

Max. File Size *

20

Comodo signature update schedule

● Hourly ?

○ Daily ?

○ Weekly ?

○ Monthly ?

*This Field is required.

Comodo Virus Signatures

Currently, no database update is running.

Event Time	**Event**

Comodo Antivirus periodically scans all files and documents in the network and automatically moves any threats to quarantine, in addition to on-access scans run based on the ATP profile .

Background Note: The quarantine facility removes and isolates suspicious files into a safe location. Any files transferred in this fashion are encrypted - meaning they cannot be run or executed. This isolation prevents infected files from affecting the rest of the network.

The Antivirus engine configuration interface allows the administrator to schedule virus database updates and to configure scan parameters.

To access the Comodo Antivirus interface

- Click 'Services' > 'Advanced Threat Protection' from the left hand side navigation
- Click the 'Comodo AV Settings' tab.

The interface has two panels:

- **Comodo Configuration**
- **Comodo virus signatures**

Comodo Configuration

The Comodo Configuration panel allows administrators to modify scan parameters and set the frequency of virus database updates.

- Anti Archive Bomb - Max File Size - (MB) Files larger than the size specified will not be scanned.

Note on archive bombs: One of the techniques used by attackers to disable an antivirus system is an 'Archive Bomb'. Similar to a Denial of Service (DoS) attack, an archive bomb is designed to overload the AV system by presenting it with more process requests than it can handle. Large files containing redundant data are compressed repeatedly and nested inside a very complicated archive structure inside the zip. When an antivirus application tries to extract those archives while scanning, it consumes an inordinate amount of system resources and often halts other operations. It is advised to configure the antivirus in a computer to skip scanning files larger than a set threshold.

- Comodo Signature update schedule - The virus signature data base of the antivirus engine will be updated at the frequency selected here.

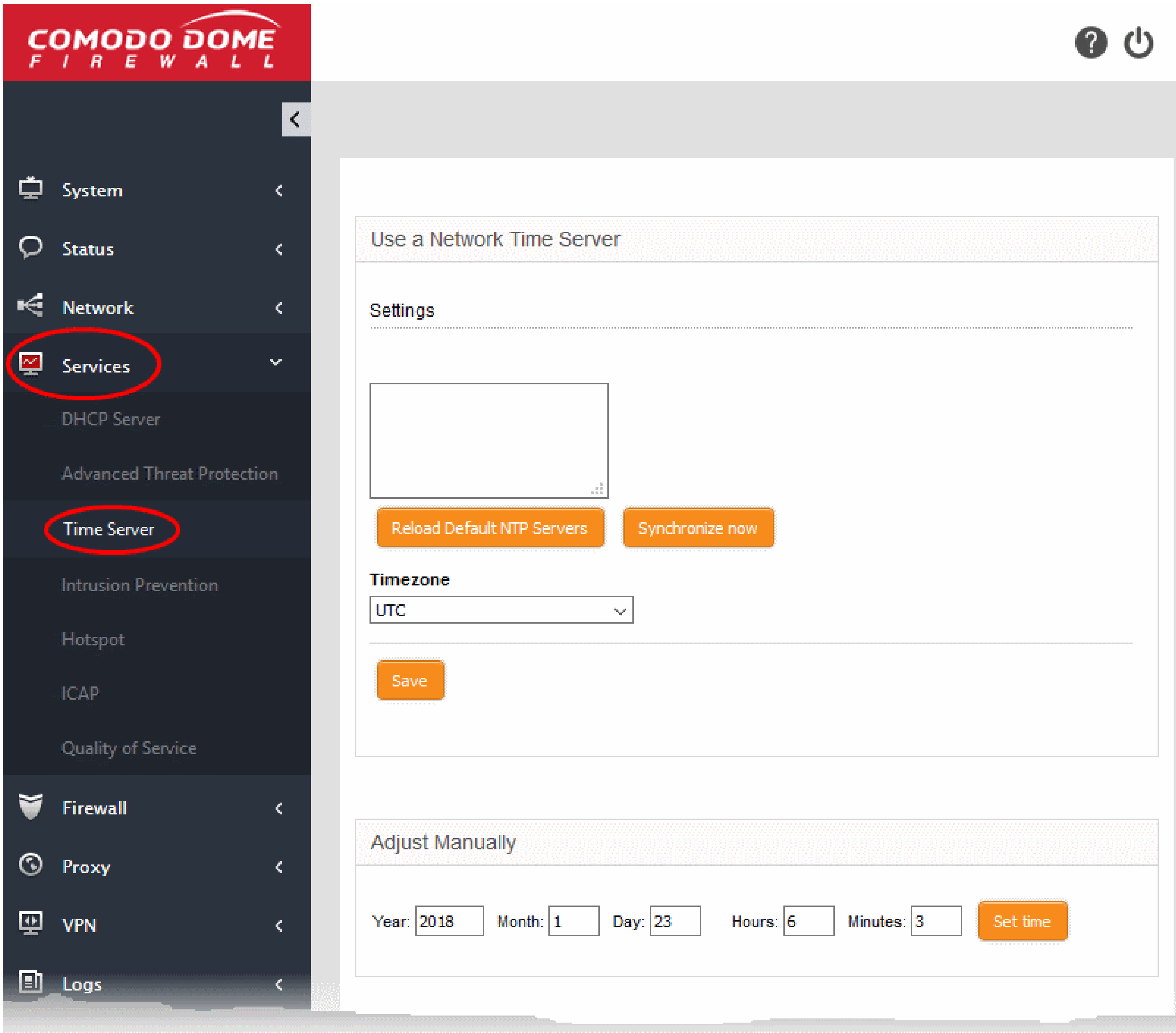
Comodo virus signatures

The 'Comodo virus signatures' panel displays a log of previous update events. Clicking the 'Update signature now' will update the virus signature database.

7.3 Time Server

- Click 'Services' on the left then select 'Time Server'.

The 'Time Server' interface allows you to configure system time and synchronization with internet time servers. Administrators can also manually set the date and time via this interface.



Timezone: UTC

Year: 2018 Month: 1 Day: 23 Hours: 6 Minutes: 3

The interface has two panels:

- Use a Network Time Server
- Adjust Manually

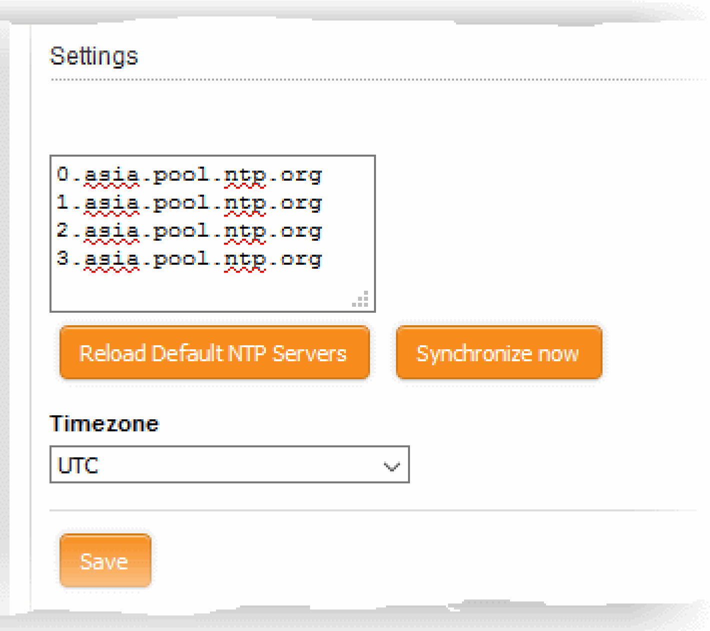
Use a Network Time Server

The firewall's system time can be synchronized with the time zones of most major cities via Network Time Protocol (NTP) servers.

- By default, the virtual appliance uses the closest NTP servers for its time synchronization
- If required, administrators can synchronize with a manually specified time server. This is useful, for example, if the virtual appliance is used in an environment without an internet connection.

To specify custom time servers

- Enter the URLs of custom time servers in the text field provided. Any number of servers can be added. Enter each URL on a separate line.


Settings

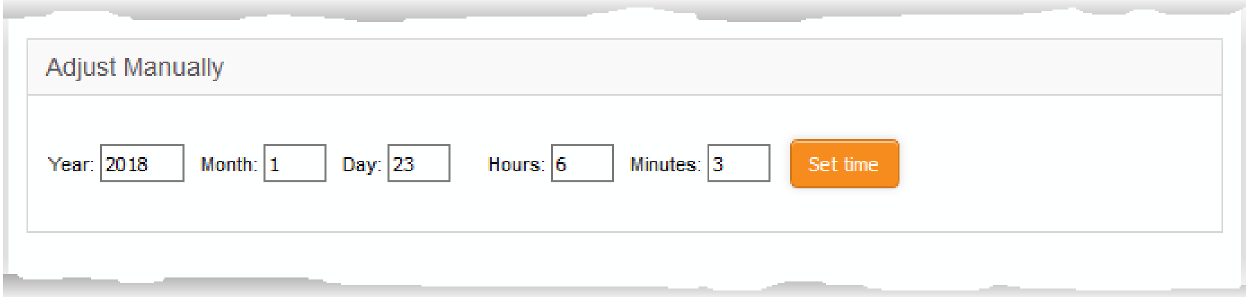
```
0.asia.pool.ntp.org
1.asia.pool.ntp.org
2.asia.pool.ntp.org
3.asia.pool.ntp.org
```

Timezone: UTC

- Time Zone - Select the time zone to which the virtual appliance should synchronize.
- Click 'Synchronize now' to synchronize the time immediately with the specified NTP servers.
- Click 'Reload Default NTP Servers' to restore the appliance to the default time servers.
- Click 'Save' to save your settings.

Adjust Manually

The lower panel lets you manually set the time in system clock. This is useful if the system clock has stopped for some time and immediate time update is needed.


Adjust Manually

Year: 2018 Month: 1 Day: 23 Hours: 6 Minutes: 3

- Enter the year, month, date, and the current time in hours and minutes
- Click 'Set time'.

Tip: The time server is used to provide time-stamps for important operations like audit generation. Hence, it is important to keep it precise and accurate.

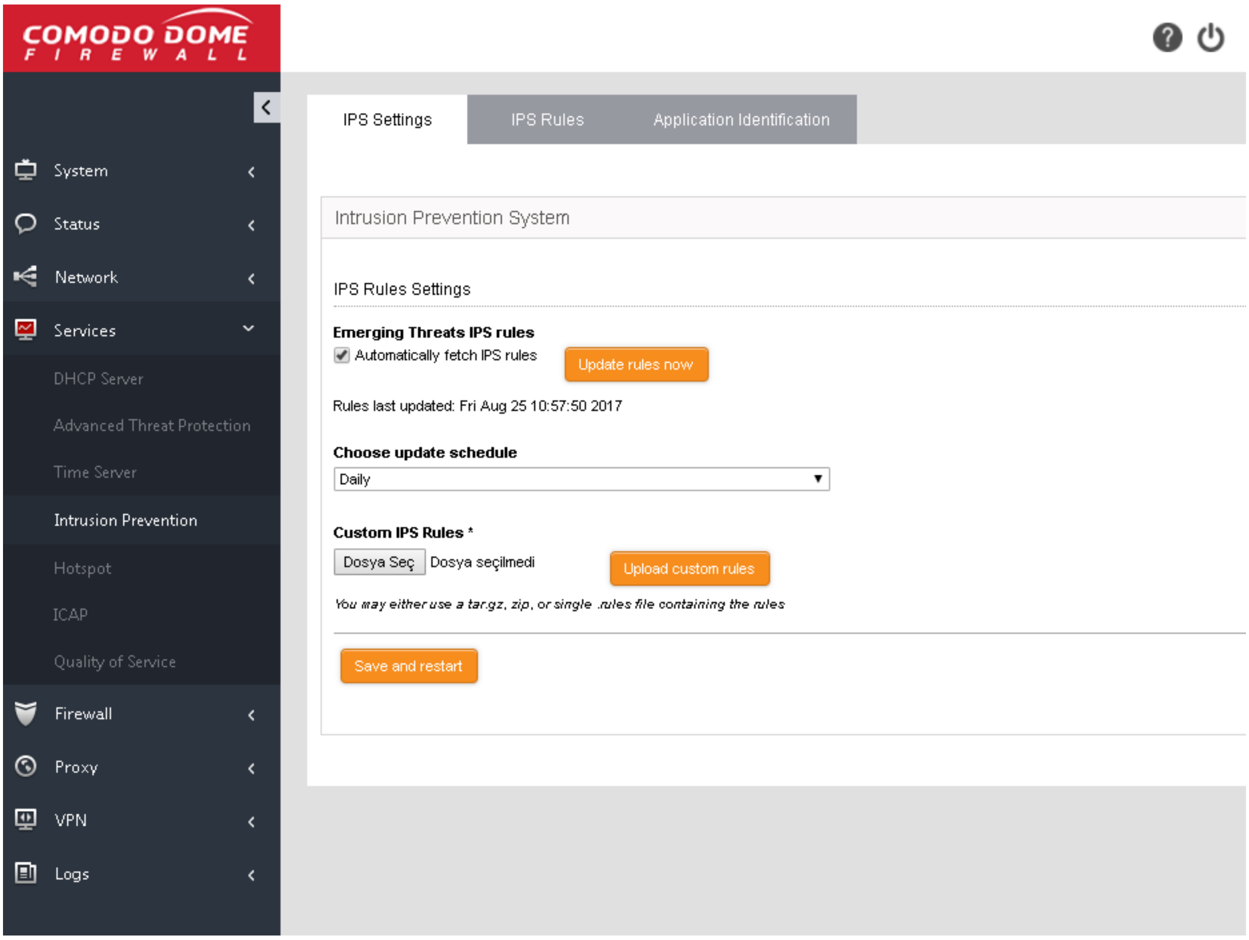
7.4 Intrusion Prevention

Comodo Dome Firewall includes 'Snort', a state-of-the-art network intrusion prevention and detection system (IDS/IPS) directly built-in to its IP tables. Snort employs signature, protocol, and anomaly-based inspection of incoming traffic and is the de facto IPS standard and checks the data flow through the network for intrusion detection and prevention.

Snort uses IPS rulesets, containing a number of intrusion detection/prevention rules and application detection rule sets containing a number of rules for identifying applications generating TCP/IP traffic on the network. The application rule sets enable reporting application names along with IPS events. The rules are developed by their Vulnerability Research Team (VRT) for inspecting different parts of data packets and actions to be taken. The rule sets are constantly updated to confront emerging network intrusion techniques, that can be periodically downloaded from Snort servers. Using up-to-date rule sets enables Dome Firewall to detect and prevent unprecedented network intrusions attempts.

The Intrusion Prevention System interface allows the administrator to configure Snort rules update schedule, create and upload Snort rules and enable/disable rule sets.

To access the 'Intrusion Prevention System' interface, click 'Services' > 'Intrusion Prevention' from the left hand side navigation.



Intrusion Prevention System

IPS Rules Settings

Emerging Threats IPS rules

☑ Automatically fetch IPS rules

Rules last updated: Fri Aug 25 10:57:50 2017

Choose update schedule

Daily

Custom IPS Rules *

Dosya Seç Dosya seçilmedi

You may either use a tar.gz, zip, or single .rules file containing the rules

The Interface has three tabs:

- **IPS Settings** - Allows the administrator to enable/disable the intrusion prevention system and configure ruleset updates. Refer to the section **Configuring Intrusion Prevention System** for more details.
- **IPS Rules** - Displays the currently loaded IPS rulesets and allows the administrator to manage them. Refer to the section **Managing IPS Rulesets** for more details.
- **Application Identification** - Displays the currently loaded Application Identification rulesets and allows the administrator to manage them. Refer to the section **Managing Application Identification Rulesets** for more details.

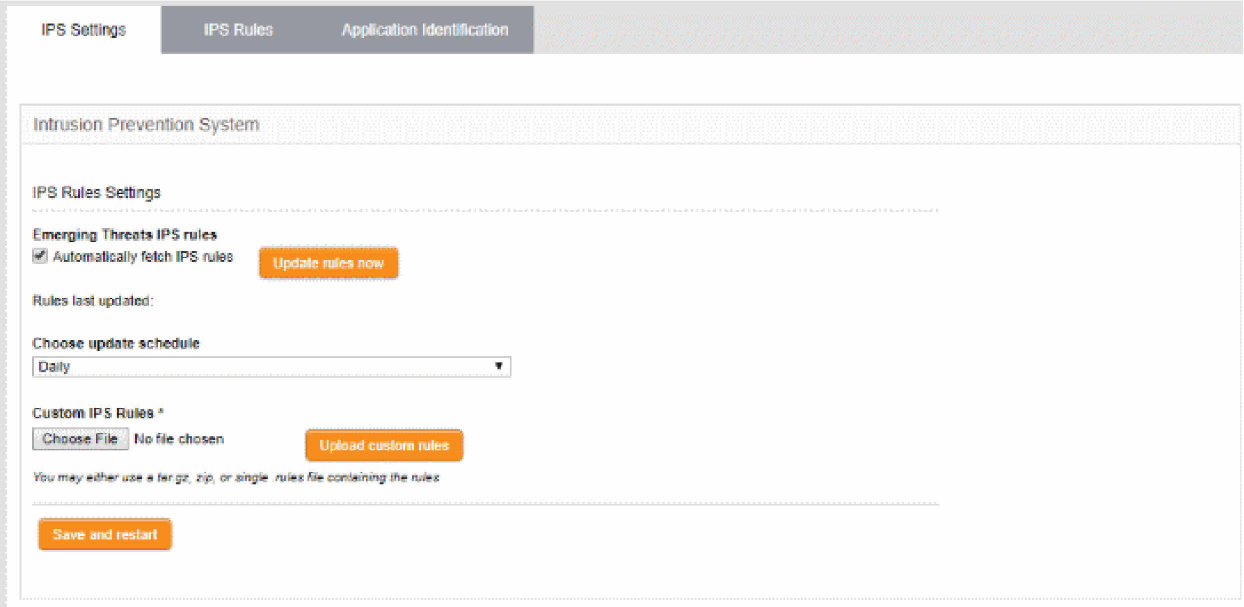
7.4.1 Configuring Intrusion Prevention System

The IPS Settings interface allows the administrator to configure the ruleset updates for Snort. The ruleset updates can be scheduled to run automatically at specified intervals and can be run manually on demand.

Advanced users can locally create custom Snort rules for network intrusion detection and prevention as per their specific needs and upload to the DFW from the 'Intrusion Prevention System' interface. For more details on creating new custom rules is available in the online page **http://manual.snort.org/node27.html**.

To open the 'Intrusion Prevention' interface

- Click 'Services' > 'Intrusion Prevention' from the left hand side navigation.
- Click the 'IPS Settings' tab



Intrusion Prevention System

IPS Rules Settings

Emerging Threats IPS rules

☑ Automatically fetch IPS rules

Rules last updated:

Choose update schedule

Daily

Custom IPS Rules *

No file chosen

You may either use a tar.gz, zip, or single .rules file containing the rules

IPS Rules Settings

- **Automatically fetch IPS rules** - Select this checkbox for scheduled automatic Snort ruleset updates. Dome Firewall will download the ruleset database updates from the Snort servers and install them locally at the selected intervals. The interval can be chosen from 'Choose update schedule' drop-down, that appears on selecting this option. The available options are:
  - Hourly
  - Daily (***Default***)
  - Weekly
  - Monthly
- **Update Ruleset Manually** - To instantly update the ruleset database, click the 'Update rules now' button.

Custom IPS Rules

IPS rulesets containing custom rules can be created as per the network requirements by the administrator and can be uploaded to the DFW virtual appliance for implementation at any time. The constituent rules can be defined in a text file and stored as .rules file to form a rule set file. The interface allows to upload single ruleset file or tar.gz or zip file containing several ruleset files.

To upload the custom ruleset file(s)

- Click 'Choose File' under 'Custom IPS Rules' and navigate to the location of the rules file and click 'Open'.
- Click 'Upload custom rules'
- Click 'Save' and 'Restart' after completing the any configuration change

The Intrusion Prevention System service will restart for your changes to take effect.

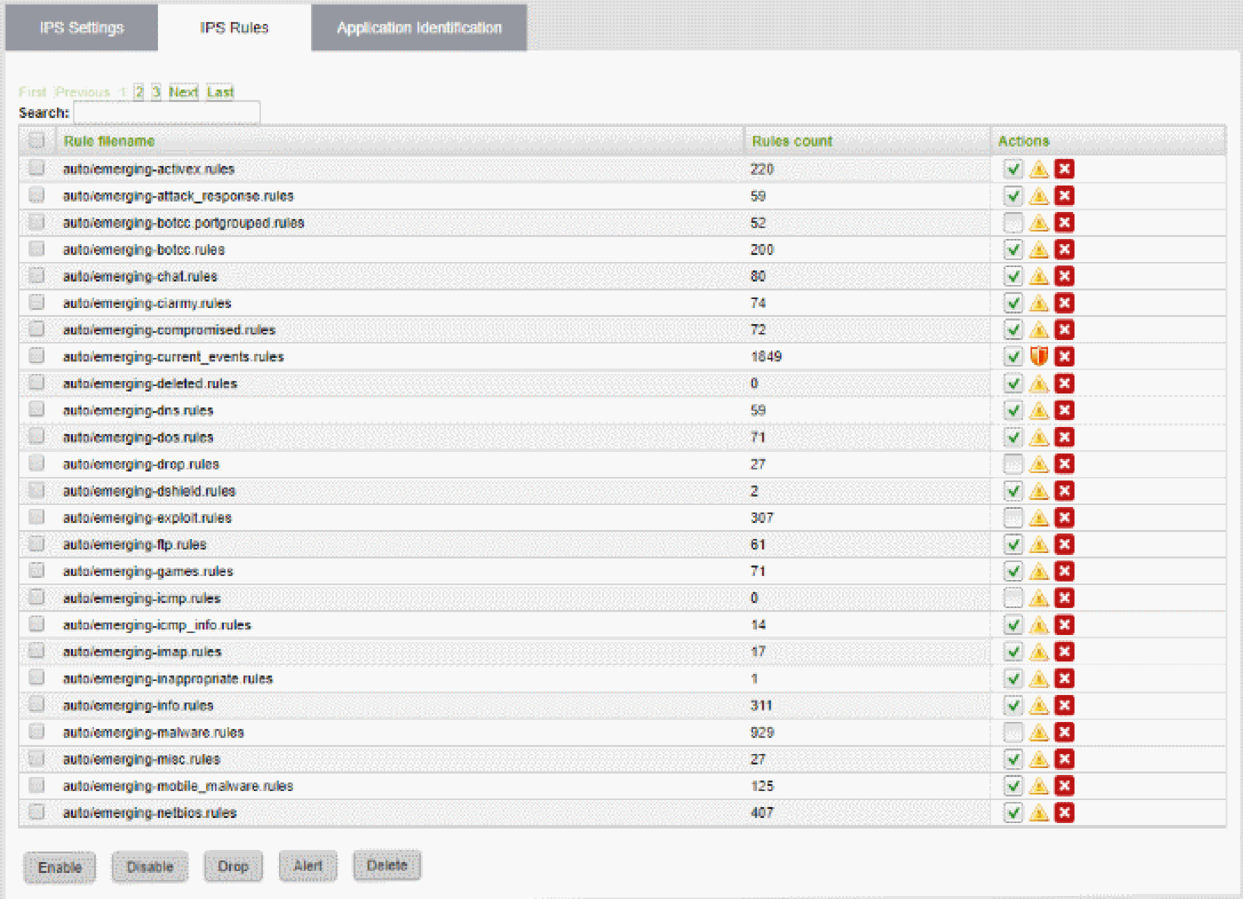
7.4.2 Managing IPS Rulesets

The 'IPS Rules' interface displays a list of currently loaded IPS rulesets and enables administrators to enable/disable rulesets, and configuring for allowing or blocking the data packets intercepted by a ruleset.

To open the IPS Rules interface

- Click 'Services' > 'Intrusion Prevention' from the left hand side navigation.

- Click the 'IPS Rules' tab



Search:

□	Rule filename	Rules count	Actions
□	auto/emerging-activex.rules	220	☑ ⚠ ☒
□	auto/emerging-attack_response.rules	59	☑ ⚠ ☒
□	auto/emerging-botcc.portgrouped.rules	52	□ ⚠ ☒
□	auto/emerging-botcc.rules	200	☑ ⚠ ☒
□	auto/emerging-chat.rules	80	☑ ⚠ ☒
□	auto/emerging-ciarmy.rules	74	☑ ⚠ ☒
□	auto/emerging-compromised.rules	72	☑ ⚠ ☒
□	auto/emerging-current_events.rules	1849	☑ 🛡 ☒
□	auto/emerging-deleted.rules	0	☑ ⚠ ☒
□	auto/emerging-dns.rules	59	☑ ⚠ ☒
□	auto/emerging-dos.rules	71	☑ ⚠ ☒
□	auto/emerging-drop.rules	27	□ ⚠ ☒
□	auto/emerging-dshield.rules	2	☑ ⚠ ☒
□	auto/emerging-exploit.rules	307	□ ⚠ ☒
□	auto/emerging-ftp.rules	61	☑ ⚠ ☒
□	auto/emerging-games.rules	71	☑ ⚠ ☒
□	auto/emerging-icmp.rules	0	□ ⚠ ☒
□	auto/emerging-icmp_info.rules	14	☑ ⚠ ☒
□	auto/emerging-imap.rules	17	☑ ⚠ ☒
□	auto/emerging-inappropriate.rules	1	☑ ⚠ ☒
□	auto/emerging-info.rules	311	☑ ⚠ ☒
□	auto/emerging-malware.rules	929	□ ⚠ ☒
□	auto/emerging-misc.rules	27	☑ ⚠ ☒
□	auto/emerging-mobile_malware.rules	125	☑ ⚠ ☒
□	auto/emerging-netbios.rules	407	☑ ⚠ ☒

Rules Table - Column Descriptions	
Column	**Description**
Rule filename	The name of the .rules file that contains the constituent rules of the ruleset
Rules count	Indicates the number of constituent rules in the rule set
Actions	Displays control buttons for the ruleset. ☑ - The checkbox allows the administrator to switch the ruleset between enabled and disabled states ⚠ / 🛡 - Indicates the application policy of the ruleset and enables the administrator to toggle the policy. See **Changing application policy of rulesets** for more details. ☒ - Removes the ruleset

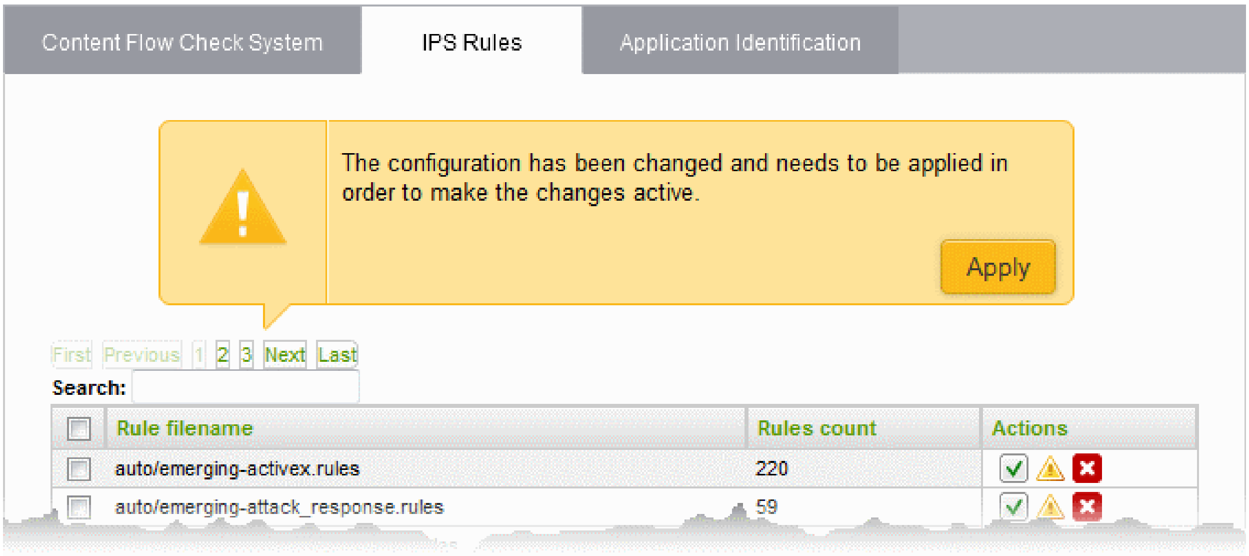
The interface allows the administrator to:

- **Enable/Disable rulesets**
- **Change application policy of rulesets**
- **Remove rulesets**

Enabling/Disabling Rulesets

The rulesets can be enabled or disabled individually or collectively from the Rules interface.

- To enable or disable a single ruleset, select or unselect the checkbox beside the ruleset in the 'Actions' column
- To enable inactive rulesets collectively, select the rules by marking the checkboxes at the left of the rulesets to be enabled and click the 'Enable' button from the bottom of the right pane.
- To disable active rulesets collectively, select the rules by marking the checkboxes at the left of the rulesets to be disabled and click the 'Disable' button from the bottom of the right pane.
- After making the changes, click the 'Apply' button in the confirmation pane that appears at the top to apply the changes.


Content Flow Check System
IPS Rules
Application Identification
Apply
First Previous 1 2 3 Next Last
Search:

The configuration has been changed and needs to be applied in order to make the changes active.

□	Rule filename	Rules count	Actions
□	auto/emerging-activex.rules	220	✓ ⚠ ✖
□	auto/emerging-attack_response.rules	59	✓ ⚠ ✖

Changing application policy of rulesets

A ruleset can be applied in two ways:

- **Alert Policy** - The IPS generates an alert when a data packet matching a rule in the ruleset is encountered and passes the packet. The policy is indicated by alert icon ⚠.
- **Drop Policy** - The IPS blocks the data packet matching a rule in the ruleset without generating an alert. The policy is indicated by shield icon 🛡.

The administrator can toggle the application policy for individual rulesets or for group of rulesets.

- To toggle the policy of a ruleset from 'Alert' policy to 'Drop' policy, click the 'Alert' icon in the row of the ruleset under the 'Actions' column
- To toggle the policy of a ruleset from 'Drop' policy to 'Alert' policy, click the 'Shield' icon in the row of the ruleset under the 'Actions' column
- To toggle the policy of a group of rulesets with 'Alert' policy to 'Drop' policy, select the rulesets by marking the checkboxes at the left of the ruleset file names and click the 'Drop' button at the bottom of the interface
- To toggle the policy of a group of rulesets with 'Drop' policy to 'Alert' policy, select the rulesets by marking the checkboxes at the left of the ruleset file names and click the 'Alert' button at the bottom of the interface
- After making the changes, click the Apply button in the confirmation pane that appears at the top to apply the changes.

Removing rulesets

Unwanted rulesets can be removed from Comodo Dome Firewall from the Rules interface.

- To remove a single ruleset click the delete icon ✖ in the row of the ruleset filename, under 'Actions' column and click 'OK' in the confirmation dialog

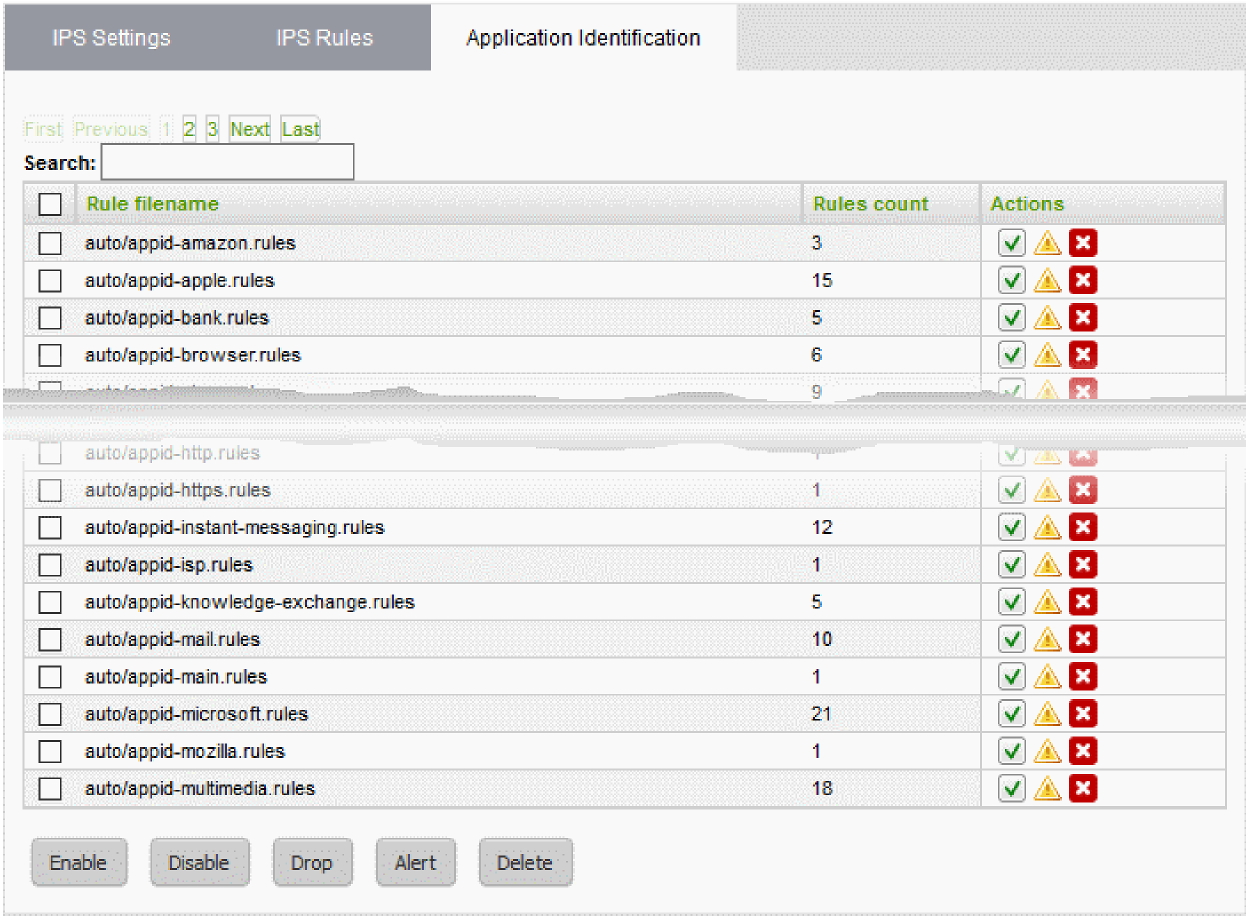
- To remove a group of rulesets collectively, select the them by marking the checkboxes at the left of the ruleset file names and click the 'Delete' button at the bottom of the interface. Click 'OK' in the confirmation dialog

7.4.3 Managing Application Identification Rulesets

The 'Application Identification' interface displays a list of Application Identification rulesets that are currently loaded to the virtual appliance and enables administrators to enable/disable rulesets. The administrator can also configure the Intrusion Prevention system to allow or block the TCP/IP traffic from the applications, identified by the rules in a ruleset.

To open the 'Application Identification' rules interface

- Click 'Services' > 'Intrusion Prevention' from the left hand side navigation.
- Click the 'Application Identification' tab



□	Rule filename	Rules count	Actions
□	auto/appid-amazon.rules	3	✓ ⚠ ✖
□	auto/appid-apple.rules	15	✓ ⚠ ✖
□	auto/appid-bank.rules	5	✓ ⚠ ✖
□	auto/appid-browser.rules	6	✓ ⚠ ✖
□	[illegible]	9	✓ ⚠ ✖
□	auto/appid-http.rules	[illegible]	✓ ⚠ ✖
□	auto/appid-https.rules	1	✓ ⚠ ✖
□	auto/appid-instant-messaging.rules	12	✓ ⚠ ✖
□	auto/appid-isp.rules	1	✓ ⚠ ✖
□	auto/appid-knowledge-exchange.rules	5	✓ ⚠ ✖
□	auto/appid-mail.rules	10	✓ ⚠ ✖
□	auto/appid-main.rules	1	✓ ⚠ ✖
□	auto/appid-microsoft.rules	21	✓ ⚠ ✖
□	auto/appid-mozilla.rules	1	✓ ⚠ ✖
□	auto/appid-multimedia.rules	18	✓ ⚠ ✖

Rules Table - Column Descriptions	
Column	**Description**
Rule filename	The name of the .rules file that contains the constituent rules of the ruleset
Rules count	Indicates the number of constituent rules in the rule set
Actions	Displays control buttons for the ruleset. ✓ - The checkbox allows the administrator to switch the ruleset between enabled and disabled states ⚠ / 🛡 - Indicates the application policy of the ruleset and enables the administrator to

	toggle the policy. See **Changing application policy of rulesets** for more details. ✖ - Removes the ruleset

The interface allows the administrator to:

- **Enable/Disable rulesets**
- **Change application policy of rulesets**
- **Remove rulesets**

Enabling/Disabling Rulesets

The rulesets can be enabled or disabled individually or collectively from the Rules interface.

- To enable or disable a single ruleset, select or unselect the checkbox beside the ruleset in the 'Actions' column
- To enable inactive rulesets collectively, select the rules by marking the checkboxes at the left of the rulesets to be enabled and click the 'Enable' button from the bottom of the right pane.
- To disable active rulesets collectively, select the rules by marking the checkboxes at the left of the rulesets to be disabled and click the 'Disable' button from the bottom of the right pane.
- After making the changes, click the 'Apply' button in the confirmation pane that appears at the top to apply the changes.

Changing application policy of rulesets

A ruleset can be applied in two ways:

- **Alert Policy** - The Intrusion Prevention system generates an alert when a data packet from applications identified by a rule in the ruleset is encountered and passes the packet. The policy is indicated by alert icon ⚠.
- **Drop Policy** - The Intrusion Prevention system blocks the data packet from an application identified by a rule in the ruleset without generating an alert. The policy is indicated by shield icon 🛡.

The 'Application Identification' rulesets can be enabled or disabled individually or collectively from the 'Application Identification' interface.

- To toggle the policy of a ruleset from 'Alert' policy to 'Drop' policy, click the 'Alert' icon in the row of the ruleset under the 'Actions' column
- To toggle the policy of a ruleset from 'Drop' policy to 'Alert' policy, click the 'Shield' icon in the row of the ruleset under the 'Actions' column
- To toggle the policy of a group of rulesets with 'Alert' policy to 'Drop' policy, select the rulesets by marking the checkboxes at the left of the ruleset file names and click the 'Drop' button at the bottom of the interface
- To toggle the policy of a group of rulesets with 'Drop' policy to 'Alert' policy, select the rulesets by marking the checkboxes at the left of the ruleset file names and click the 'Alert' button at the bottom of the interface
- After making the changes, click the Apply button in the confirmation pane that appears at the top to apply the changes.

Removing rulesets

Unwanted Application Identification rulesets can be removed from Comodo Dome Firewall from the 'Application Identification' interface.

- To remove a single ruleset click the delete icon ✖ in the row of the ruleset filename, under 'Actions' column and click 'OK' in the confirmation dialog

- To remove a group of rulesets collectively, select the them by marking the checkboxes at the left of the ruleset file names and click the 'Delete' button at the bottom of the interface. Click 'OK' in the confirmation dialog

7.5 Configuring Wireless Hotspot

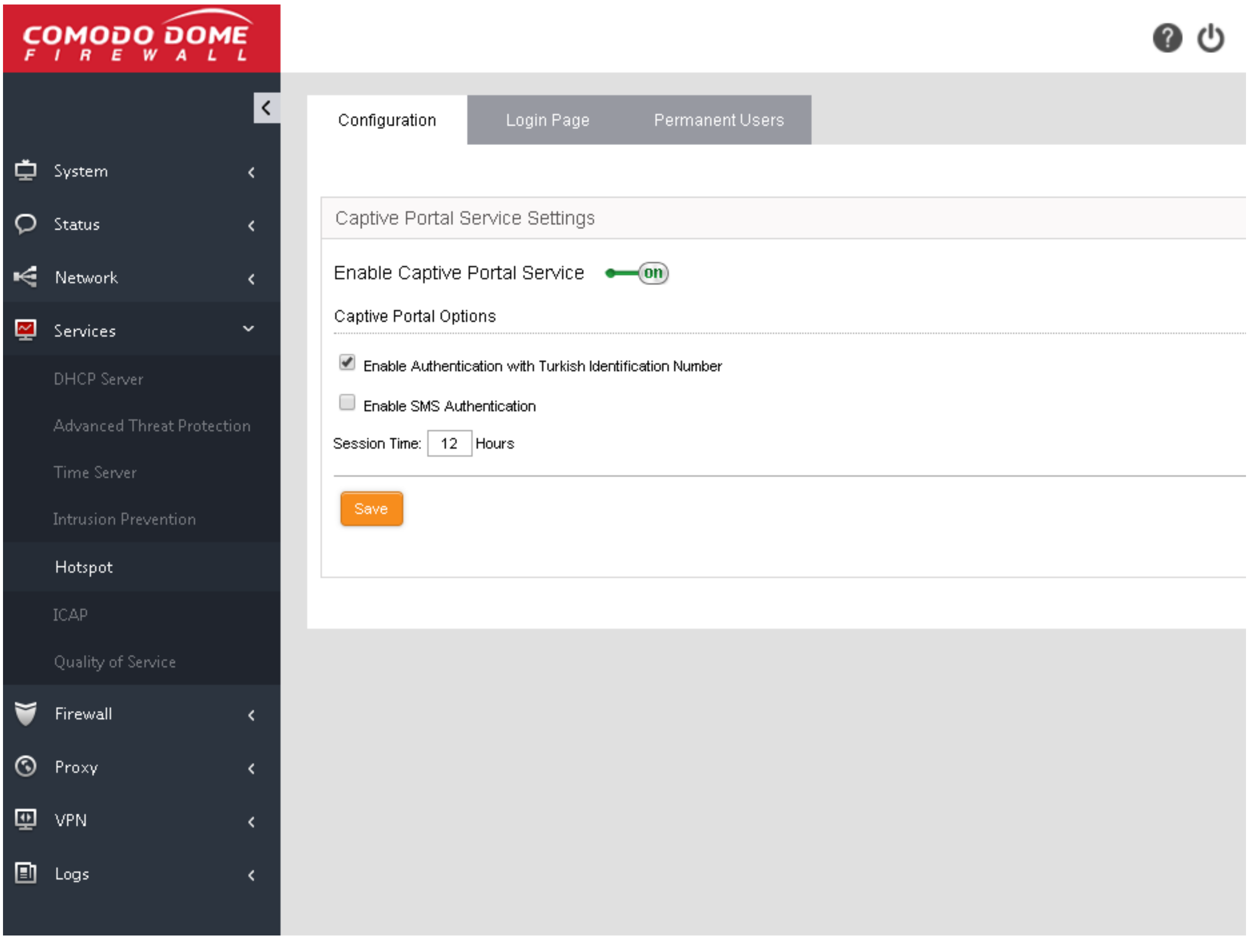
Comodo Dome Firewall features Hotspot service that provides internet connection to mobile device users through WiFi from the uplink device or external network zone interface by which the virtual appliance is connected to internet. The Hotspot interface enables the administrator to configure the captive portal service for authenticating the Wi-Fi connections and regulate the connection sessions. The authentication can be chosen from two methods:

- Using Turkish Identification Number
- Using one time password (OTP) sent to the user's device through SMS

Note: For enabling authentication through SMS, the administrator should have subscribed for the OTP service from a SMS token service provider.

The administrator can also create a whitelist of devices, enabling the device users to login to the Hotspot service without the need of authenticating themselves every time.

To access the 'Hotspot' interface, click 'Services' > Hotspot' from the left hand side navigation.



Captive Portal Service Settings

Enable Captive Portal Service: on

Captive Portal Options

☑ Enable Authentication with Turkish Identification Number

□ Enable SMS Authentication

Session Time: 12 Hours

The following sections provide more details on:

- **Configuring Captive Portal Service**
- **Customizing the Login Page**

- Adding and Managing Permanent Users

7.5.1 Configuring Captive Portal Service

The Configuration interface allows the administrator to enable/disable the Captive Portal service and configure the authentication process for the end-users to login and connect to the hotspot.

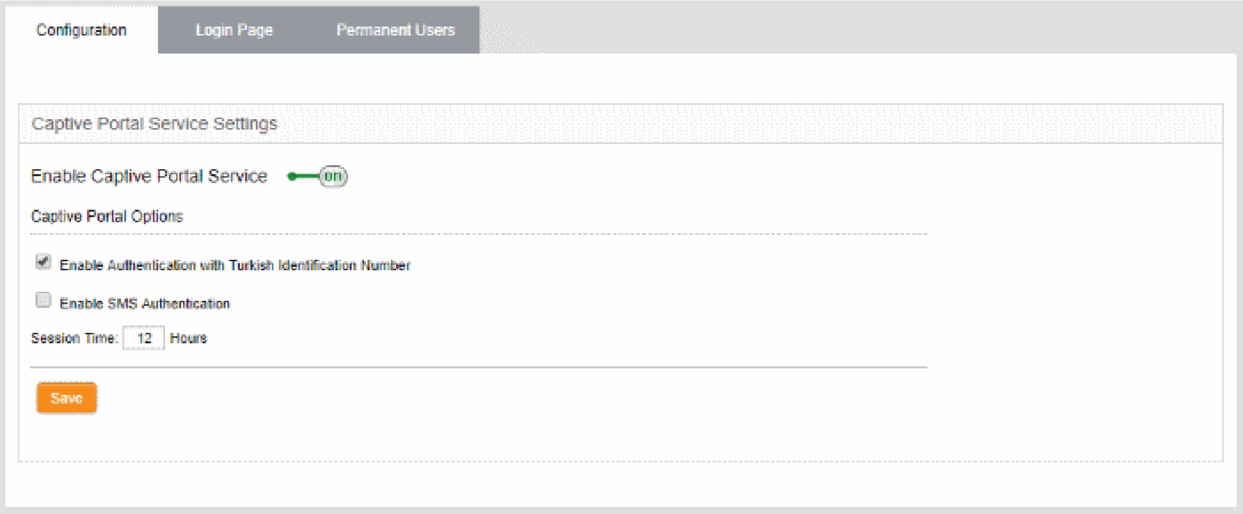
If the captive portal service is enabled, the administrator can choose the method of authentication for the users to login to the WiFi hotspot and connect to internet.

Authentication Options:

- **Authentication with Turkish Identification Number** - The end-users that attempt to connect to the hotspot need to enter their 11 digit Turkish Identification Number. The user will be authenticated upon validation of the number.
- **SMS Authentication** - Dome Firewall sends an one-time-password (OTP) as authentication token to the user's SMS enabled mobile device. The end-user needs to enter the token in the login screen displayed at the time of login attempt to connect to the hotspot.
  - When an user attempts to connect o the hotspot, the login screen will be displayed requesting the user to enter the phone number.
  - On receiving the phone number, Dome Firewall sends a random generated OTP to the device through SMS. The user needs to enter the OTP in the next screen to authenticate him/herself.

To configure the Captive Portal Service

- Open the Configuration interface by clicking Services > Hotspot from the left hand side navigation and selecting the 'Configuration' tab.



Enable Captive Portal Service: on

Captive Portal Options

☑ Enable Authentication with Turkish Identification Number

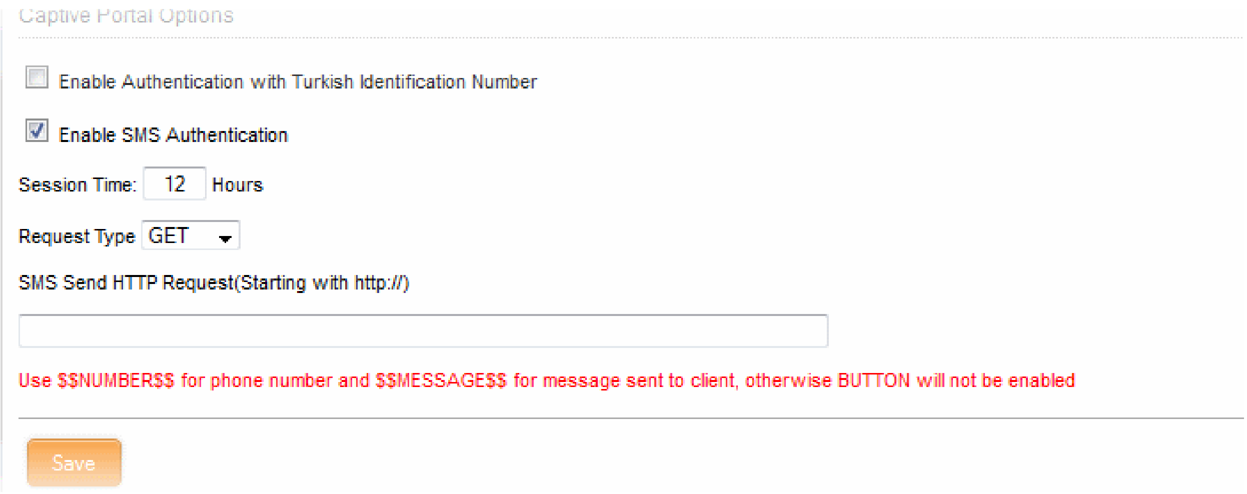
☐ Enable SMS Authentication

Session Time: 12 Hours

- **Enable Captive Portal Service** - Use the toggle switch to enable or disable the captive portal service for the Wi-Fi hotspot

Captive Portal Options

- **Enable Authentication with Turkish Identification Number** - Enables the end-users to authenticate themselves by entering their Turkish Identification Number.
- **Enable SMS Authentication** - Enables the end-users to authenticate themselves by entering the the OTP sent to their mobile devices.



Captive Portal Options

□ Enable Authentication with Turkish Identification Number

☑ Enable SMS Authentication

Session Time: 12 Hours

Request Type GET

SMS Send HTTP Request(Starting with http://)

Use $$NUMBER$$ for phone number and $$MESSAGE$$ for message sent to client, otherwise BUTTON will not be enabled

Note: For SMS type authentication, the administrator should have subscribed for the SMS token service from a third-party SMS service provider and obtained the API URL for the same. The API should be integrated to the DFW virtual appliance by entering the URL in this interface.

On selecting the SMS authentication, you need to configure the following options:

- Request type - Choose the HTTP Request Type of the API from the SMS service provider from the drop-down. The options available are GET and POST.
- Request URL - Enter the SMS Send Request URL obtained from the service provider in the 'SMS Send HTTP Request' text field. The URL should contain $$NUMBER$$ for the phone number variable and $$MESSAGES$$ variable for the OTP to be sent.

  Example: http://smsprovider.com/number=$$NUMBER$$&message=$$MESSAGES$$

Session Time Option

- Session Time - Enter the maximum period (in hours) for which a single Wi-Fi connection session is allowed for a user. The user will be automatically logged out on lapse of the period. To continue, the user needs to re-authenticate and login to the hotspot.
- Click 'Save' for your settings to take effect.

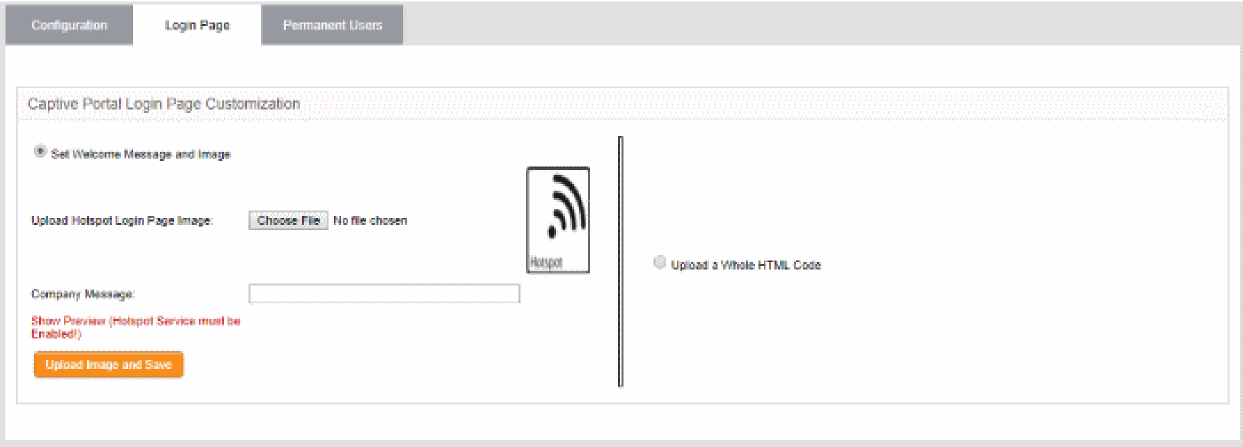
7.5.2 Customizing the Login Page

DFW allows the administrator to choose either built-in login page that will be displayed to hotspot users or a custom built login page. The built in login page allows to customize the login page image and welcome message.

- **Customize built-in login page**
- **Upload custom login page**

To customize the built-in Wi-Fi login page

- Click 'Services' > 'Hotspot' from the left hand side navigation and select the 'Login Page' tab.



Captive Portal Login Page Customization

● Set Welcome Message and Image

Upload Hotspot Login Page Image: No file chosen

Company Message:

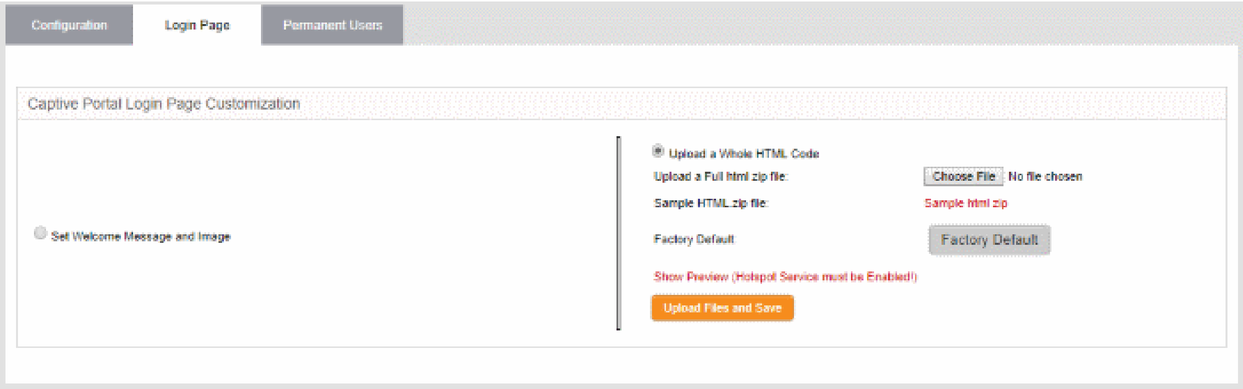
Show Preview (Hotspot Service must be Enabled!)

○ Upload a Whole HTML Code

- Select the option 'Set Welcome Message and Image'
- To upload the logo/brand image of the organization click 'Choose File', navigate to the image file stored in the local disk of the computer and click 'Open'.
- To display a custom message in the login screen, enter the message in the 'Company Message' text box.
- Clicking 'Show Preview' will display the login page in a new browser window for confirmation.
- Click 'Upload image and Save' to save your login page.

To upload the custom login page

- Select the option 'Upload a Whole HTML Code'.



Captive Portal Login Page Customization

○ Set Welcome Message and Image

● Upload a Whole HTML Code

Upload a Full html zip file: No file chosen

Sample HTML zip file: Sample html zip

Factory Default

Show Preview (Hotspot Service must be Enabled!)

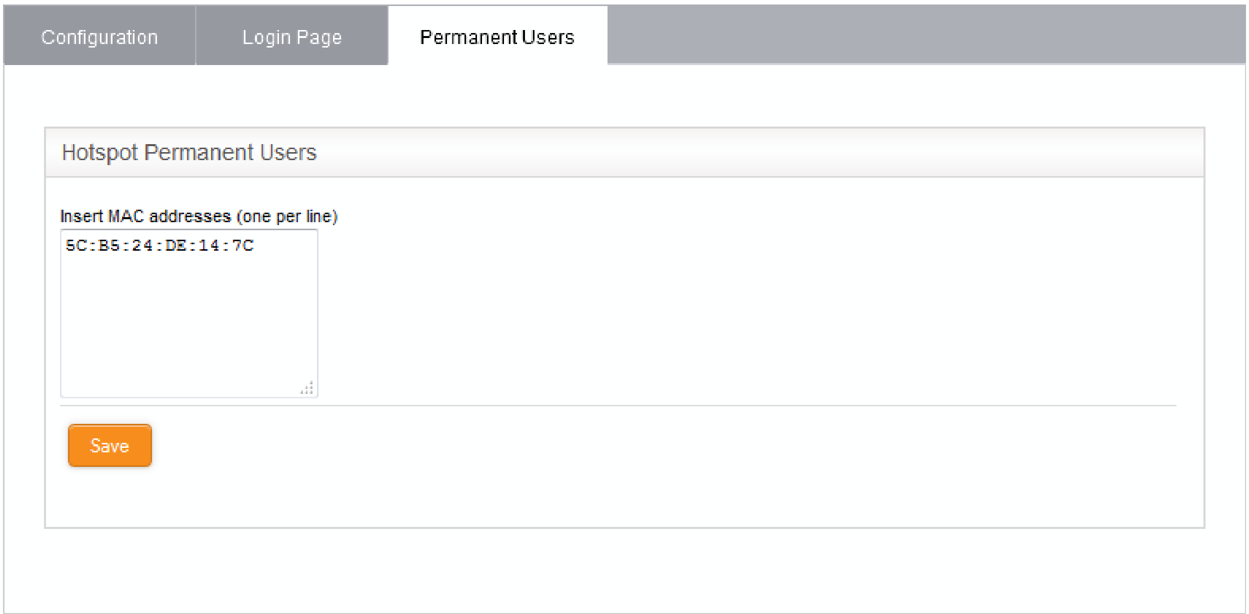
- Click 'Sample html zip' to download and view the sample custom login page.
- To upload your custom login page, click 'Choose File', navigate to the file stored in the local disk of the computer and click 'Open'.
- Clicking 'Show Preview' will display the login page in a new browser window for confirmation.
- Click 'Upload image and Save' to save your login page.
- Click 'Factory Default' to reset the login page to default hotspot welcome page

7.5.3 Adding and Managing Permanent Users

Dome Firewall allows the administrator to add a list of permanent users, who can be given access to the hotspot without the need of authenticating them. The hotspot service maintains a whitelist of devices to which access can be granted without authentication. The administrator can obtain the MAC address of the devices to be added to the whitelist and add them to the virtual appliance through the 'Permanent Users' interface.

The users added to the Permanent Users interface can connect to the hotspot without entering the Turkish

Identification number/one time password (OTP) to the login page.



Hotspot Permanent Users

Insert MAC addresses (one per line)

5C:B5:24:DE:14:7C

To add devices to the whitelist

- Click 'Services' > 'Hotspot' from the left hand side navigation and select the 'Permanent Users' tab.
- Enter the MAC address of the device to be added to the whitelist and click 'Save'.

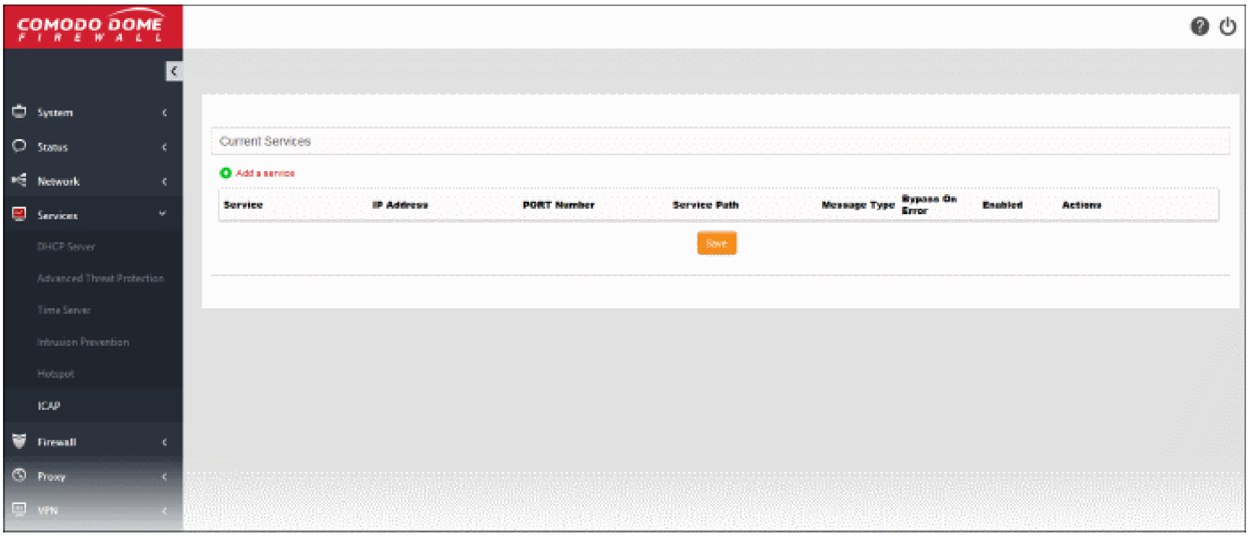
The device will be added to the whitelist.

- To remove a device from whitelist, delete the MAC address from the box and click 'Save'.

7.6 Internet Content Adaptation Protocol

The Internet Content Adaptation Protocol (ICAP) allows services to adapt, filter and translate content over the internet. For example, you can prevent data exfiltration from your network by entering the IP and ICAP port of a server running Comodo Dome Data Protection or Comodo Dome Secure Web Gateway services.

To open the 'ICAP Services' screen, click 'Services' on the left then 'ICAP'



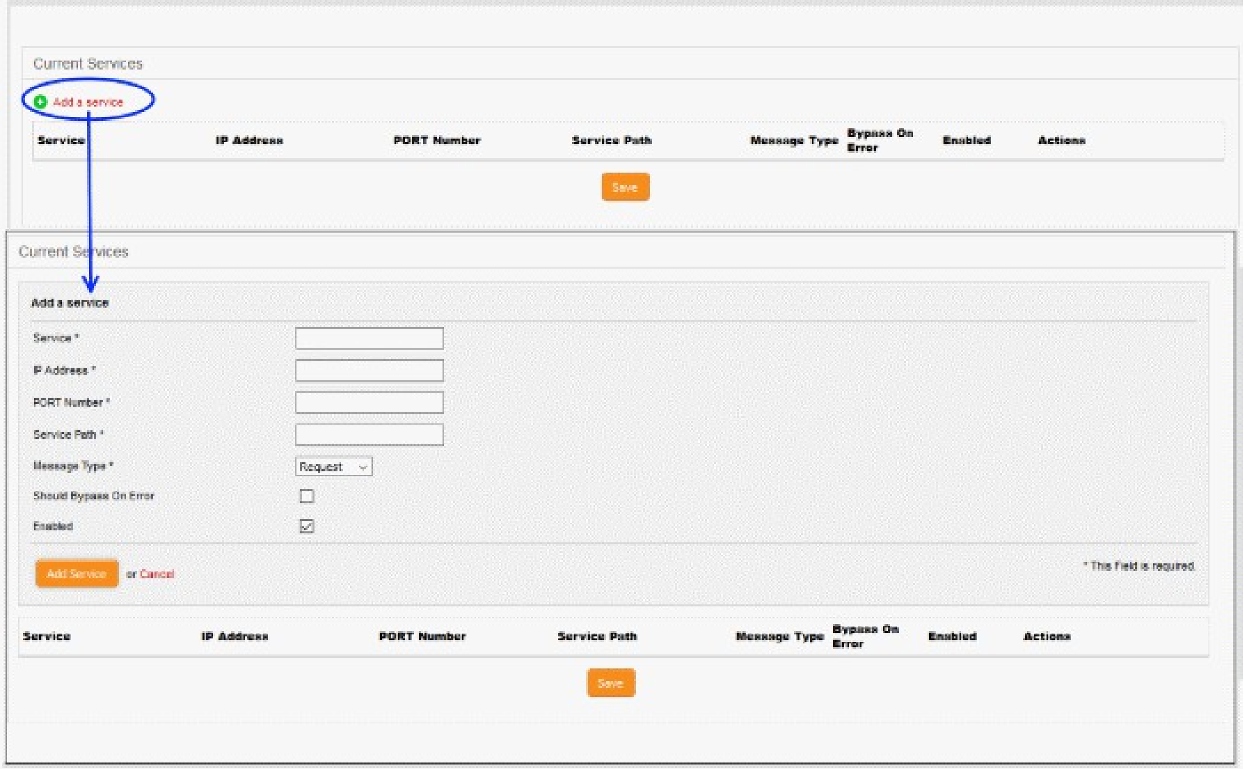
Current Services

Add a service

Service	IP Address	PORT Number	Service Path	Message Type	Bypass On Error	Enabled	Actions

To add ICAP service:

- Click 'Add a service' at the top



Current Services

Add a service

Service	IP Address	PORT Number	Service Path	Message Type	Bypass On Error	Enabled	Actions

Save

Current Services

Add a service

Service *	
IP Address *	
PORT Number *	
Service Path *	
Message Type *	Request
Should Bypass On Error	□
Enabled	☑

Add Service or Cancel

* This Field is required

Service	IP Address	PORT Number	Service Path	Message Type	Bypass On Error	Enabled	Actions

Save

- Service - Enter the service name, for example : 'Dome Data Protection'
- IP Address - Enter IP address of the node on which the service is installed
- Port Number - Enter the ICAP service port number.
- Service Path - Enter the path where the service is located.
- Message Type - Choose the message type of the data packet from the drop down.
- Check the options 'Should Bypass on Error' as per your requirement.
- If you need to have the service enabled, leave the 'Enable' option checked. Please note that this option is enabled by default.

- Click the 'Add Service' button at the bottom.

7.7 Quality of Service

- Quality of Service (QoS) rules allow you to set the priority of traffic used by various services according to their importance to your organization.
- For example, you may wish to prioritize traffic for interactive services like VoIP over traffic for data transfer.
- You can set bandwidth for both incoming and outgoing traffic.

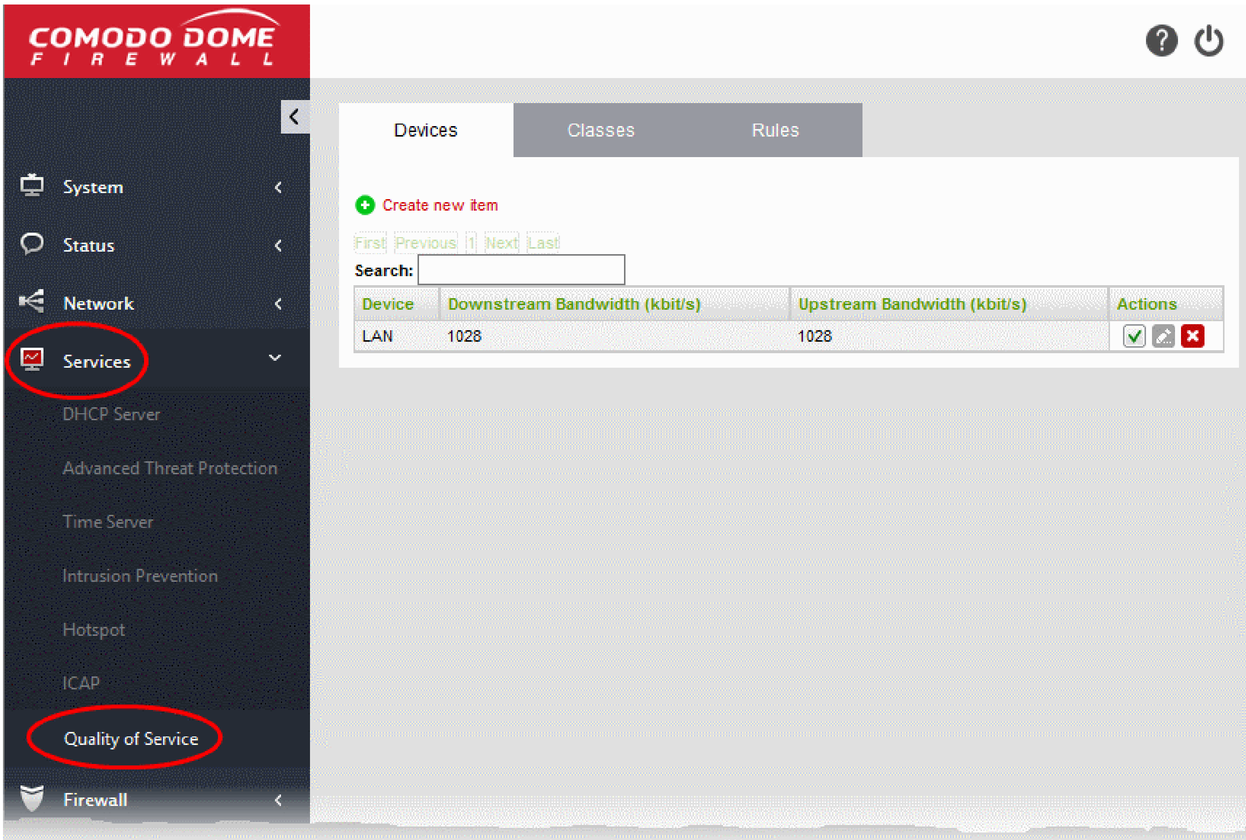
A QoS rule is built from three building blocks:

- **Target Device** - A target device is a network interface (LAN, WiFI, Uplink, etc) or network zone to which bandwidth controls are applied. Administrators can allocate maximum downstream and upstream bandwidth in Kbits/s for each selected device. Devices need to be defined before creating classes and rules.
- **Class** - Classes are logical groups of traffic with specific bandwidth throttling settings. For each device you create, four default 'classes' are automatically created with high, medium, low and bulk traffic priority levels. Administrators can edit the settings of these default classes and add new classes as required. Classes can be added to the rules that you deploy.
- **Rule** - Implementation of a bandwidth 'class' to the traffic of a selected service from/to a device. Administrators can select traffic according to services (ex: TCP port 22), traffic source or TOS/DSCP flag

(Standard IP header) and can apply a traffic class that has been defined previously.

The QoS rules can be created from the Quality of Services interface.

- Click 'Services' on the left and select 'Quality of Service' .



Device	Downstream Bandwidth (kbit/s)	Upstream Bandwidth (kbit/s)	Actions
LAN	1028	1028	✓ ✎ ✖

The interface contains three tabs:

- **Devices**
- **Classes**
- **Rules**

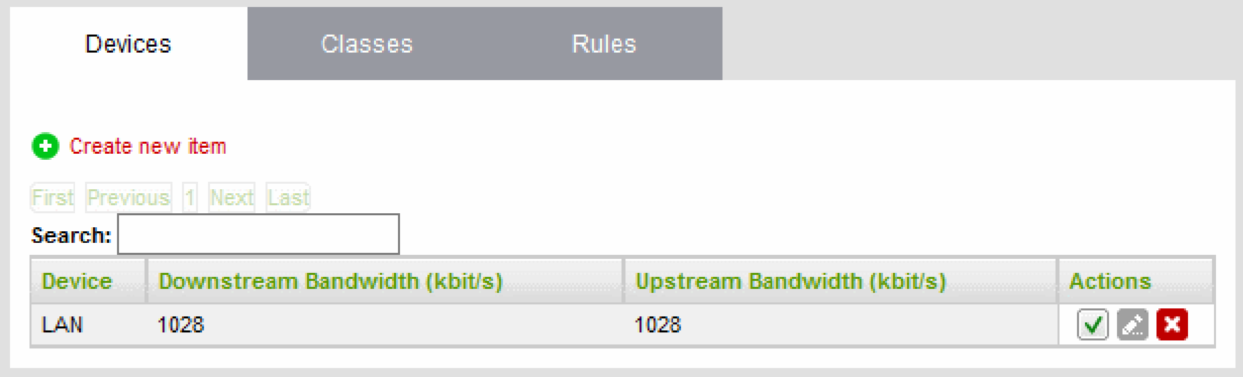
Devices

The 'Devices' tab displays the list of target interfaces configured with bandwidth resource allocations and allows you to define new target device to be used in a QoS rule.

A target device is a combination of interface device 'Type' (LAN, WiFI, Uplink etc) and that interface's maximum downstream and upstream bandwidth, in Kbits/s.

- It is possible to specify more than one device of the same type. For example, LAN 1 may have a different upstream/downstream speeds to LAN 2
- Once a device is added, all devices of that type will be assigned a color designation to easily identify that type. For example, all 'WIFI' devices will be assigned the color 'Blue'.
- Four default 'Classes' (bandwidth rules) will be automatically created for each device in the 'Classes' tab. These classes are suggestions. They have not yet been applied to any device and can be edited at at anytime.
- Devices are used to form the basis of 'Classes'

See **Step 1 - Define the target device for QoS rule** for more details about creating a new target device.



Device	Downstream Bandwidth (kbit/s)	Upstream Bandwidth (kbit/s)	Actions
LAN	1028	1028	✓ ✎ ☒

QoS Devices Table - Column Descriptions	
Column	**Description**
Device	The target network interface device for a QoS rule
Downstream Bandwidth (kbit/s)	The allotted bandwidth for incoming traffic for the device in kbits/sec
Upstream Bandwidth (kbit/s)	The allotted bandwidth for outgoing traffic for the device in kbits/sec
Actions	Controls for managing the device. ✓ - Enable or disable the device ✎ - Modify the device parameters. The 'Edit' interface is similar to creating a new target device for a QoS rule. See **Step 1 - Define the target device for QoS rule** for more details. ☒ - Remove the device.

Classes

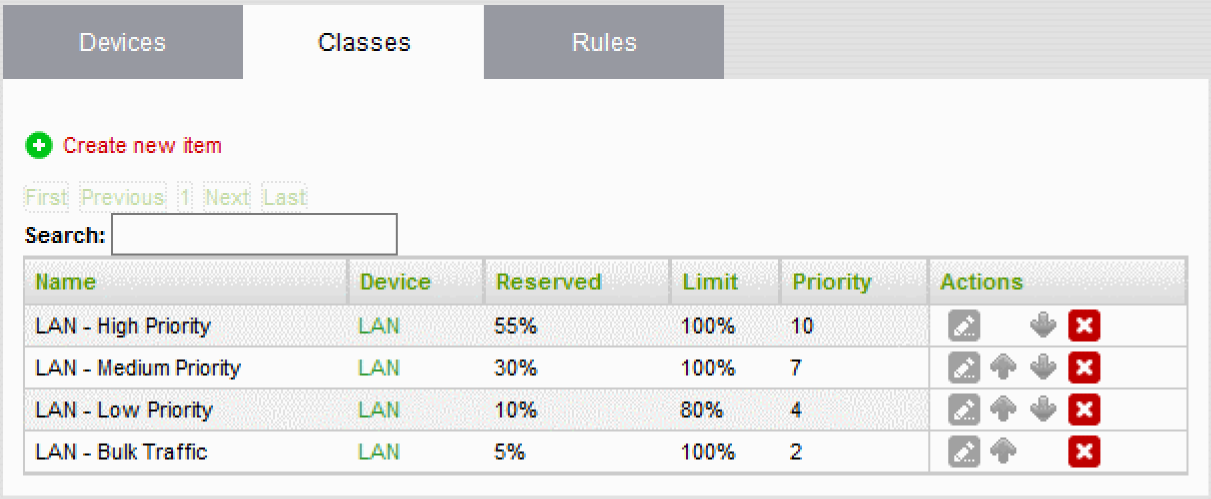
The 'Classes' tab contains a list of bandwidth throttling settings which can be added to a rule. Rules are, in turn, applied to a specific type of traffic. Four priority classes are available for each target device listed in the 'Devices' tab:

- High Priority
- Medium Priority
- Low Priority
- Bulk Traffic

The classes above can be edited as required:

- Admins can modify the maximum and minimum % of available bandwidth that can be used by a class. Available bandwidth was determined in the 'Devices' section.
- Admins can apply 'priority' (High, Medium, low). This determines the process priority level assigned to the traffic relevant to the service defined in the rule.
- Classes can be ordered using the arrow buttons. Classes at the top are the first to be processed when there is insufficient bandwidth for all traffic.

The interface allows administrators to edit existing classes and add new classes. See **Step 2 - Manage QoS classes** for more details.



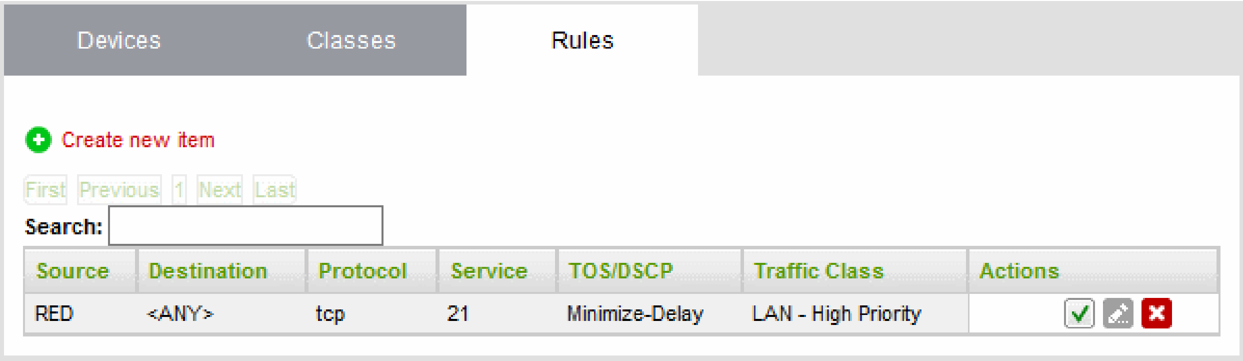
Name	Device	Reserved	Limit	Priority	Actions
LAN - High Priority	LAN	55%	100%	10	
LAN - Medium Priority	LAN	30%	100%	7	
LAN - Low Priority	LAN	10%	80%	4	
LAN - Bulk Traffic	LAN	5%	100%	2	

QoS Classes Table - Column Descriptions

Column	Description
Name	The label of the class. The auto-created classes include the target device name and the priority in their names.
Device	The target device associated with the class
Reserved	The bandwidth resource reserved for the class, shown as percentage of the bandwidth allotted for the target device
Limit	The maximum bandwidth resource that may be used the class, shown as percentage of the bandwidth allotted for the target device
Priority	The priority allotted to the class.
Actions	Controls for managing the class item. ✎ - Opens the 'Edit' interface and enables to edit the parameters of the class. Refer to the section **Step 2 - Manage QoS classes** for more details. ▲ / ▼ - The arrows allow the administrator to move the class up or down. The classes are processed in order from the top for prioritizing traffic when the available bandwidth for the firewall falls below sufficient level. ☒ - Remove the class.

Rules

A QoS Rule defines which bandwidth class should be applied to traffic pertaining to a specific service. The 'Rules' tab lets you view existing rules and create new rules to specify the traffic class for a selected service.



Source	Destination	Protocol	Service	TOS/DSCP	Traffic Class	Actions
RED	<ANY>	tcp	21	Minimize-Delay	LAN - High Priority	✓ ✎ ✖

QoS Rules Table - Column Descriptions	
Column	**Description**
Source	The source of the traffic pertaining to the service for which the rule is created. The source can be a network zone, interface device, a network, IP address or a MAC Address.
Destination	The destination of the traffic. The destination can be a network zone or IP address(es) connected to the target network interface device specified in the Traffic Class column.
Protocol	The protocol adopted by the traffic.
Service	The service for which the rule is created.
TOS/DSCP	The Type of Service (TOS)/Differentiated Services Code Point (DSCP) of the service.
Traffic Class	Select the QoS Class for the traffic.
Actions	Controls for managing the rule. ✓ - Enable or disable the rule. ✎ - Open the 'Edit' interface and enables to edit the parameters of the rule. The Edit interface is similar to Add QoS Rule interface. Refer to the section **Step 3 - Create QoS rule for the service** for more details. ✖ - Remove the rule.

Add a Qos Rule

Defining a QoS rule involves three steps:

- **Step 1 - Define the target device for Qos Rule**
- **Step 2 - Manage QoS classes**
- **Step 3 - Create QoS rule for the service**

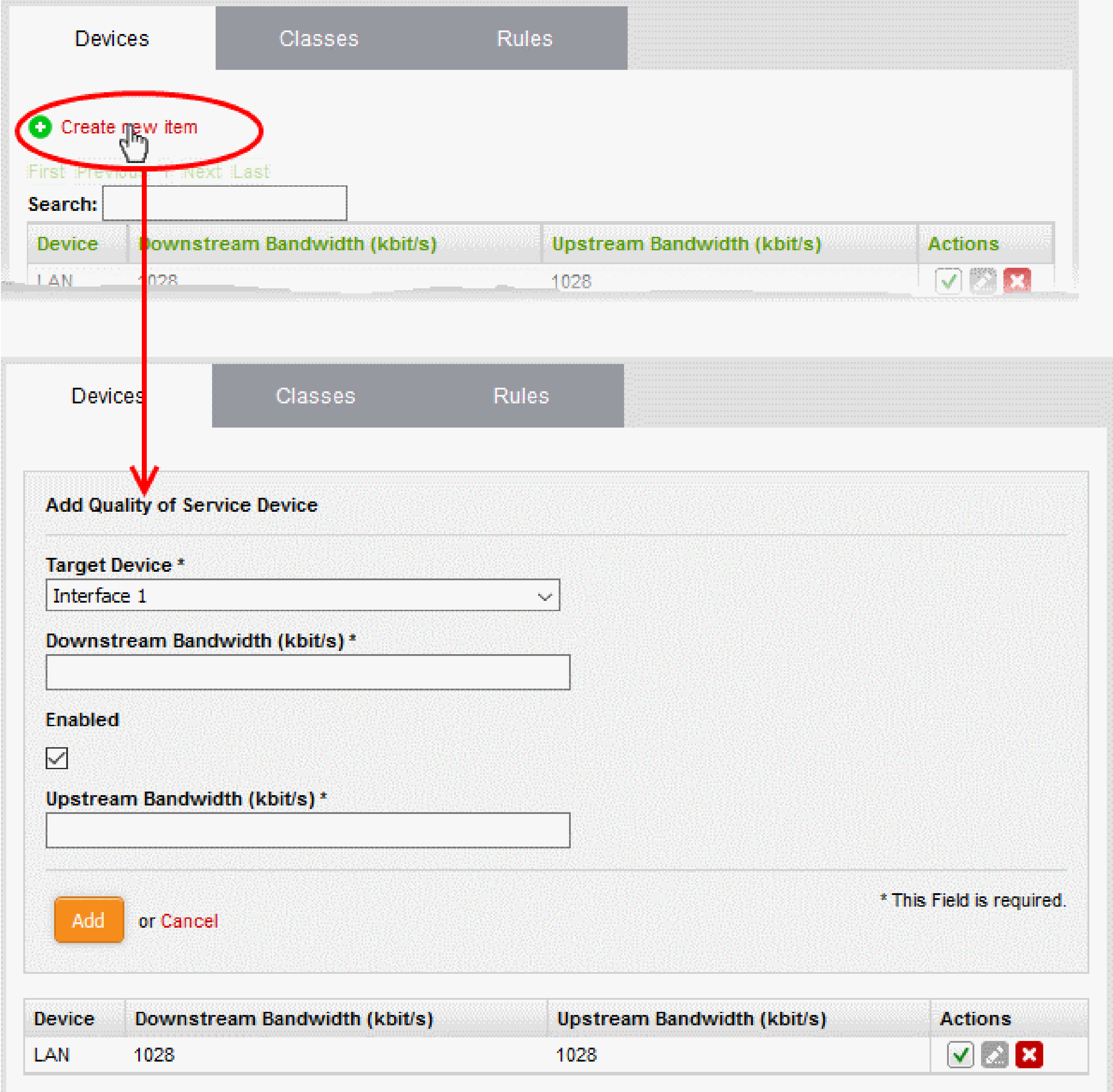
Step 1 - Define the target device for QoS rule

The first step in creating a QoS rule for a service is to define a target network interface device with pre-allotted bandwidth resource usage.

To create a target device

- Click 'Services' > 'Quality of Service' on the left
- Select the 'Devices' tab
- Click the Create new item link at the top left

The 'Add Quality of Service Device' pane will open.



Device	Downstream Bandwidth (kbit/s)	Upstream Bandwidth (kbit/s)	Actions
LAN	1028	1028	✓

Add Quality of Service Device

Target Device *
Interface 1

Downstream Bandwidth (kbit/s) *

Enabled
☑

Upstream Bandwidth (kbit/s) *

Add or Cancel

* This Field is required.

Device	Downstream Bandwidth (kbit/s)	Upstream Bandwidth (kbit/s)	Actions
LAN	1028	1028	✓

- Enter the parameters for the new target device as shown below:
    - Target Device - Select the network interface device from the drop-down
    - Downstream Bandwidth - Enter the usable bandwidth for incoming traffic in kbits/sec
    - Upstream Bandwidth - Enter the usable bandwidth for outgoing traffic in kbits/sec
    - Enabled -Select this checkbox to activate the device immediately upon creation
- Click 'Add' to save the target device with its bandwidth resource allocations.

The target device will be added to the 'Devices' list.

Step 2 - Manage the QoS classes

For each target device added under the 'Devices' tab, four classes are automatically created with different priority levels:

- High Priority
- Medium Priority
- Low Priority

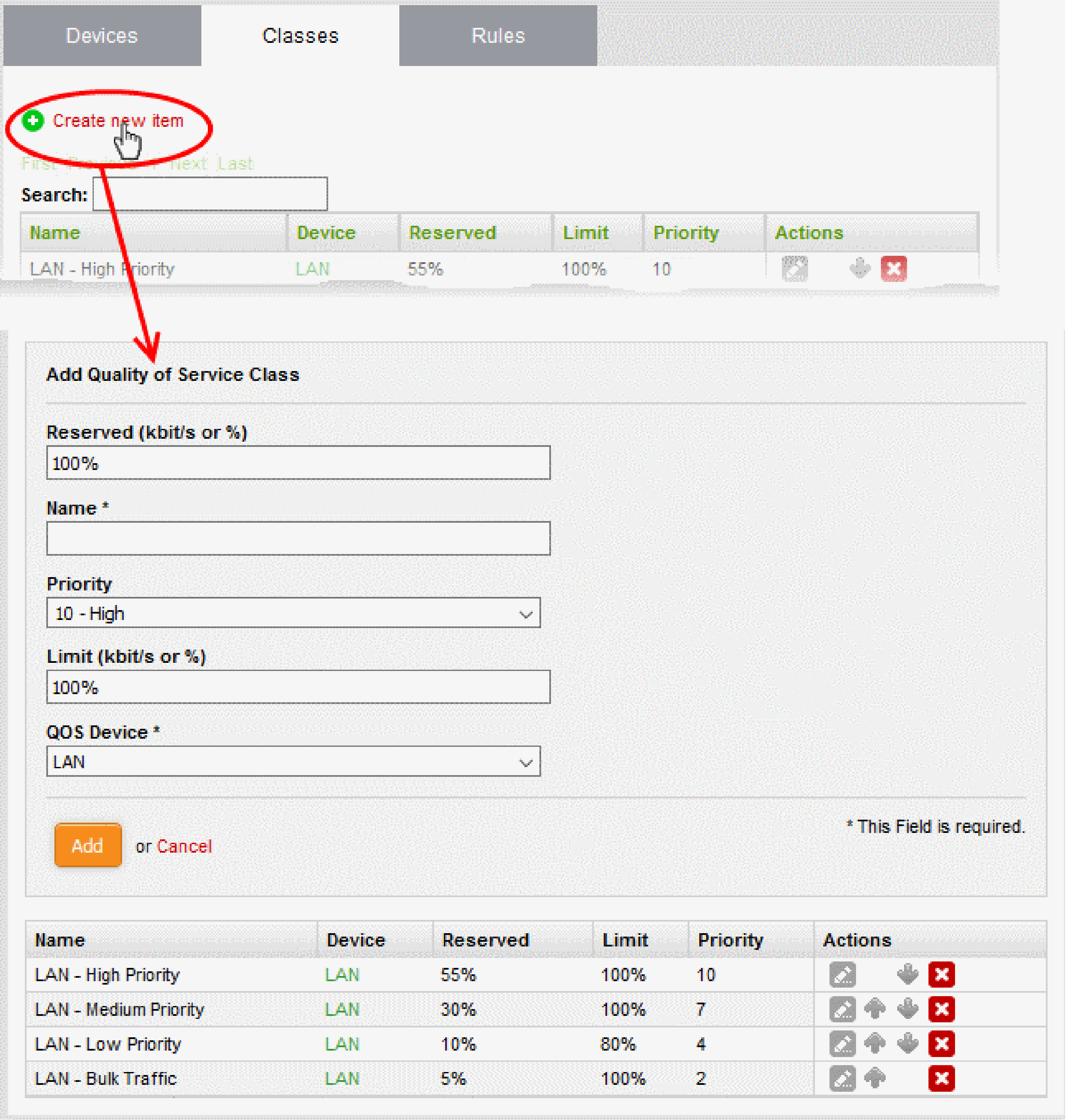
- Bulk Traffic

Each class will be assigned with reserved bandwidth usage from the bandwidth allotted to the target device and a priority ranking between one and ten. The administrator can edit these parameters of the auto-created classes and change their order in the list of classes as the classes and hence the rules using these classes, are processed in order from the top for prioritizing traffic when the available bandwidth for the UTM appliance falls below sufficient level. If needed, the administrator can create new QoC classes for use in rules.

To add a new class

- Open the 'Quality of Service Classes' interface by clicking the 'Classes' tab under 'Services' > 'Quality of Service'
- Click the Create new item link at the top left

The 'Add Quality of Service Class' pane will open.



Search:

Name	Device	Reserved	Limit	Priority	Actions
LAN - High Priority	LAN	55%	100%	10	✎ ↓ ✖

Add Quality of Service Class

Reserved (kbit/s or %)
100%

Name *

Priority
10 - High

Limit (kbit/s or %)
100%

QOS Device *
LAN

* This Field is required.

Name	Device	Reserved	Limit	Priority	Actions
LAN - High Priority	LAN	55%	100%	10	✎ ↓ ✖
LAN - Medium Priority	LAN	30%	100%	7	✎ ↑ ↓ ✖
LAN - Low Priority	LAN	10%	80%	4	✎ ↑ ↓ ✖
LAN - Bulk Traffic	LAN	5%	100%	2	✎ ↑ ✖

- Enter the parameters for the new class as shown below:
  - Reserved - Specify the bandwidth usage that can be reserved for the class, as a percentage of the overall bandwidth resource allotted to the target device. You can choose the target device from the

QOS Device drop-down in the same pane..

- Name - The name of the class for identification.
- Priority - The priority ranking for the class, chosen between 1 an 10 from the drop-down
- Limit - The maximum percentage of the overall bandwidth resource available to the target device, that can be assigned to the class
- QoS Device - The target device for which the class is created, chosen from the drop-down

Note: The sum of the reserved bandwidths for all the classes pertaining to a single device cannot exceed 100%. The reserved bandwidth for a single class cannot exceed its limit bandwidth.

- Click 'Save' to add the QoS class to the list.

To modify the parameters of a class

- Click the 'Edit' icon in the row of the class to be edited, from the Actions column.

The 'Edit' pane will appear, enabling the administrator to modify required parameters. The edit pane is similar to the 'Add Quality of Service Class' pane. Refer to the section above for more details.

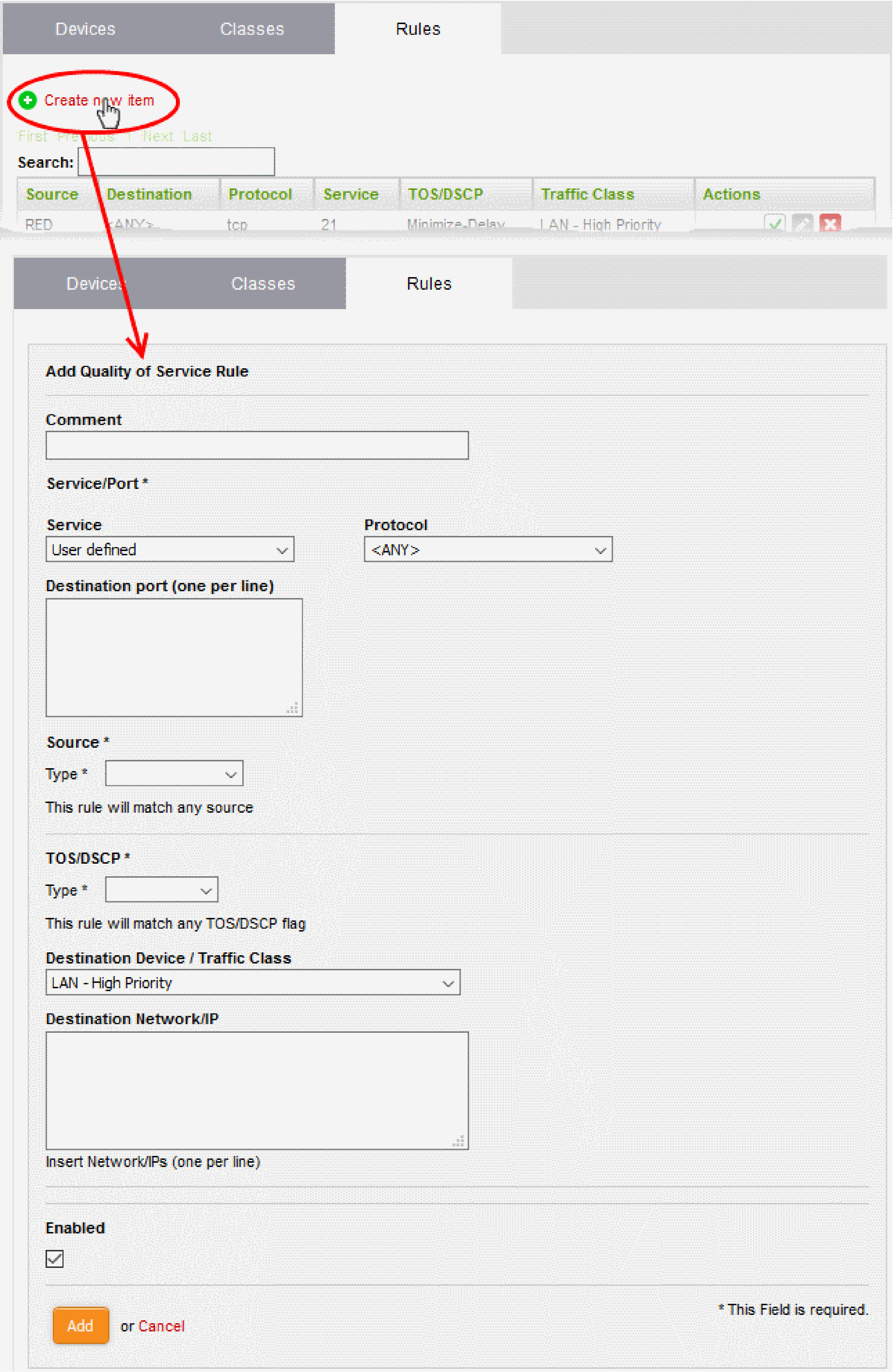
Step 3 - Create QoS rule for the service

You can specify QoS rule that specifies the QoS class to be adopted by the type of traffic pertaining to a specified class.

To create a new rule

- Open the 'Quality of Service Rules' interface by clicking the 'Rules' tab under 'Services' > 'Quality of Service'
- Click the 'Create new item' link at the top left

The 'Add Quality of Service Rule' pane will open.



Search:

Source	Destination	Protocol	Service	TOS/DSCP	Traffic Class	Actions
RED	<ANY>	tcp	21	Minimize-Delay	LAN - High Priority	✓

Add Quality of Service Rule

Comment

Service/Port *

Service: User defined

Protocol: <ANY>

Destination port (one per line)

Source *

Type *

This rule will match any source

TOS/DSCP *

Type *

This rule will match any TOS/DSCP flag

Destination Device / Traffic Class: LAN - High Priority

Destination Network/IP

Insert Network/IPs (one per line)

Enabled

☑

* This Field is required.

- Enter the parameters for the new rule as shown below:
    - Comment - Enter a short description for the rule
- **Service/Port** - The Service/Port area enables you to specify the service for which the rule is created, the protocol used by the service and the destination port(s).
    - Service - Choose the type of service from the drop-down
    - Protocol - Choose the protocol used by the service
    - Destination port - Specify the destination port(s) of the service one by one, in the 'Destination Port' text box.

Tip: The appliance is loaded with predefined combinations of service/protocol/port, like HTTP/TCP/80, <ALL>/TCP+UDP/0:65535, or <ANY>, which is a shortcut for all services, protocols, and ports. If you want to specify custom protocol/port combination, then select 'User Defined' from the service. You can also specify additional destination ports for standard combinations, for the services that run on ports different from the standard ones.

- **Source** - The Source area enables you to specify the source from which the traffic pertaining to the service originates.
    - Choose the type of the source from the Type drop-down. Depending on the chosen type, you need to specify the values in the text box that appears on selecting the type. The options available are:
        - Zone/Interface - If the source is a Network Zone/Interface, select the network zone(s)/interface device(s) from the Select interfaces text box.
        - Network/IP - If the source is external network(s) or a machine(s), enter the network address(es) or IP address(es) one by one in the text box.
        - MAC Address - If the source is machine(s) identified by its/their MAC address(es), enter the MAC address(es) one by one in the textbox.
- **TOS/DSCP** - The TOS/DSCP area enables you to specify the Type of Service (TOS) or Differentiated Services Code Point (DSCP) parameters,
    - Choose the type of the TOS/DSCP parameter to be specified from the Type drop-down. Depending on the chosen type, you need to specify the values in the text box that appears on selecting the type. The options available are:
        - TOS - Choose the TOS flag from the Match traffic drop-down, so that the traffic containing the flag will be applied with the rule
        - DSCP Class - Choose the DSCP class from the Match traffic drop-down, so that the traffic with the DSCP class will be applied with the rule
        - DSCP Value - Enter the DSCP value in the Match traffic text box, so that the traffic with the DSCP value will be applied with the rule
- **Destination Device/Traffic Class** - The Destination Device/Traffic Class area allows you to select the QOS class to be used for the traffic and the Destination Netwrok/IP.
    - The first drop-down displays all the classes added to the QoS Classes interface. Choose the class from the drop-downs
    - Enter the network address or IP address of the destination of the traffic in the Destination Network/IP textbox
    - Enabled - Select the checkbox if you wish the rule to take effect immediately upon creation.
- Click 'Add' to save your rule. The rule will be added to the Qos Rules list and will be applied to the traffic, if enabled.

8 Manage Firewall Configuration

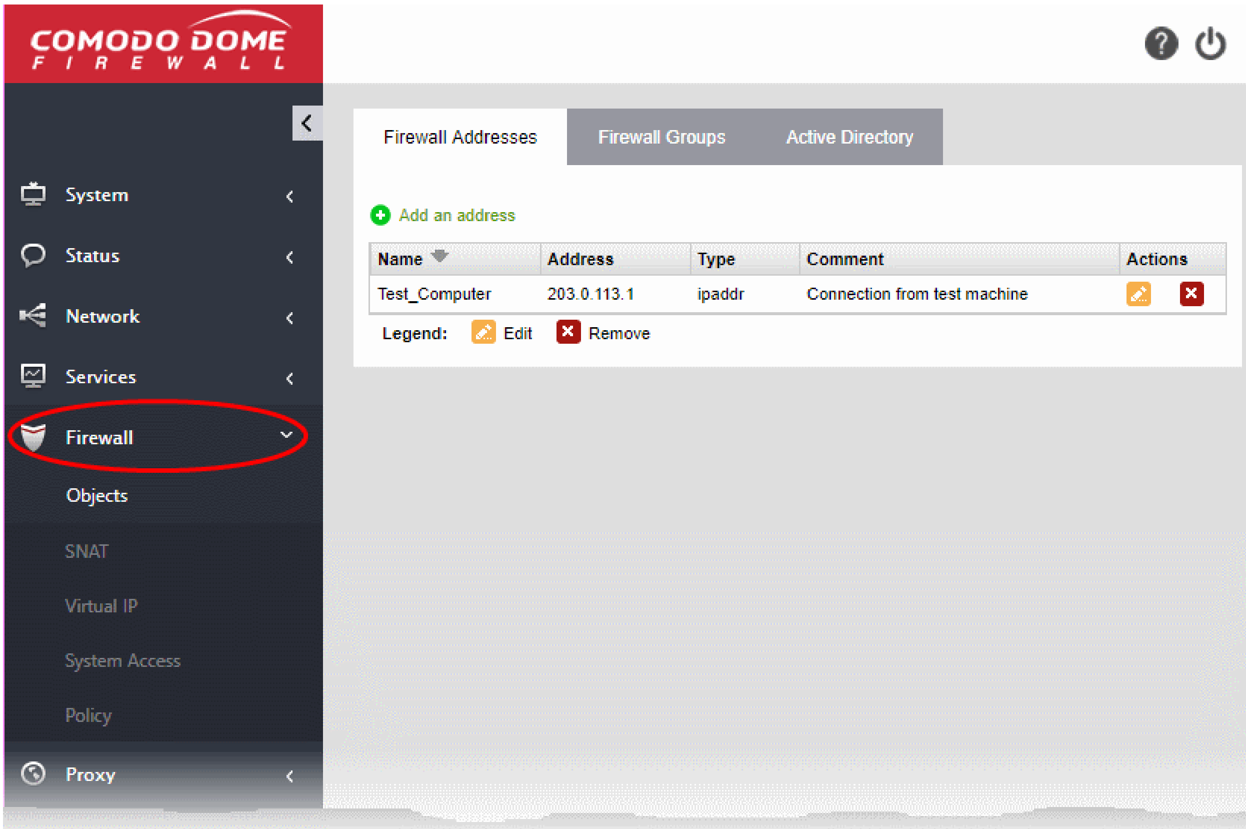
Comodo Dome Firewall contains a highly configurable packet filtering firewall which offers the highest levels of security against inbound and outbound threats.

The firewall allows you to create rules to manage the following types of traffic:

- NAT - Network address translation (NAT) for traffic from a host in the network to external (SNAT), traffic from external source directed to a host in the network (Virtual IP) with port forwarding
- Incoming traffic - Traffic from external network zones to hosts in the internal network zone
- Outgoing traffic - Traffic from hosts to the external network zone
- Inter-zone traffic - Traffic between network zones connected to the virtual appliance
- VPN traffic - Traffic generated by VPN users
- System Access - Access to the DFW virtual appliance

Each kind of traffic requires a specific type of rule in order to allow or block traffic of that type.

- In addition to any rules that you create, the virtual appliance generates a set of 'System Rules' which cannot be disabled or edited.
- System rules are essential to ensure interoperability between firewall services and your network infrastructure.
- Click the 'Firewall' link on the left to open a sub-menu which allows you to create and manage rules.



Name	Address	Type	Comment	Actions
Test_Computer	203.0.113.1	ipaddr	Connection from test machine	✎ ☒

Legend: ✎ Edit ☒ Remove

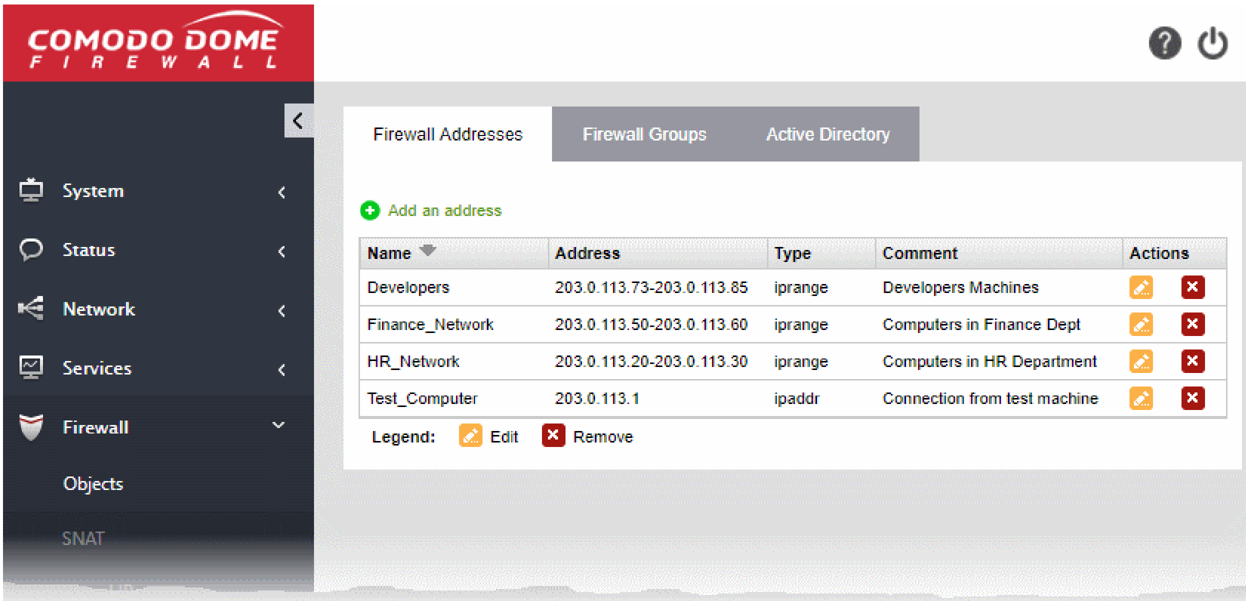
The following sections provide detailed descriptions on rule construction for each firewall module:

- **Firewall Objects**
- **Source Network Address Translation**
- **Configuring Virtual IP for Destination Network Address Translation**

- **Configuring System Access**
- **Configuring Firewall Policy Rules and VPN Traffic Rules**

8.1 Firewall Objects

- Click 'Firewall' > 'Objects' to open the firewall objects interface.
  - A firewall address object can be a network IP address, a range of IP addresses, a sub-net, or a domain (FQDN)
  - Once defined, a firewall object can added as the source or destination address to firewall rules, SNAT rules, Virtual IP rules and System Access rules.
    - Firewall rules are configured in 'Firewall' > 'Policy'
    - SNAT rules are configured in 'Firewall' > 'SNAT'
    - Virtual IP for DNAT rules are configured in 'Firewall' > 'Virtual IP'
    - System Access rules are configured in 'Firewall' > 'System Access'
  - Objects can be edited at any time to change the referenced host(s).
  - If you change the addresses in an object, the change will be propagated to all firewall rules which include the object. This saves time over editing each individual firewall rule.
  - A firewall object group can include multiple firewall objects. Firewall object groups can also be added to rules.
  - The 'Active Directory' tab lets you integrate an LDAP server to create objects from AD users and user groups. AD objects can then be added to Firewall Address and Firewall Group objects. After adding the firewall object to a rule, the rule's settings will apply to all users in the AD object.



Name	Address	Type	Comment	Actions
Developers	203.0.113.73-203.0.113.85	iprange	Developers Machines	✎ ☒
Finance_Network	203.0.113.50-203.0.113.60	iprange	Computers in Finance Dept	✎ ☒
HR_Network	203.0.113.20-203.0.113.30	iprange	Computers in HR Department	✎ ☒
Test_Computer	203.0.113.1	ipaddr	Connection from test machine	✎ ☒

Legend: ✎ Edit ☒ Remove

The interface contains three tabs:

- **Firewall Addresses** - Create firewall address objects. See **Managing Firewall Address Objects** for more details.
- **Firewall Groups** - Create and manage groups of firewall objects. See **Managing Firewall Object Groups** for more details.
- **Active Directory** - Integrate your company's Active Directory (AD) server in order to import AD users and user groups as Firewall objects. See **Active Directory Integration** for more details.

8.1.1 Manage Firewall Address Objects

- Click 'Firewall' > 'Objects' to open the firewall objects interface.

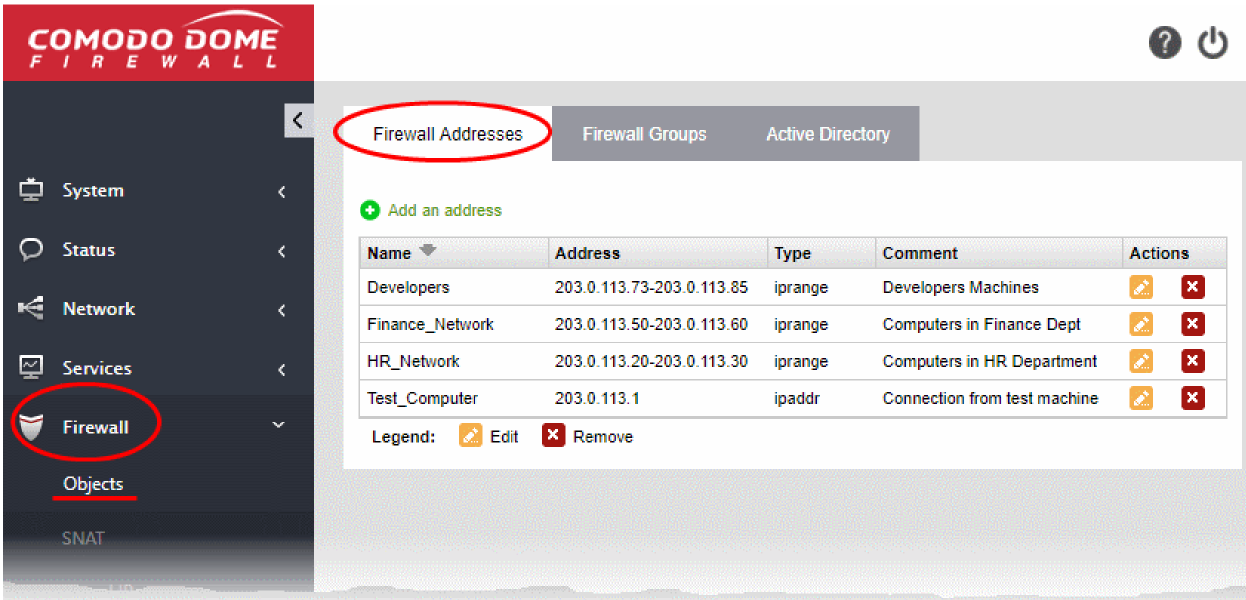
Firewall address objects represent a specific address or a group of addresses in your network.

- Firewall objects can then be referenced when creating a firewall rule, saving you time.
- You can also create firewall object groups to further streamline policy and rule creation.

Firewall address objects can be edited at anytime. Any change to an object will be reflected in all rules which include the object.

To create or manage firewall address objects

- Click 'Firewall' > 'Objects' in the left-hand menu.
- Click the 'Firewall Addresses' tab.



Name	Address	Type	Comment	Actions
Developers	203.0.113.73-203.0.113.85	iprange	Developers Machines	✎ ✖
Finance_Network	203.0.113.50-203.0.113.60	iprange	Computers in Finance Dept	✎ ✖
HR_Network	203.0.113.20-203.0.113.30	iprange	Computers in HR Department	✎ ✖
Test_Computer	203.0.113.1	ipaddr	Connection from test machine	✎ ✖

Legend: ✎ Edit ✖ Remove

The addresses interface shows all firewall address objects added to Dome Firewall and allows you to create new objects.

Firewall Address Objects Table - Column Descriptions	
Column	**Description**
Name	Label of the firewall address object. The object name will become available for selection in the 'source' and 'destination' address fields when creating a rule.
Address	IP addresse(s) of host computer(s) contained in the object.
Type	Category of address. Can be IP address, IP range, subnet or fully qualified domain name (FQDN).
Comment	A short description of the object
Actions	Control buttons to manage the object. ✎ - Edit. Allows you to modify object parameters. The Edit interface is similar to the 'Add Object' interface. See **Creating a Firewall Address Object** for more details. ✖ - Removes the object. Note: The object which is currently referenced in a firewall rule or in a group cannot be removed. To remove a group, the group is to be first removed from the firewall rule or

	group in which it is included.

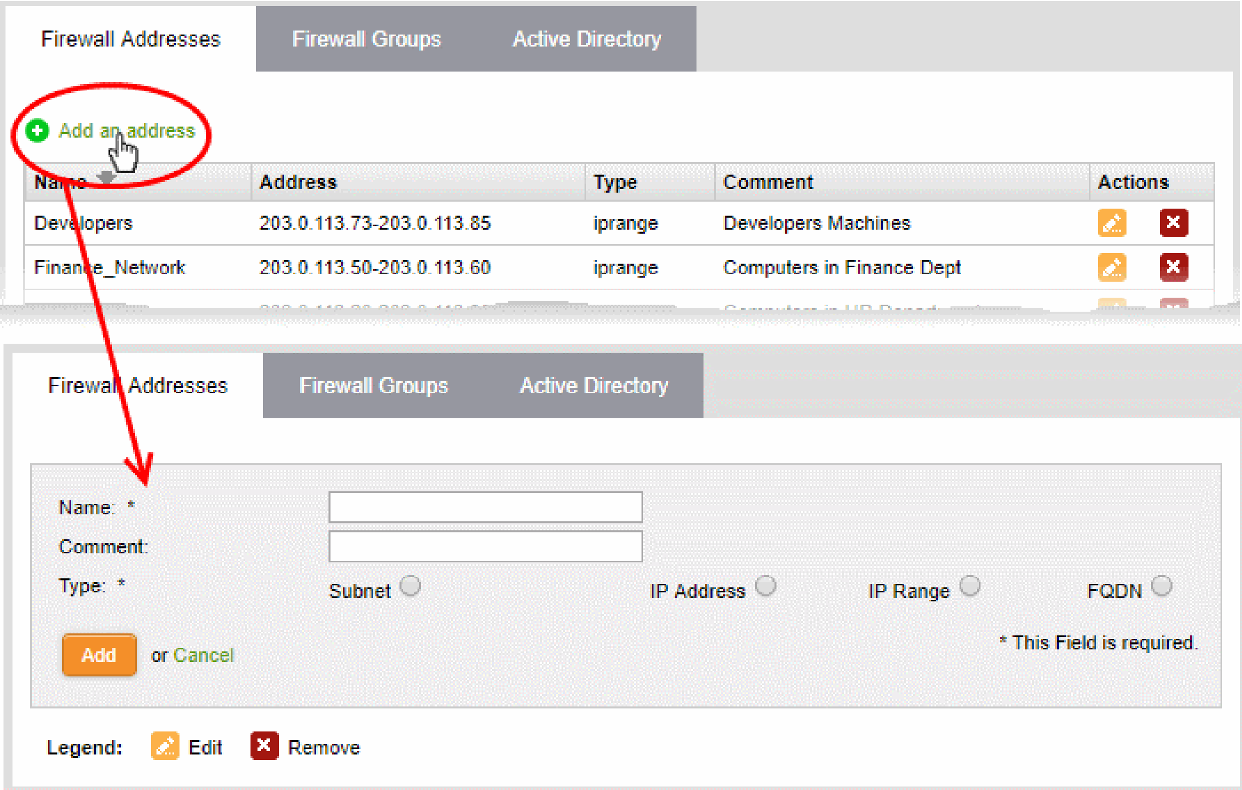
Create a Firewall Address Object

A firewall address object can be created in two ways:

- In the 'Add an Address' area. You need to define a name and addresses for the object. See below for more details.
- Import users from Active Directory. See **Adding Users to Firewall Objects** in **Active Directory Integration**.

To create a new object

- Click 'Firewall' > 'Objects' in the left-hand navigation
- Click the 'Firewall Addresses' tab
- Click 'Add an address':



Name	Address	Type	Comment	Actions
Developers	203.0.113.73-203.0.113.85	iprange	Developers Machines	✎ ✖
Finance_Network	203.0.113.50-203.0.113.60	iprange	Computers in Finance Dept	✎ ✖

Name: *

Comment:

Type: * Subnet ○ IP Address ○ IP Range ○ FQDN ○

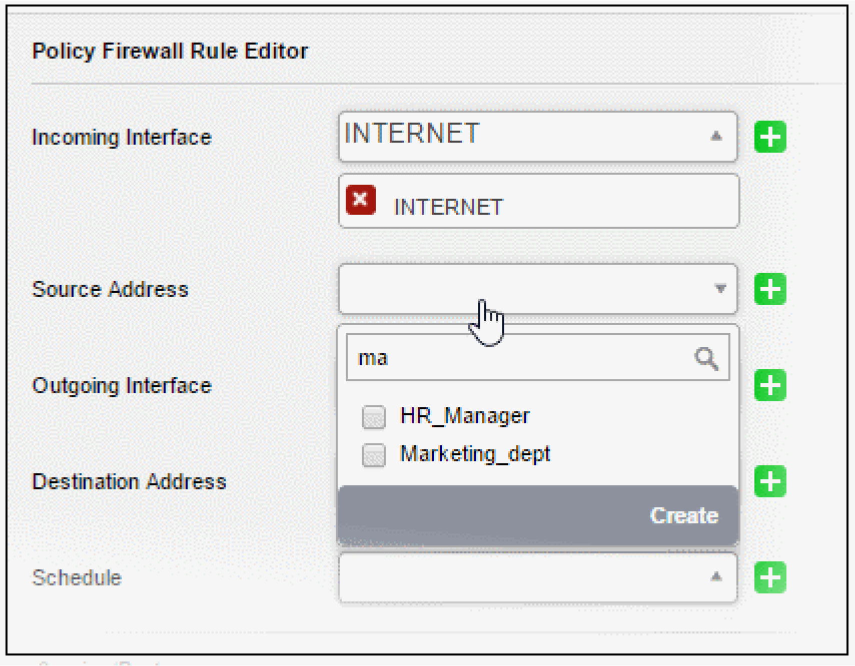
Add or Cancel

* This Field is required.

Legend: ✎ Edit ✖ Remove

- Enter the parameters for the new object as shown below:
  - **Name** - Create a label for the object (15 characters max). Only alphanumeric characters and two special characters '-' and '_' are allowed. Ideally, the object name should clearly identify the hosts in the object.
  - **Comment** - Enter a short description of the object.
  - **Type** - Address type. The available options are:
    - Subnet - Select if the object should point to a sub-network of computers. Enter the subnet address in the space provided.
    - IP address - Select if the object should point to a single IP address. Enter the address in the space provided.
    - IP range - Select if the object should point to a range of IP addresses. Enter the range in the space provided.
    - FQDN - Select if the object should point to a fully qualified domain name. Enter the domain in the space provided.

- Click 'Add'. The new object will be added to the list.
- The object will become available for selection as a source or destination when creating a firewall rule. You can locate the object by typing the first few letters of its name:



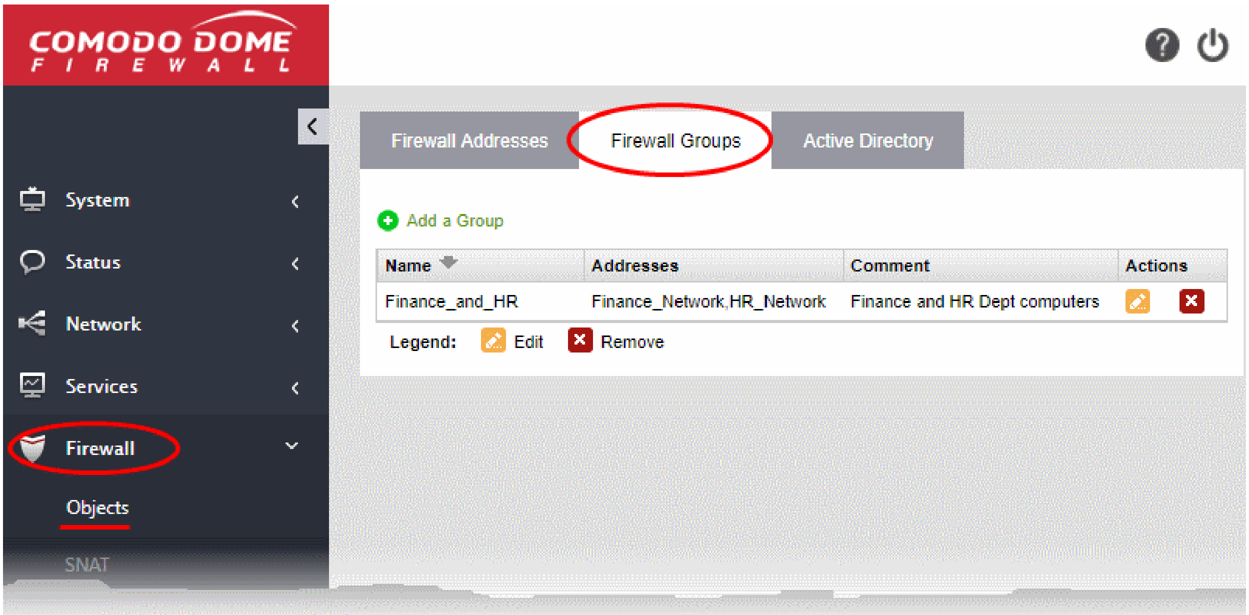
8.1.2 Manage Firewall Object Groups

- A firewall object group is a collection of firewall address objects.
- An object group can be referenced as a source or destination in a firewall rule.
- Object groups make it easier to create rules for large networks by allowing you to reference a single item instead of multiple items.

Object groups can be edited at anytime to change their member objects. The change will affect all firewall rules which contain the object group.

To create or manage firewall address object groups

- Click 'Firewall' on the left then 'Objects'
- Click the 'Firewall Groups' tab:



Name	Addresses	Comment	Actions
Finance_and_HR	Finance_Network,HR_Network	Finance and HR Dept computers	✎ ✖

- The groups interface lists all object groups that have been added to Comodo Dome Firewall.
- You can also create new groups and edit groups.

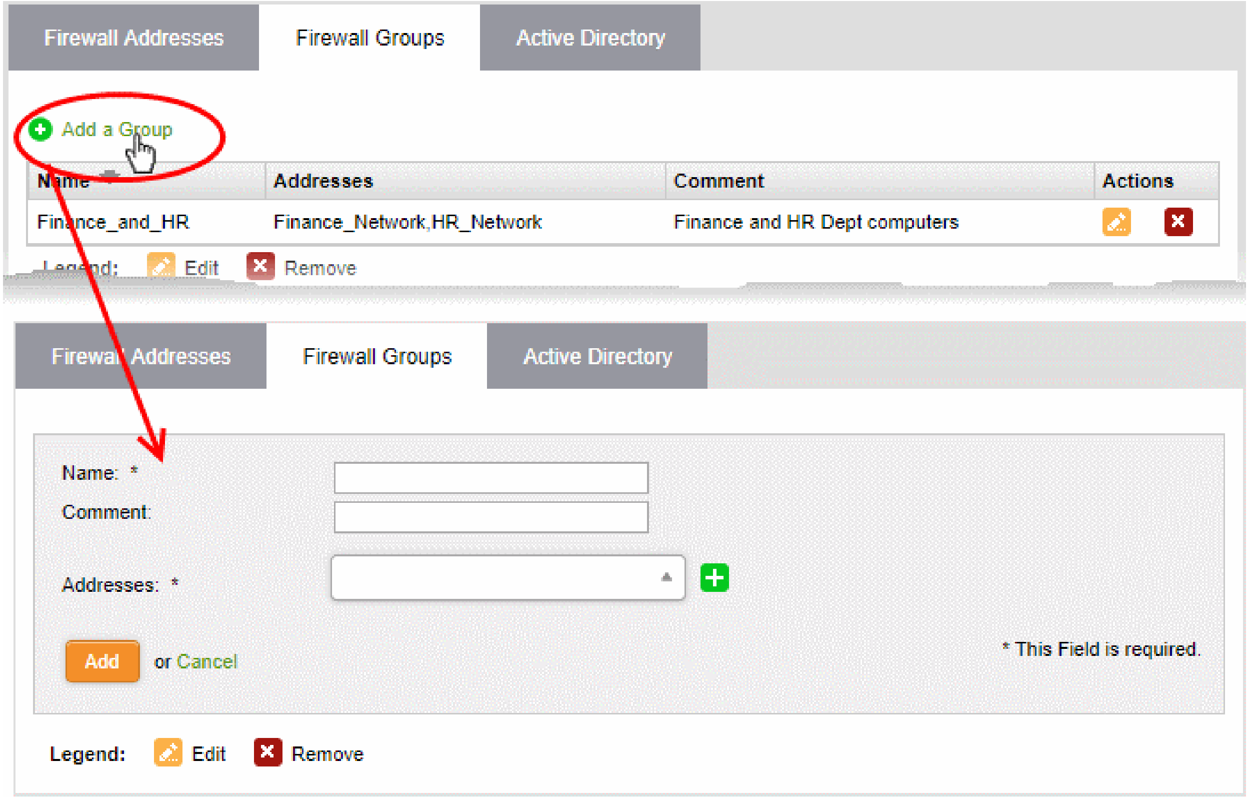
Firewall Groups Table - Column Descriptions	
Column	**Description**
Name	Label of the firewall address object group.
Addresses	The member objects of the group.
Comment	A short description of the object group.
Actions	Control buttons to manage the object group. ✎ - Edit. Allows you to modify group parameters. The edit interface is similar to the 'Add Group' interface. See **Create a Firewall Address Object Group** for more details. ✖ - Removes the object group. Note: You cannot remove object groups which are referenced in a firewall rule. You must remove the group from all rules before it can be deleted.

There are two ways to create an object group:

- In the 'Add a Group' area. You need to define a name and member objects for the group. See below for instructions.
- Import users from Active Directory. See **Adding User Groups as Firewall Object Groups** in **Active Directory Integration**.

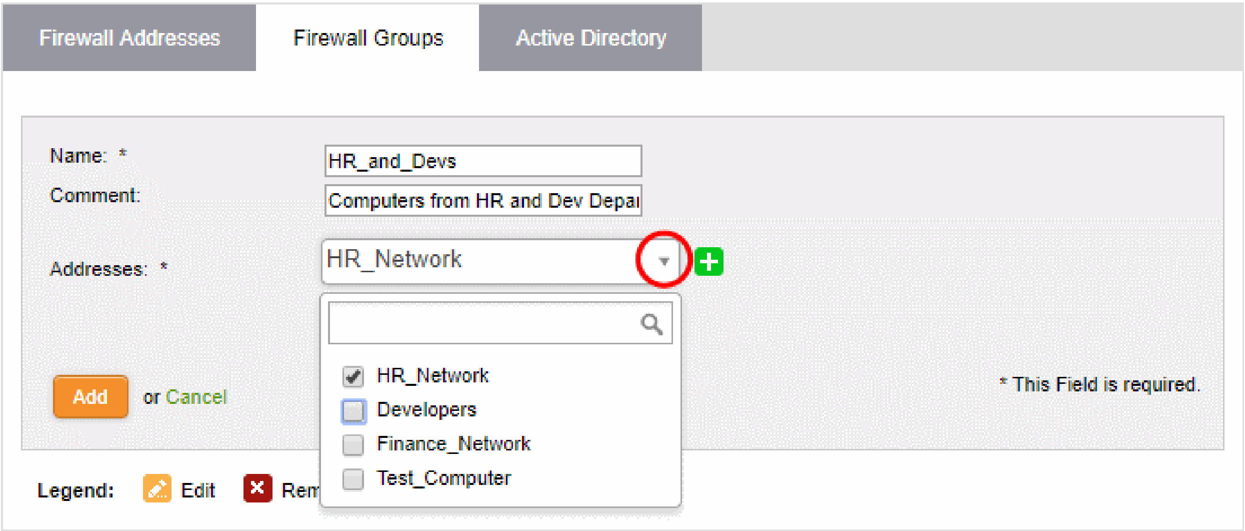
To create a new object group

- Click 'Firewall' on the left then choose 'Objects'
- Select the 'Firewall Groups' tab
- Click 'Add a group' at the top-left



Name	Addresses	Comment	Actions
Finance_and_HR	Finance_Network,HR_Network	Finance and HR Dept computers	✎ ✖

- Enter parameters for the new group as shown below:
  - **Name** - Label for the group (15 characters max).
  - **Comment** - Short description of the group.
  - **Addresses** - Select the firewall address objects to be included in the group.
    - Start typing an object name to locate the object in the drop-down
    - Use the check-boxes to select objects you wish to add to the group.



Name: * HR_and_Devs

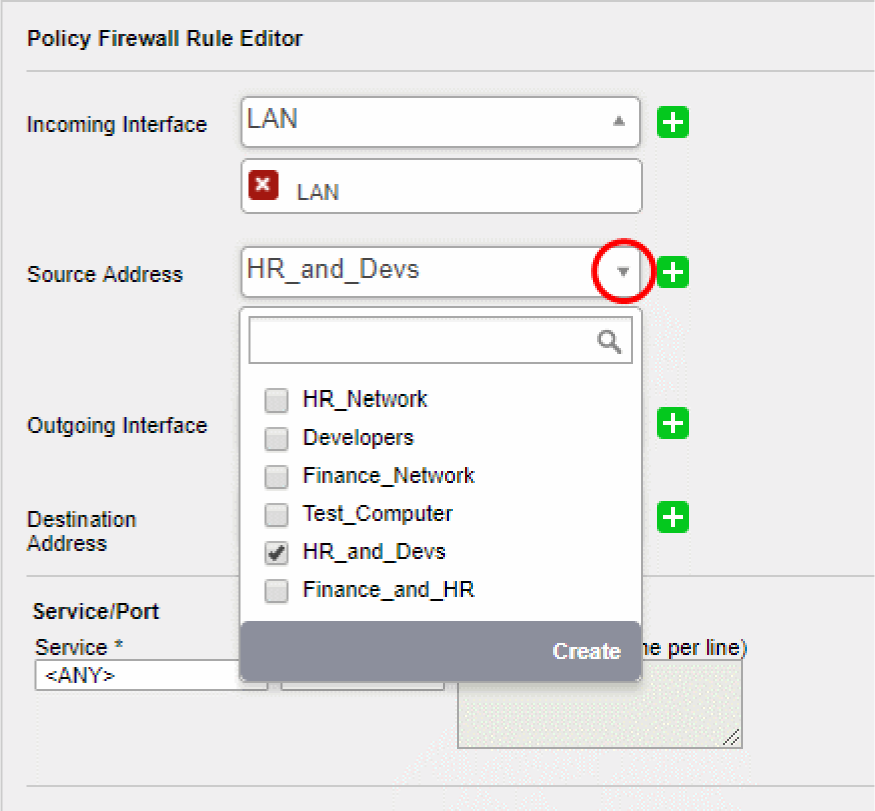
Comment: Computers from HR and Dev Depai

Addresses: * HR_Network

- ☑ HR_Network
- ☐ Developers
- ☐ Finance_Network
- ☐ Test_Computer

- Click 'Add'.

The group will be available for selection as a source or destination when creating a firewall rule.



8.1.3 Active Directory Integration

- Integrating Dome Firewall with your Active Directory (AD) server allows you to implement identity-based security on your network.
- Once a directory has been imported, Dome Firewall will map usernames to IP addresses, allowing you to apply firewall policies to individuals or groups.
- The firewall uses LDAP (Lightweight Directory Access Protocol) to import users from the AD server, track login activity, and regulate user traffic to and from IP addresses.

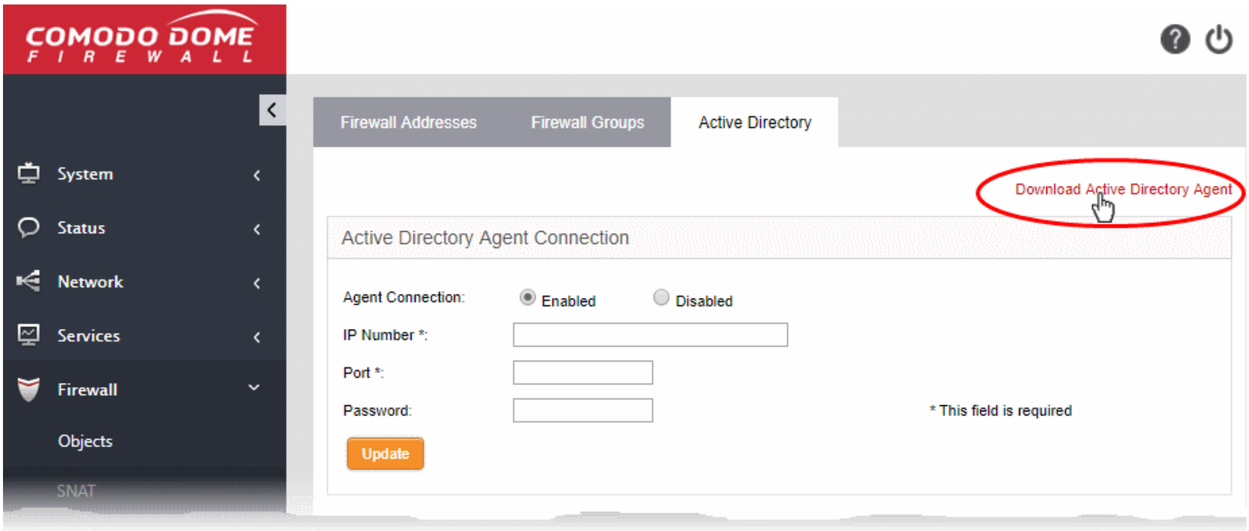
AD server integration involves four steps:

- **Step 1- Install the Comodo Dome Firewall AD Agent onto the AD Server**
- **Step 2 - Add Socket Exception for the AD Agent in the server**
- **Step 3 - Configure the AD Agent**
- **Step 4 - Configure the AD Agent connection and LDAP server connection to the virtual appliance**

Step 1- Install the Active Directory Agent onto your AD Server

You first need to install an agent on your AD server to facilitate communications:

1. Download the agent setup file:
   - Login to your Dome Firewall account
   - Click 'Firewall' on the left then 'Objects' > 'Active Directory'.
   - Click the 'Download Active Directory Agent' link at the top-right
   - Copy the setup files to your AD server



Active Directory Agent Connection

Agent Connection: ● Enabled ○ Disabled

IP Number *:

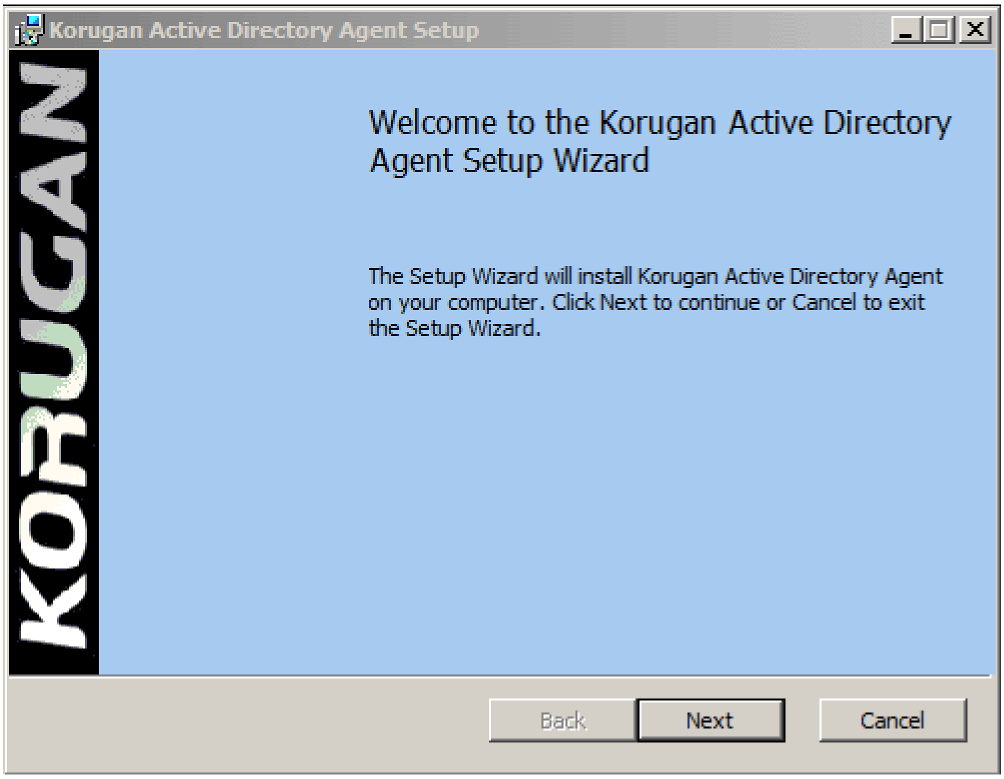
Port *:

Password:

* This field is required

Update

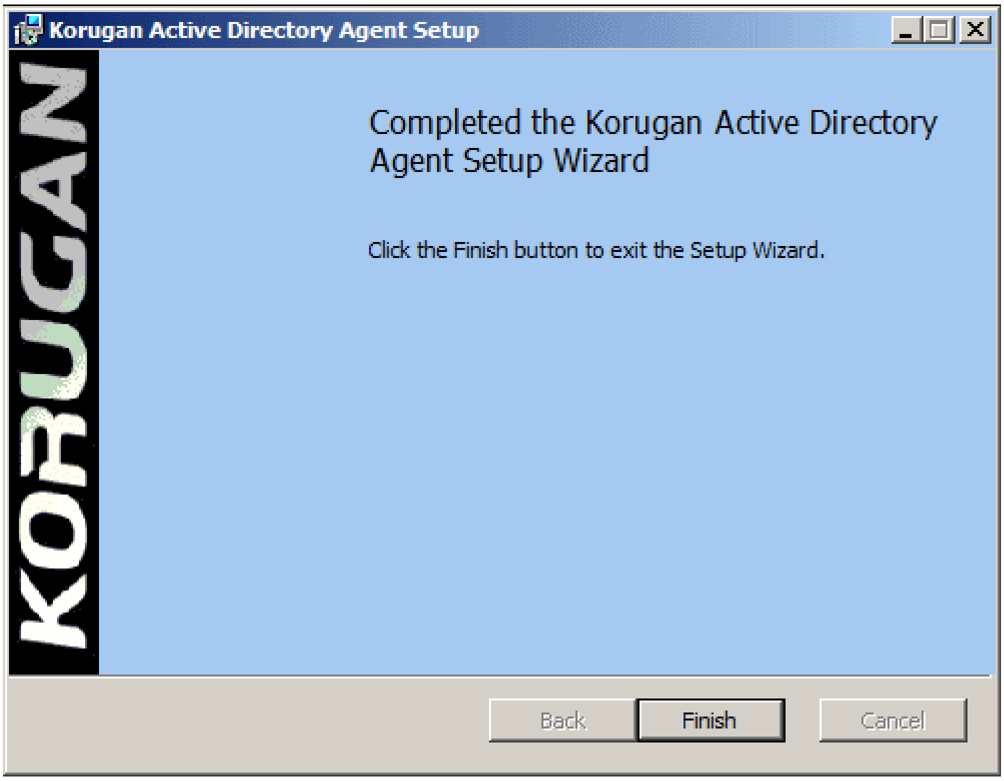
2. Open the setup file to start the installation wizard:



Welcome to the Korugan Active Directory Agent Setup Wizard

The Setup Wizard will install Korugan Active Directory Agent on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

3. Follow the wizard to complete the installation. By default, the agent will be installed to C:\Program Files (32 bit system) or C:\Program Files (x86) (64-bit system).



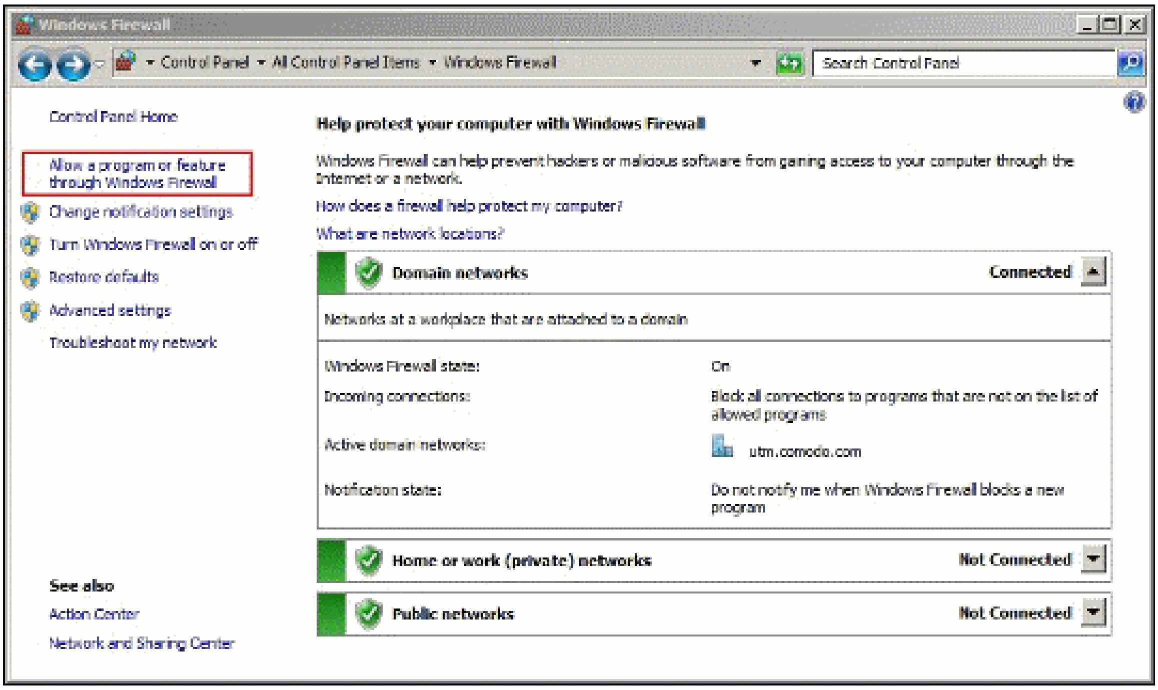
Completed the Korugan Active Directory Agent Setup Wizard

Click the Finish button to exit the Setup Wizard.

Step 2 - Add Socket Exception for the AD Agent in the server

The next step is to configure a socket exception for the agent in Windows Firewall on your server. This will allow the agent to communicate with Dome Firewall.

1. Open the Windows control panel on the server
2. Click the 'Windows Firewall' icon to open the firewall configuration panel. Please note, the following instructions may vary slightly depending on your server version.
3. Click 'Allow a program or feature':


Windows Firewall
Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
How does a firewall help protect my computer?
What are network locations?
Domain networks
Connected
Home or work (private) networks
Not Connected
Public networks
Not Connected

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

Networks at a workplace that are attached to a domain

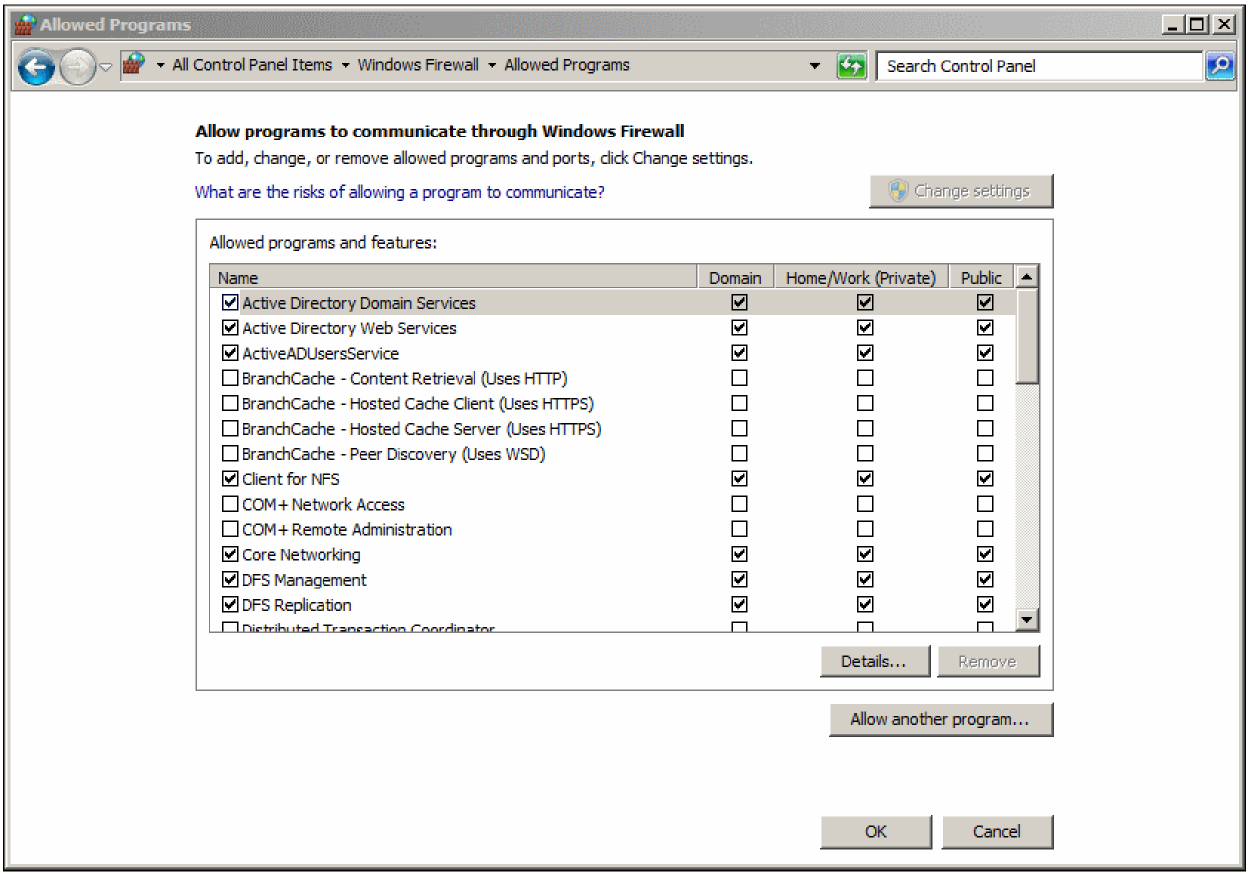
Windows Firewall state: On

Incoming connections: Block all connections to programs that are not on the list of allowed programs

Active domain networks: utm.comodo.com

Notification state: Do not notify me when Windows Firewall blocks a new program

4. On the next screen, click 'Allow another program' to add the agent to the list of exceptions.



Allowed Programs

All Control Panel Items ▸ Windows Firewall ▸ Allowed Programs

Search Control Panel

Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

Change settings

Allowed programs and features:

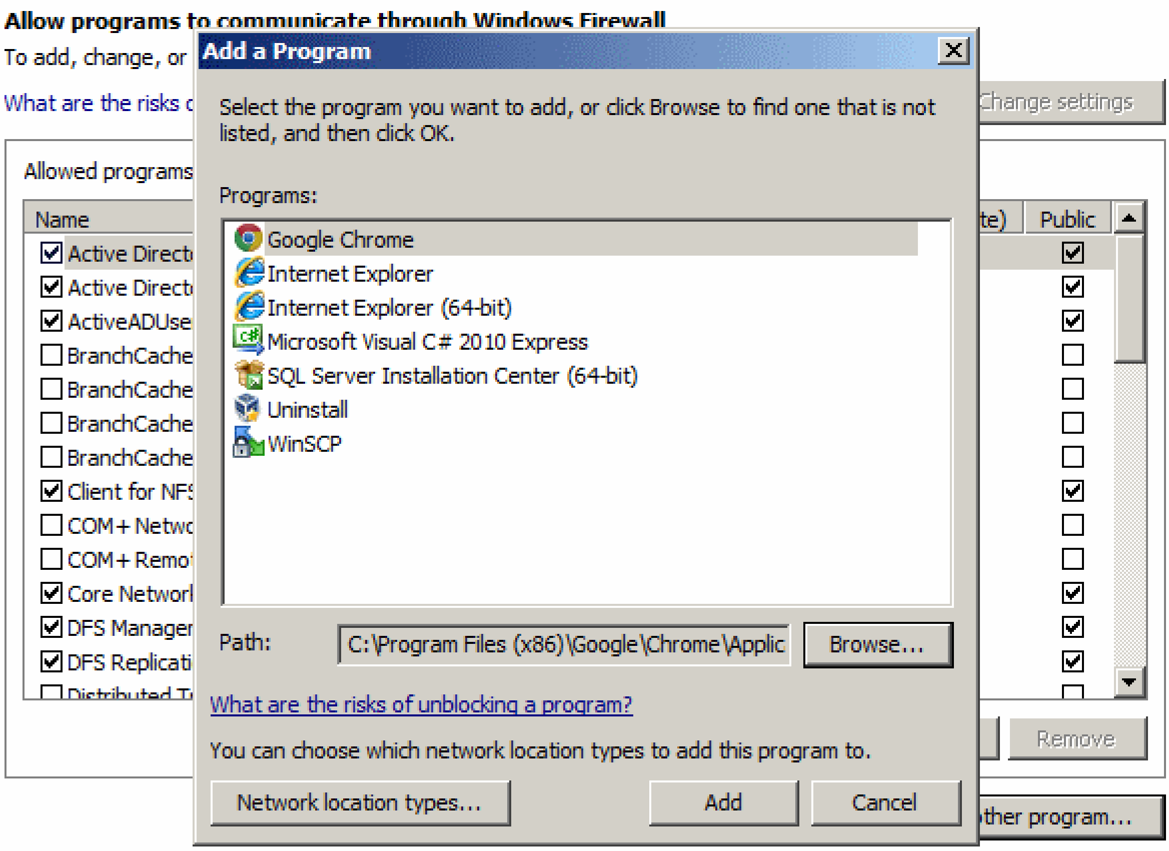
Name	Domain	Home/Work (Private)	Public
☑ Active Directory Domain Services	☑	☑	☑
☑ Active Directory Web Services	☑	☑	☑
☑ ActiveADUsersService	☑	☑	☑
☐ BranchCache - Content Retrieval (Uses HTTP)	☐	☐	☐
☐ BranchCache - Hosted Cache Client (Uses HTTPS)	☐	☐	☐
☐ BranchCache - Hosted Cache Server (Uses HTTPS)	☐	☐	☐
☐ BranchCache - Peer Discovery (Uses WSD)	☐	☐	☐
☑ Client for NFS	☑	☑	☑
☐ COM+ Network Access	☐	☐	☐
☐ COM+ Remote Administration	☐	☐	☐
☑ Core Networking	☑	☑	☑
☑ DFS Management	☑	☑	☑
☑ DFS Replication	☑	☑	☑
☐ Distributed Transaction Coordinator	☐	☐	☐

Details... Remove

Allow another program...

OK Cancel

5. Click 'Browse' in the resulting 'Add a Program' dialog. Navigate to the agent's install folder, select 'ActiveADUsersService.vshost' and click 'Open'.



Allow programs to communicate through Windows Firewall

To add, change, or

What are the risks c

Change settings

Allowed programs

Name	te)	Public
☑ Active Directo		☑
☑ Active Directo		☑
☑ ActiveADUse		☑
☐ BranchCache		☐
☐ BranchCache		☐
☐ BranchCache		☐
☐ BranchCache		☐
☑ Client for NFS		☑
☐ COM+ Netwo		☐
☐ COM+ Remo		☐
☑ Core Networl		☑
☑ DFS Manager		☑
☑ DFS Replicati		☑
☐ Distributed T		☐

Remove

ther program...

Add a Program

Select the program you want to add, or click Browse to find one that is not listed, and then click OK.

Programs:

- Google Chrome
- Internet Explorer
- Internet Explorer (64-bit)
- Microsoft Visual C# 2010 Express
- SQL Server Installation Center (64-bit)
- Uninstall
- WinSCP

Path: C:\Program Files (x86)\Google\Chrome\Applic Browse...

What are the risks of unblocking a program?

You can choose which network location types to add this program to.

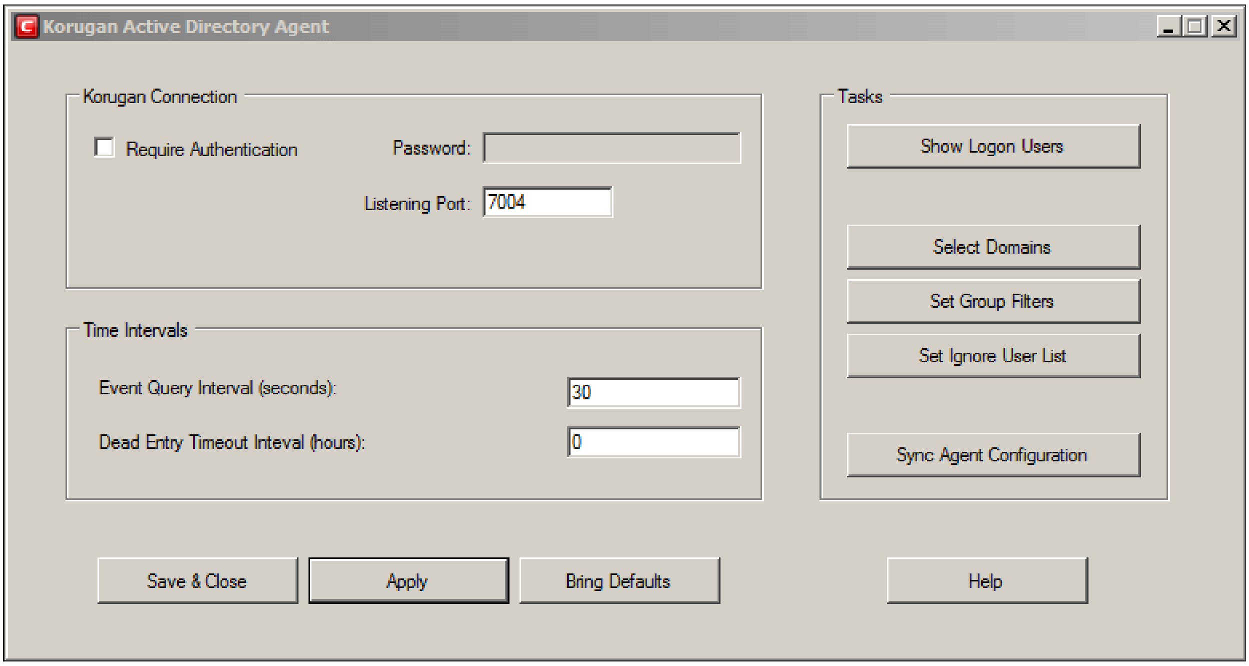
Network location types... Add Cancel

6. Click 'Add' in the 'Add a program' dialog then 'OK' in the 'Allow programs to communicate...' screen.

Step 3 - Configure the AD Agent

Next, the agent needs to be configured to connect to the Dome Firewall virtual appliance.

1. Browse to the agent installation folder (C:\Program Files on 32-bit system or C:\Program Files (x86)) and open 'ActiveADUsersService.exe'.


Korugan Active Directory Agent

Korugan Connection

☐ Require Authentication Password:

Listening Port: 7004

Time Intervals

Event Query Interval (seconds): 30

Dead Entry Timeout Inteval (hours): 0

2. Configure the parameters as shown below:

Connection Parameters

- **Require Authentication** - Enable if you want the agent to supply a password in order to connect to the AD server. Specify the password in the space provided.
- **Listening Port** - By default, the server listens to the virtual appliance through port 7004. If you want to change the port, enter the port number in the text field.

Time Intervals

- **Every Query Interval** - Enter the time interval (in seconds) at which the agent should poll Dome Firewall for updates. It is recommended to set the interval according to the size of the directory. Directories with a large amount of users should be checked more frequently.
- **Dead Entry Interval** - Dome Firewall will delete a username/IP pair if a user does not login for a certain period of time. For example, if the 'Dead Entry Interval' is set as 720 hours then the pair will be deleted if the user does not login for 30 days.

Tasks

- **Show Logon Users** - Displays the currently logged-in users and their IP addresses
- **Select Domains** - By default, the agent tracks login events for all domains which have been added to the AD server. Click the 'Select Domains' button to enable or disable tracking on specific domains.
- **Set Group Filters** - By default, the agent tracks login events for all AD user groups. Click the 'Set Group Filters' button to enable or disable tracking on specific domains.
- **Set Ignore List** - By default, the agent tracks login events for all AD users. Click the 'Set Ignore Users' button to choose which users should not be tracked.
- **Sync Agent Configuration** - Enables you to export the current configuration of the agent.

- Click 'Apply' to save the configuration

- Click 'Save and Close' to close the application window. The agent process will continue to run in the background.

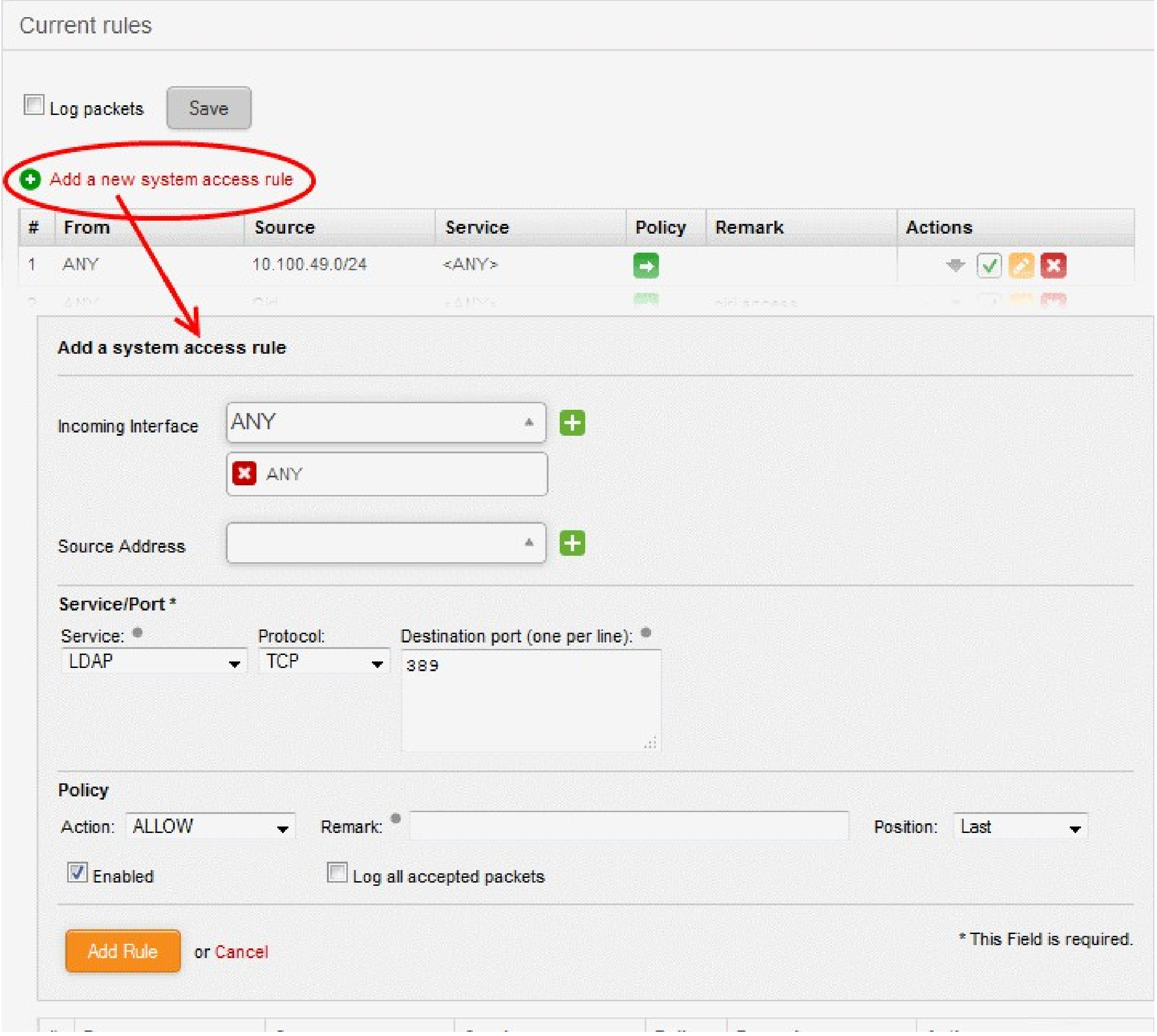
The agent is now configured to connect to the virtual appliance. The next step is to configure Dome firewall to receive the connection.

Step 4 - Configure the firewall to communicate with the agent

- You need to create a rule in 'Firewall' > 'System Access' to allow the agent to access the firewall. See **below** for help with this.
- You also need to add the IP address and port of the AD server so the firewall can receive the username/IP mapping tables. See **Configure the Active Directory Connection** for more details.

Allow Access to the virtual appliance

- Click 'Firewall' > 'System Access' to open the 'System Access' interface
- Click the 'Add a new system access rule' link at top-left:



Current rules

☐ Log packets Save

Add a new system access rule

#	From	Source	Service	Policy	Remark	Actions
1	ANY	10.100.49.0/24	<ANY>			

Add a system access rule

Incoming Interface: ANY
ANY

Source Address:

Service/Port *
Service: LDAP
Protocol: TCP
Destination port (one per line): 389

Policy
Action: ALLOW
Remark:
Position: Last
☑ Enabled
☐ Log all accepted packets

Add Rule or Cancel

* This Field is required.

- Enter the following settings:

Incoming Interface - Select 'Any' from the drop-down

Source Address - You do not need to select any firewall object

Service/Port - Select the LDAP service traffic received at port 389

  - Service - Choose 'LDAP' from the drop-down
  - Protocol - By default TCP will be chosen
  - Destination port - The default port number of 389 will be auto-populated. Enter a new port number if the LDAP port of your server is different.

Policy - Choose 'Allow'.

General Settings

  - Remark (optional) - Enter a short description of the rule. The description will appear in the 'Remark' column of the rules interface.
  - Position - Set the priority of the rule with respect to other rules in the list. Rules in iptables are processed in the order they appear on the list.
  - Enabled - If selected, the rule will be activated immediately after saving.
  - Log all accepted packets - All packets allowed by the rule will be logged. See **Viewing Logs** for more details on configuring storage of logs and viewing the logs.

- Click 'Add Rule'

To add the rule for the agent to access the virtual appliance

- Open the 'System Access' interface by clicking Firewall > System Access from the left hand side navigation
- Click 'Add a new system access rule' link from the top left.
- Enter the parameters for the new rule as shown below:

Incoming Interface - Select 'Any' from the drop-down

Source Address - Need not select any firewall object

Service/Port - Select the TCP traffic received at port 389

  - Service - Choose 'User Defined' from the drop-down
  - Protocol - Choose TCP from the drop-down
  - Destination port - Enter the agent port as configured in the server in **Step 3**. (Default = 7004).

Policy - Choose 'Allow'.

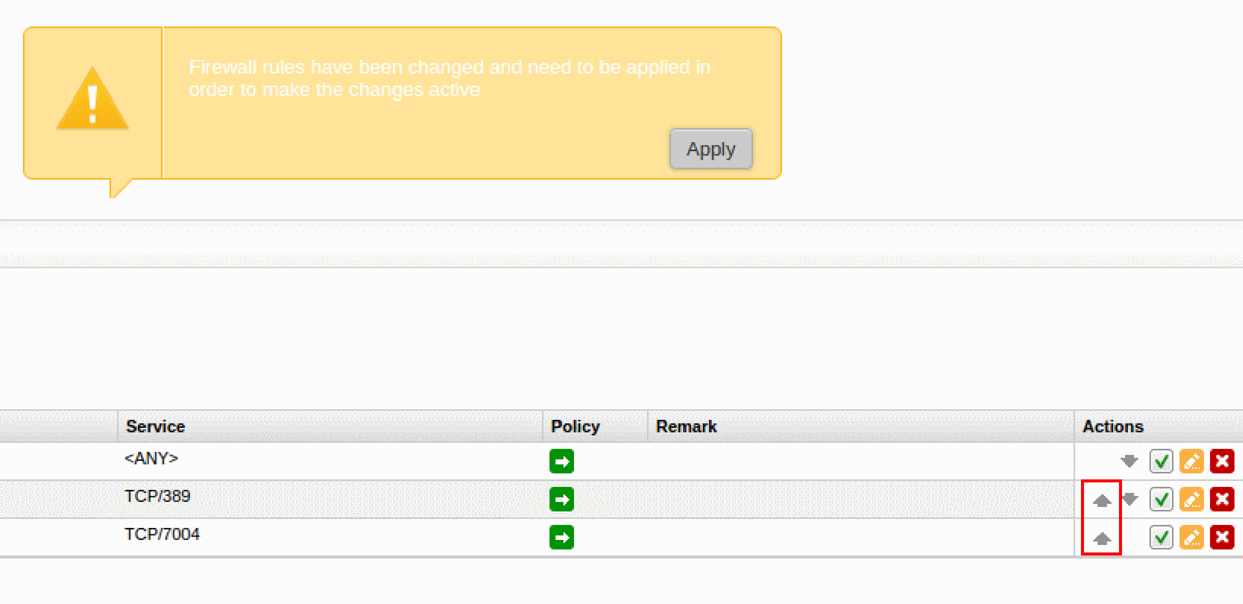
General Settings

  - Remark (optional) - Enter a short description for the rule. The description will appear in the Remark column of the rules interface.
  - Position - Set the priority of the rule with respect to other rules in the list. Rules in iptables are processed in the order they appear on the list.
  - Enabled - If selected, the rule will be activated immediately after saving.
  - Log all accepted packets - All packets allowed by the rule will be logged. See **Viewing Logs** for more details on configuring storage of logs and viewing the logs.

- Click 'Add Rule'.

The rules will be added to the System Access interface.

- Place new two rules to uppermost levels by clicking arrow buttons ▲ / ▼ and Click 'Apply' to apply new order.



Firewall rules have been changed and need to be applied in order to make the changes active

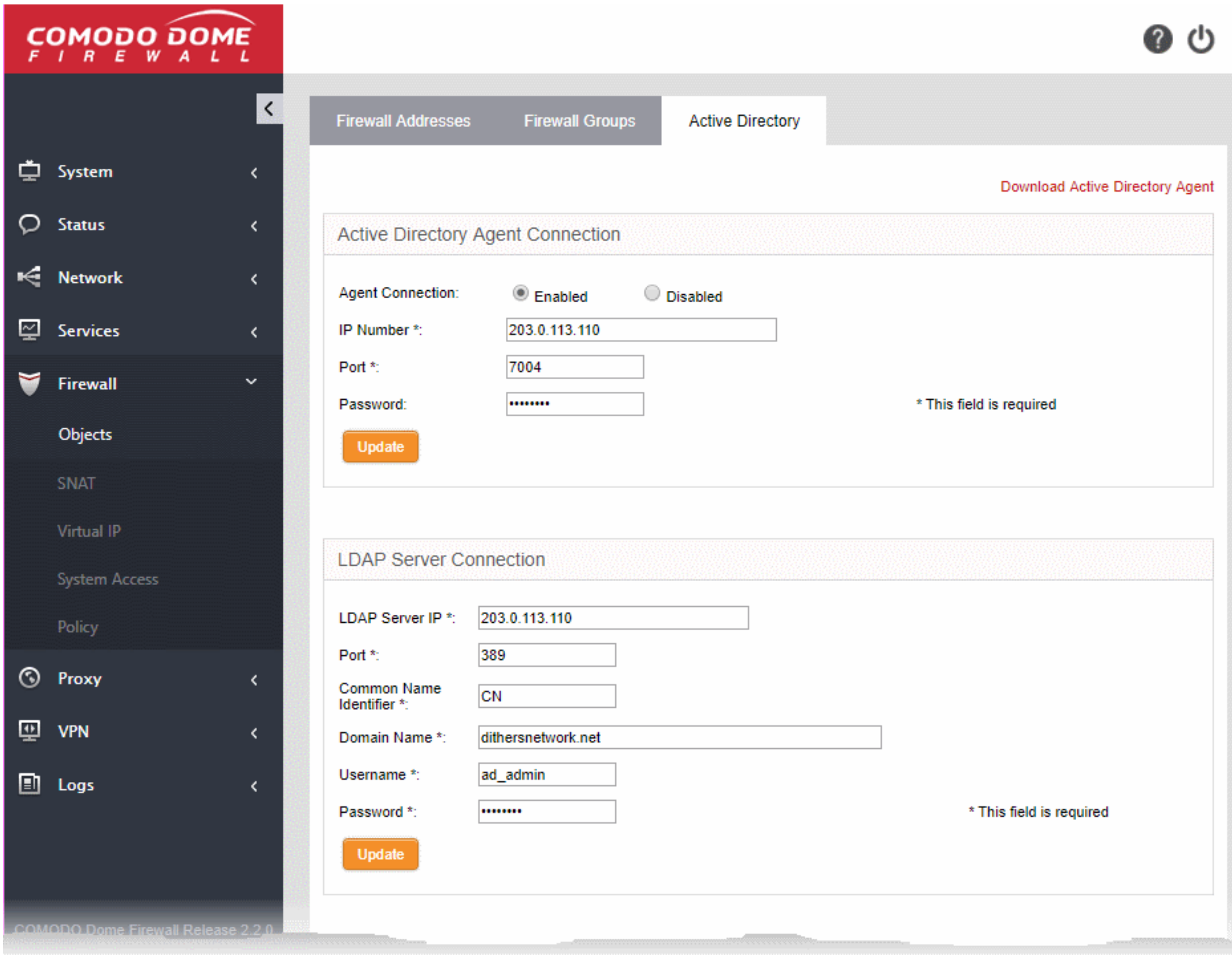
Service	Policy	Remark	Actions
<ANY>	➡		▼ ✓ ✎ ✖
TCP/389	➡		▲ ▼ ✓ ✎ ✖
TCP/7004	➡		▲ ✓ ✎ ✖

Configure the Active Directory Connection

The Active Directory interface in the administrative console allows you to configure the virtual appliance for the connection.

To access the Active Directory interface

- Click 'Firewall' > 'Objects' from the left hand side pane
- Click the 'Active Directory' tab



Active Directory Agent Connection

Agent Connection:	● Enabled ○ Disabled
IP Number *:	203.0.113.110
Port *:	7004
Password:	••••••••

* This field is required

Update

LDAP Server Connection

LDAP Server IP *:	203.0.113.110
Port *:	389
Common Name Identifier *:	CN
Domain Name *:	dithersnetwork.net
Username *:	ad_admin
Password *:	••••••••

* This field is required

Update

- Enter the parameters for the agent and the AD server as shown below:

Active Directory Agent Connection

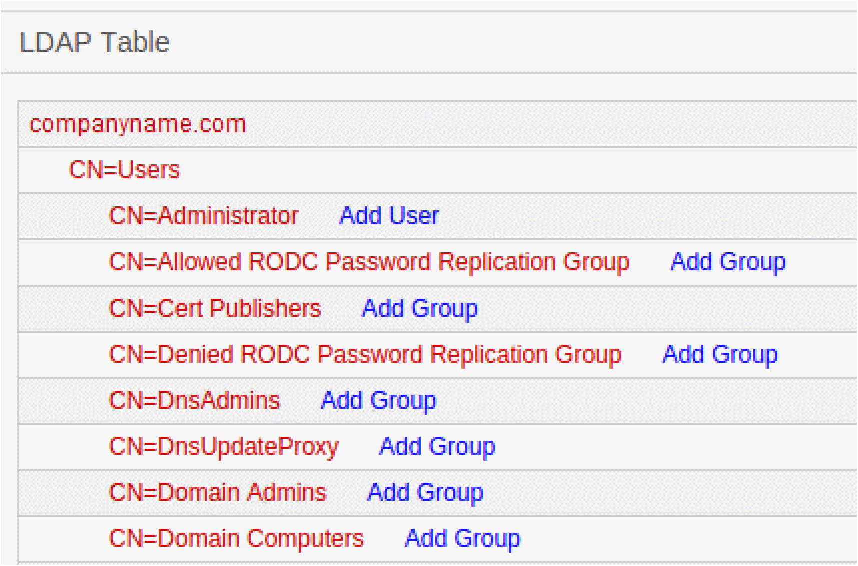
  - Agent Connection - Choose 'Enabled' to enable the connection from the agent
  - IP Number - Enter the IP address of the server on which the agent is installed
  - Port - Enter the agent connection port as configured in the server in **Step 3**. (Default = 7004).
  - Password - Enter the password if it is set on agent in **Step 3**
- Click 'Update' to save and activate the agent connection.

LDAP Server Connection

  - LDAP Server IP - Enter the IP address of the AD server. The IP address is generally same with the agent's address.
  - Port - Enter the LDAP service port of the server. By default, the LDAP port is 389. If you have configured a different port, enter the new port number.
  - Common Name Identifier - Enter the Common Name Identifier of Active Directory. (Default = CN).
  - Domain Name - Enter the Domain Name to select which domain is going to monitored on LDAP Table displayed at the bottom of the page.
  - Username and Password - Enter the Username and Password of a user account that has the 'Read' access the AD server. 'Write' access is not required.
- Click 'Update' to save and activate the AD server connection.

The selected domain(s) will be displayed in the 'LDAP Table' at the bottom of the interface.

- Click the Domain name to expand the tree structure of the active directory.



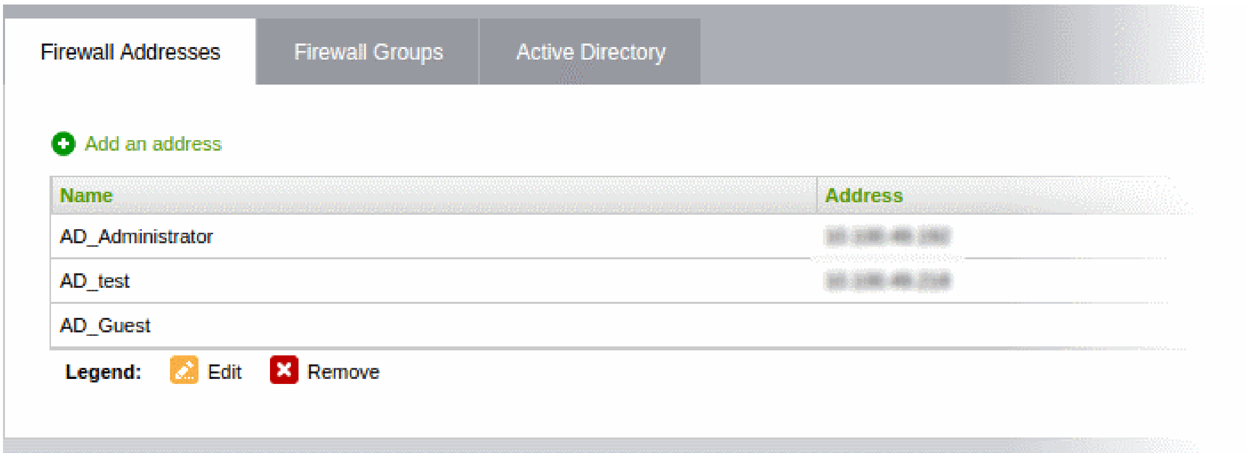
LDAP Table

companyname.com
CN=Users
CN=Administrator Add User
CN=Allowed RODC Password Replication Group Add Group
CN=Cert Publishers Add Group
CN=Denied RODC Password Replication Group Add Group
CN=DnsAdmins Add Group
CN=DnsUpdateProxy Add Group
CN=Domain Admins Add Group
CN=Domain Computers Add Group

You can add the users to firewall objects and user groups to firewall object groups from the tree LDAP table.

Add User to Firewall Objects

- Click the Domain name to expand the tree structure of the active directory.
- Locate the user by expanding the parents.
- Click 'Add User' to add the user to Firewall Objects.

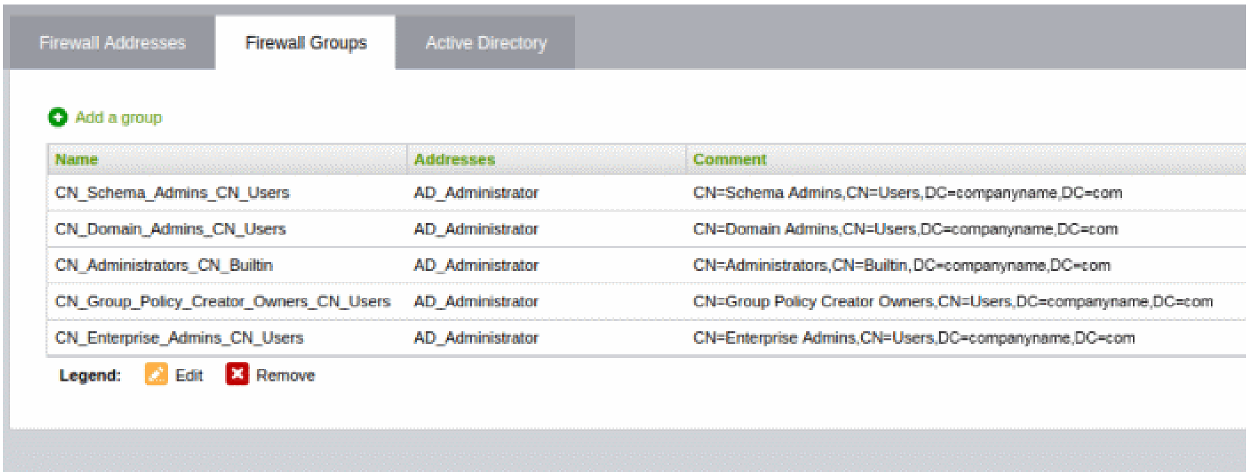


Name	Address
AD_Administrator	[redacted]
AD_test	[redacted]
AD_Guest	

Legend: Edit Remove

Add User Groups to Firewall Objects

- Click the Domain name to expand the tree structure of the active directory.
- Locate the user group by expanding the parents.
- Click 'Add Group' to add the user group to Firewall Object Groups.



Name	Addresses	Comment
CN_Schema_Admins_CN_Users	AD_Administrator	CN=Schema Admins,CN=Users,DC=companyname,DC=com
CN_Domain_Admins_CN_Users	AD_Administrator	CN=Domain Admins,CN=Users,DC=companyname,DC=com
CN_Administrators_CN_Builtin	AD_Administrator	CN=Administrators,CN=Builtin,DC=companyname,DC=com
CN_Group_Policy_Creator_Owners_CN_Users	AD_Administrator	CN=Group Policy Creator Owners,CN=Users,DC=companyname,DC=com
CN_Enterprise_Admins_CN_Users	AD_Administrator	CN=Enterprise Admins,CN=Users,DC=companyname,DC=com

Legend: Edit Remove

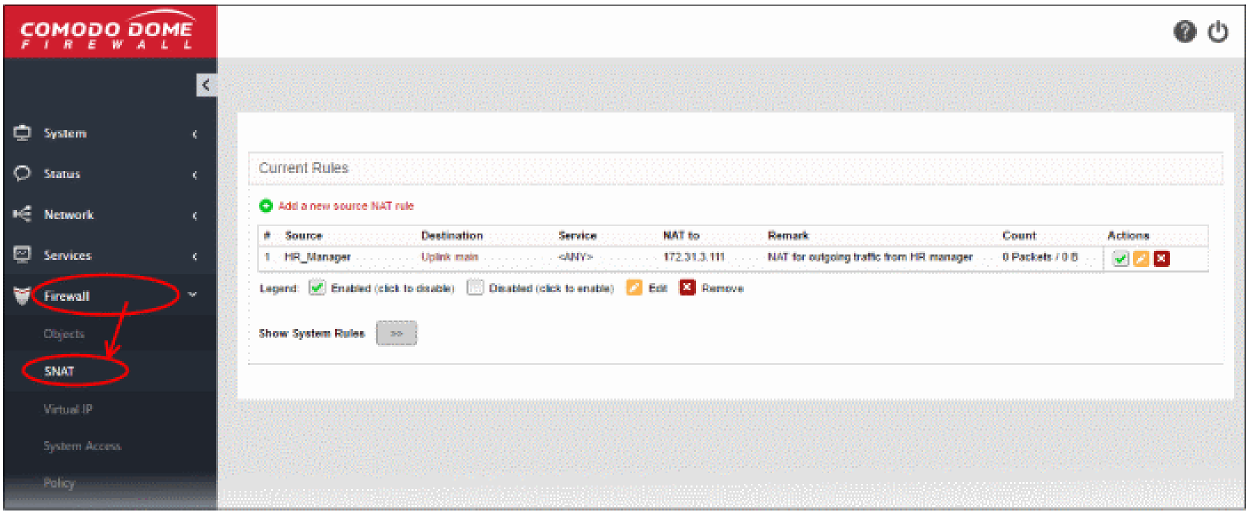
8.2 Source Network Address Translation

- By default, Dome Firewall provides the IP address of the primary uplink device as the source address of all outbound traffic.
- If outgoing traffic from an internal host must contain the host's IP address, then administrators should configure a Source NAT (SNAT) rule. This is useful If a host is running a web or mail service and the outgoing packets should contain the external IP address of the server.

Tip: Dome Firewall also allows you to create Destination NAT (DNAT) rules for incoming traffic. DNAT rules redirect service-specific traffic from a port on a host or interface to another host/port combination. See **Configuring Virtual IP for Destination Network Address Translation** for more details.

SNAT rules can be created and managed from the 'SNAT' interface.

- To open the SNAT interface, click 'Firewall' > 'SNAT' on the left-hand menu



Current Rules

Add a new source NAT rule

#	Source	Destination	Service	NAT to	Remark	Count	Actions
1	HR_Manager	Uplink main	<ANY>	172.31.3.111	NAT for outgoing traffic from HR manager	0 Packets / 0 B	☑ ✎ ☒

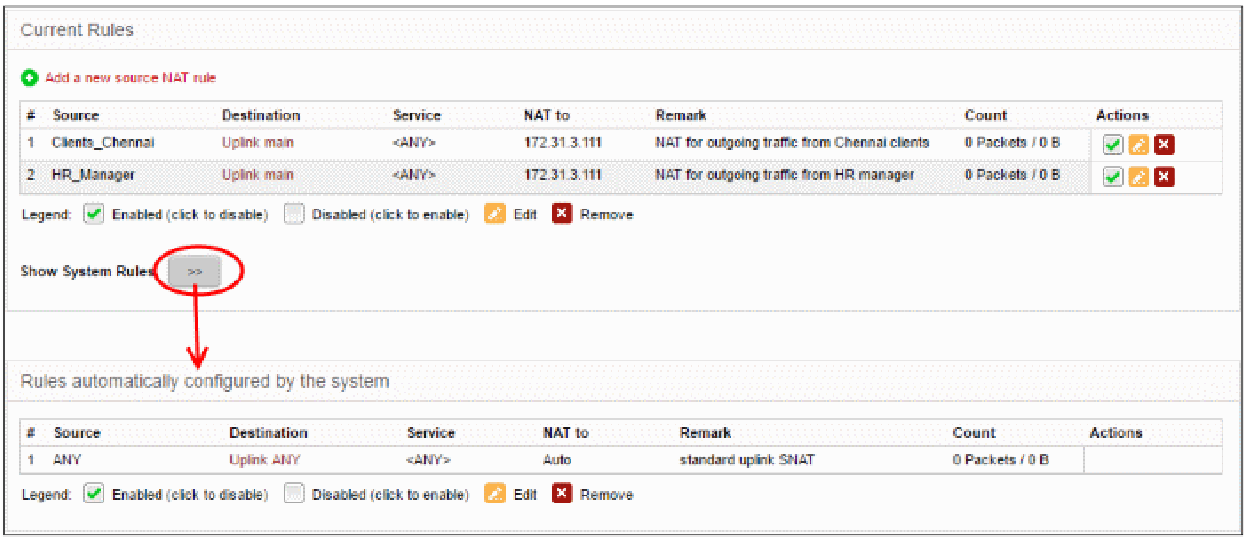
Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Show System Rules >>

The interface displays all current SNAT rules in effect and allows you to create new rules.

SNAT Table - Column Descriptions	
Column	**Description**
#	ID number of the rule. Translation is applied based on the first matching rule in the list, regardless of other matching rules that follow.
Source	The Firewall Object containing the IP address, IP address range or subnet of the host(s) from which the traffic originates
Destination	The interface device through which the traffic is directed to external network
Service	The service that uses the traffic, indicated as the protocol and the port used
NAT to	The IP address of the host, to be contained in the headers of the outgoing packets
Remark	A short description of the rule
Count	Indicates the number of packets and size of data intercepted by the rule.
Actions	Displays control buttons for managing the rule. ☑ - Enable or disable the rule. ✎ - Edit rule parameters. The 'Edit' interface is similar to the 'Add Rule' interface. See '**Creating an SNAT rule**' for more details. ☒ - Removes the rule.

- Clicking the right arrow button beside 'Show system rules' displays a list of SNAT rules auto generated by the DFW virtual appliance. These rules cannot be modified or removed.



Current Rules

Add a new source NAT rule

#	Source	Destination	Service	NAT to	Remark	Count	Actions
1	Clients_Chennai	Uplink main	<ANY>	172.31.3.111	NAT for outgoing traffic from Chennai clients	0 Packets / 0 B	☑ ✎ ☒
2	HR_Manager	Uplink main	<ANY>	172.31.3.111	NAT for outgoing traffic from HR manager	0 Packets / 0 B	☑ ✎ ☒

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Show System Rules >>

Rules automatically configured by the system

#	Source	Destination	Service	NAT to	Remark	Count	Actions
1	ANY	Uplink ANY	<ANY>	Auto	standard uplink SNAT	0 Packets / 0 B	

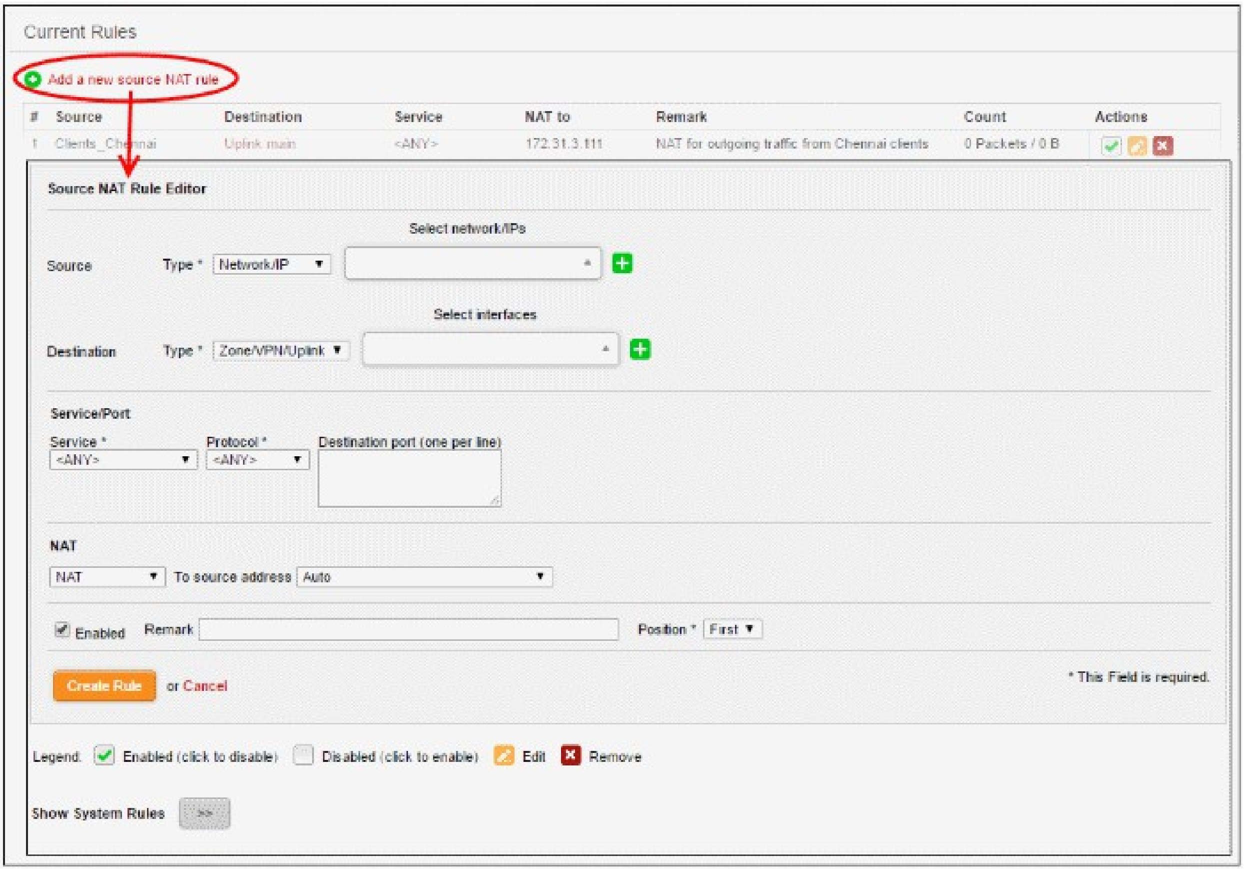
Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Creating an SNAT rule

The source rule can be created by defining the source of the outgoing traffic, destination, service and the IP address to be masqueraded.

To create a new SNAT rule

- Click 'Firewall' > 'SNAT' on the left menu
- Click 'Add a new Source NAT Rule'



Current Rules

Add a new source NAT rule

#	Source	Destination	Service	NAT to	Remark	Count	Actions
1	Clients_Chennai	Uplink main	<ANY>	172.31.3.111	NAT for outgoing traffic from Chennai clients	0 Packets / 0 B	☑ ✎ ☒

Source NAT Rule Editor

Source Type * Network/IP ▾ Select network/IPs +

Destination Type * Zone/VPN/Uplink ▾ Select interfaces +

Service/Port

Service * <ANY> ▾ Protocol * <ANY> ▾ Destination port (one per line)

NAT

NAT ▾ To source address Auto ▾

☑ Enabled Remark Position * First ▾

Create Rule or Cancel

* This Field is required.

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Show System Rules >>

- Enter the parameters for the new rule as shown below:

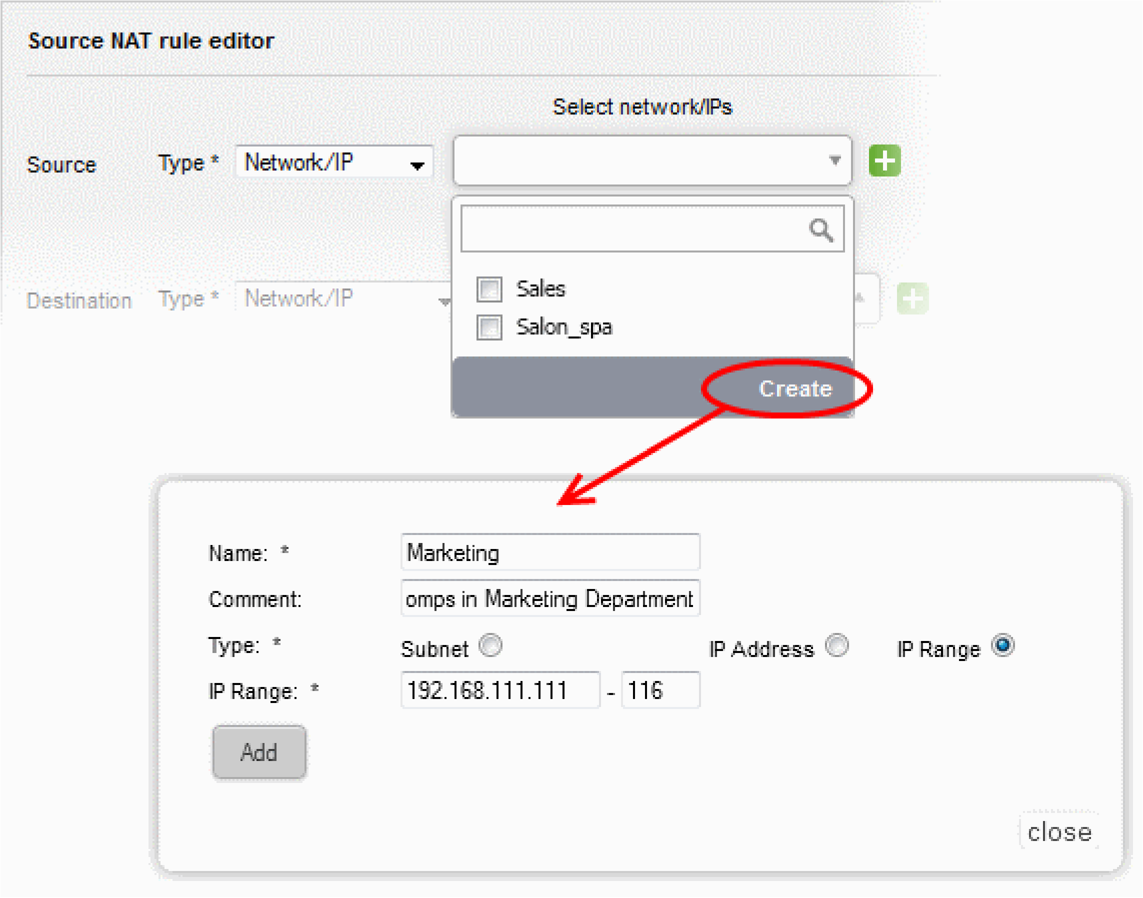
Source - Specify whether the origin of the traffic to be intercepted by this rule, is a Network address/IP address or the SSL VPN user by choosing the option from the 'Type' drop-down.

1. Network address/IP address - Choose the Firewall Object containing the IP address, IP Address Range or the subnet of the host(s) from the 'Select network/IPs' drop-down.

   If a firewall object covering the IP address/IP Address range or the subnet to be specified has not been created under the Firewall Objects interface previously, you an create a new object from this interface too.

   To create a new firewall object

   - Click the drop-down arrow and click 'Create' at the bottom of the list. A new pane for creating a new object will appear.



Source NAT rule editor

Source Type * Network/IP

Select network/IPs

□ Sales

□ Salon_spa

Destination Type * Network/IP

Name: * Marketing

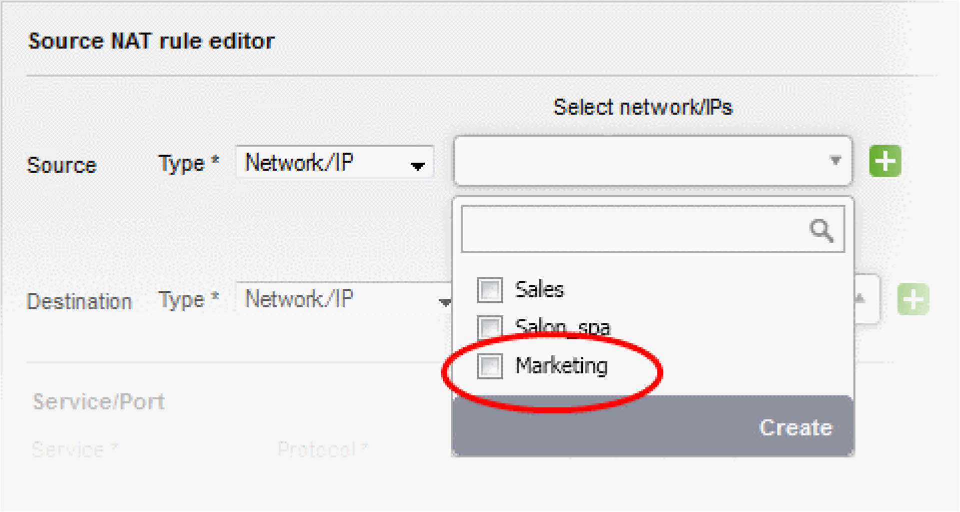
Comment: omps in Marketing Department

Type: * Subnet ○ IP Address ○ IP Range ●

IP Range: * 192.168.111.111 - 116

   - **Name** - Specify a name for the object (15 characters max) representing the host(s) included in the object.
   - **Comment** - Enter a short description of the object.
   - **Type** - Select the type by which the hosts are to be referred in the object. The available options are:
     - Subnet - Select this if a sub network of computers is to be covered by the object and enter the sub network address
     - IP address - Select this if a single host is to be covered by the object and enter the IP address of the host
     - IP range - Select this if more than one host is to be covered by the object and enter the IP address range of the hosts
   - Click 'Add'.

   The new object will be added and will be available for selection from the Select network/IPs drop-down.



The new object will also be added to the list of objects under Firewall Objects and will be available for selection for creating other firewall rules too.

2. SSLVPN User - Choose the SSL VPN user from the 'Select SSLVPN users' drop-down.

Destination - Specify the whether the destination of the traffic is network zone/uplink device/VPN, network address/IP address or the SSL VPN user.

1. Zone/VPN/Uplink - Choose the interface device, the VPN or the physical port to which the interface is connected, from the 'Select interfaces' drop-down.
2. Network address/IP address - Choose the Firewall Object containing the IP address, IP Address Range or the subnet of the host(s) from the 'Select network/IPs' drop-down.

   If a firewall object covering the IP address/IP Address range or the subnet to be specified has not been created under the Firewall Objects interface previously, you an create a new object from this interface too. Refer to the **explanation above** for more details.
3. SSLVPN User - Choose the SSL VPN user from the 'Select SSLVPN users' drop-down.

Service/Protocol/Port - Select the type or the service hosted by the source, the protocol and the port used by the service.

- Service - Choose the type of service from the drop-down
- Protocol - Choose the protocol used by the service
- Destination port - Specify the destination port(s) of the service one by one, in the 'Destination Port' text box.

Tip: The virtual appliance is loaded with predefined combinations of service/protocol/port, like HTTP/TCP/80, <ALL>/TCP+UDP/0:65535, or <ANY>, which is a shortcut for all services, protocols, and ports. If you want to specify custom protocol/port combination, then select 'User Defined' from the service. You can also specify additional destination ports for standard combinations, for the services that run on ports different from the standard ones.

NAT - The NAT option allows you to choose whether or not to apply the NAT. On applying NAT, the IP address/Port contained in the headers of the data packets will be changed to the IP address selected from the drop-down at the right. Choose the NAT option from the drop-down at the left. The options available are:

1. NAT - The NAT will be applied. Choose the source IP address to be contained in the headers of the data packets from the drop-down at the right.

   The drop-down at the right displays the network zones, network interface devices and the IP addresses from which the outgoing traffic is allowed.

   - Ensure that the outgoing traffic is allowed from the host. Open the Policy Firewall interface by clicking Firewall > Firewall. Add a rule to allow outgoing traffic from the host. See **Configuring Firewall Policy Rules** for more details.

- If you want a static IP address assigned to the server to be shown in the outgoing traffic, then add the IP address as an additional address for the uplink device through which the traffic will be routed to external network.
  - Open Uplink Editor interface by clicking Network > Interfaces > Uplink Editor tab
  - Click the Edit icon in the row of the uplink device
  - Ensure that the 'Add additional addresses' checkbox is selected, enter the IP address/netmask into the textbox and click 'Update Uplink'.
- Selecting 'Auto' or 'Zone <network zone> - IP: Auto' chooses the IP address of the respective outgoing interface

2. No NAT - The Network Address Translation will not be applied
3. Map Network - All IPs from the source subnet will be statically mapped to another network of the same size. Specify the subnet to which the IPs are to be mapped in the textbox at the right.

General Settings - Configure the General Settings to enable/disable, enter a short description and select a position for the rule in the list.

- Enabled - Leave this checkbox selected if you want the rule to be activated upon creation.
- Remark - Enter a short description for the rule. The description will appear in the Remark column of the respective Rules interface
- Position - Set the priority for the rule in the list of rules in the respective rules interface. The rules in the iptables are processed in the order they appear on the list.

- Click 'Create Rule'. A confirmation dialog will appear.
- Click 'Apply'. The firewall will be restarted with the new rule applied.

SNAT rule management activities are logged - including date, time, type of event, subject id, component name and event outcome.

8.3 Configure Virtual IP for Destination Network Address Translation

Comodo Dome Firewall allows you to redirect service specific traffic from a port on a host or interface to another host/port combination. Virtual IP rules can be used to limit access from untrusted external networks to the hosts in the network infrastructure.

Examples:

1. Virtual IP rules can be used to publish services on a private host through a public IP address. For example, If a service is hosted on a server within the LAN network zone connected to the DFW virtual appliance, it can be made accessible at the IP address/port combination of an uplink device connected to the virtual appliance.

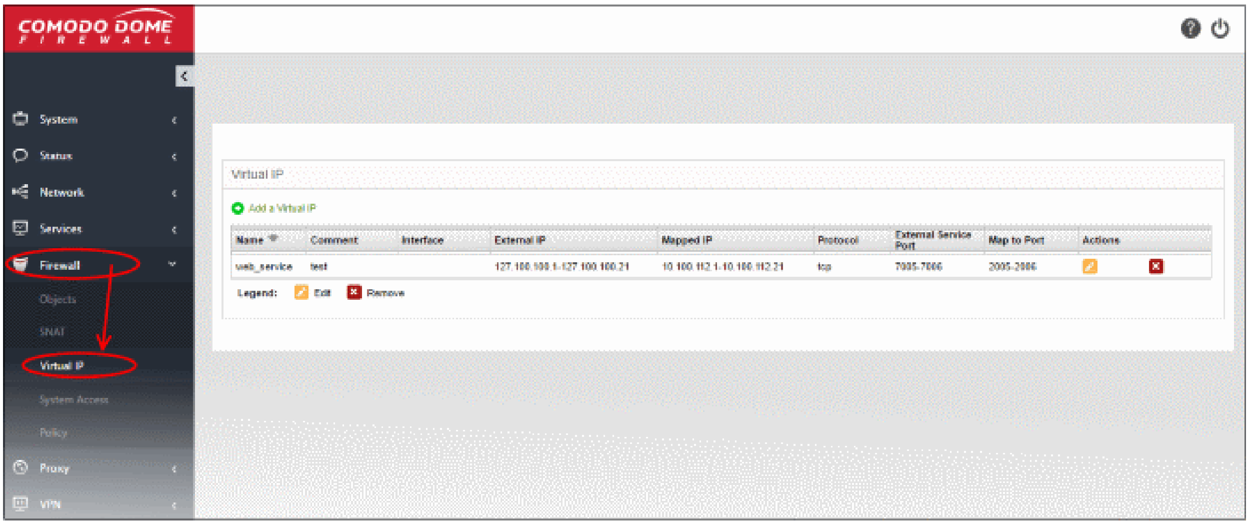
2. DFW blocks SSH connection requests from untrusted external IP addresses to any host within the DMZ zone by default. If required, rules can be created to allow SSH access to specific host in the DMZ.

Virtual IP rules can also be created for:

- **Load distribution** - Distribute traffic directed to a single host to a range of IP addresses to avoid bottlenecks and overloading a single IP.
- **Network Mapping** - Translate the incoming traffic to a different sub-network. The network translation statically maps the addresses of a whole network onto addresses of another network.

Virtual IP rules can be created and managed from the 'Virtual IP' interface.

- To open the interface, click 'Firewall' > 'Virtual IP' on the left



Virtual IP

Add a Virtual IP

Name	Comment	Interface	External IP	Mapped IP	Protocol	External Service Port	Map to Port	Actions
web_service	test		127.100.100.1-127.100.100.21	10.100.112.1-10.100.112.21	tcp	7005-7006	2005-2006	✎ ☒

Legend: ✎ Edit ☒ Remove

The 'Virtual IP' interface displays a list of the Virtual IP rules and allows the administrator to create new rules.

DNAT Table - Column Descriptions	
Column	**Description**
Name	Name to identify the rule
Comment	A short description of the rule
Interface	The interface through which the traffic is received
External IP	The external IP address or IP address range the host(s) to which the traffic pertaining to a service is directed.
Mapped IP	The IP address or IP address range of the destination host/device to which the traffic is to be redirected
Protocol	The protocol used by the service
External Service Port	The port or port range in the host(s)/device(s) to which the traffic is directed.
Map to Port	The port or port range in the destination host/device to which the traffic is to be redirected
Actions	Displays control buttons for managing the rule. ✎ - Opens the 'Edit' interface and enables to edit the parameters of the rule. The Edit interface is similar to Add Rule interface. Refer to the section **Creating a Virtual IP rule** for more details. ☒ - Removes the rule.

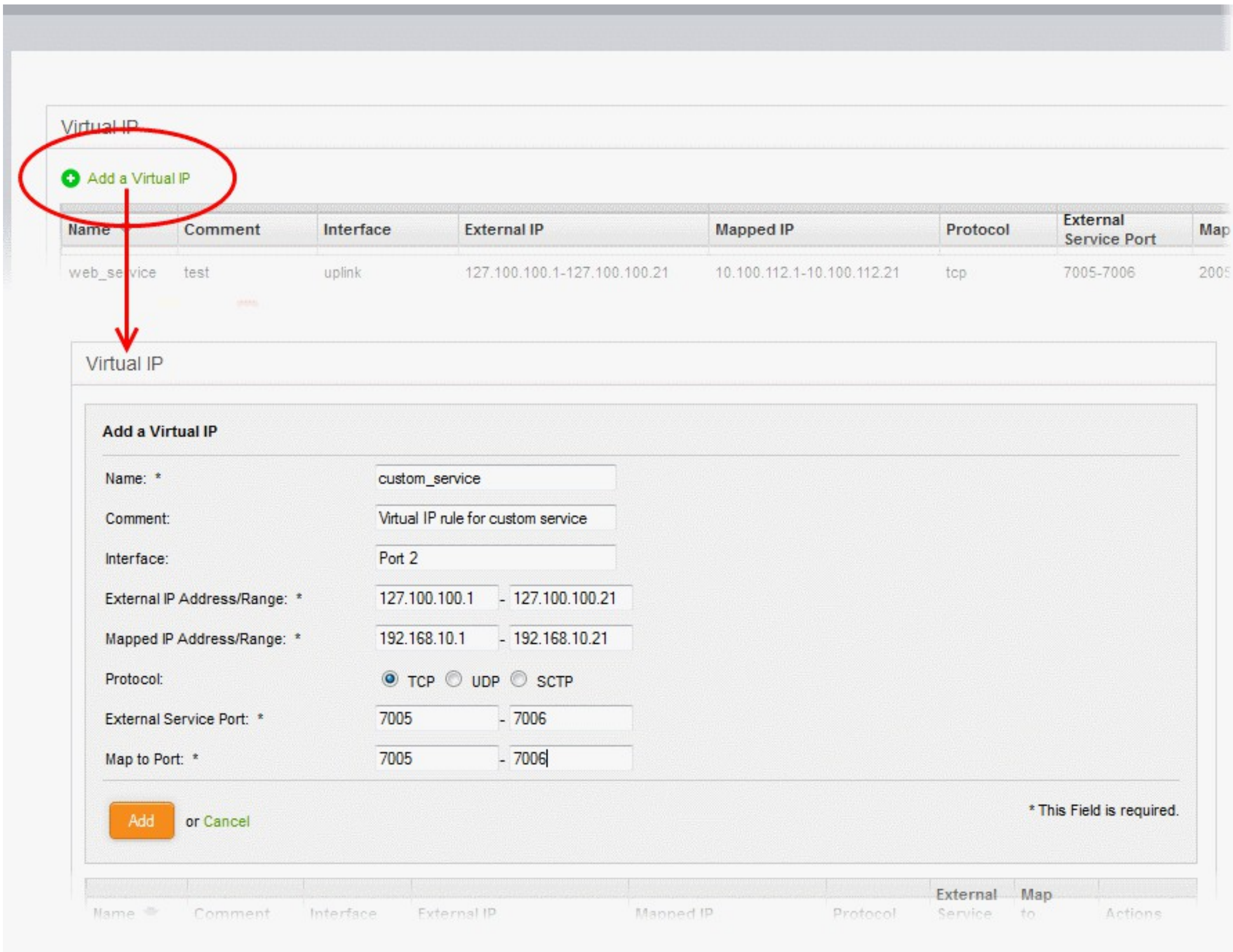
Creating a Virtual IP rule

Virtual IP rules can be created from the 'Add a Virtual IP' pane.

To create a DNAT rule

- Open the 'Virtual IP' interface by clicking the 'Firewall' > 'Virtual IP' from the left hand side navigation.
- Click the 'Add a Virtual IP' link at the top left

The 'Add a Virtual IP' pane will open.



Name	Comment	Interface	External IP	Mapped IP	Protocol	External Service Port	Map
web_service	test	uplink	127.100.100.1-127.100.100.21	10.100.112.1-10.100.112.21	tcp	7005-7006	2005

Virtual IP

Add a Virtual IP

Name: *	custom_service
Comment:	Virtual IP rule for custom service
Interface:	Port 2
External IP Address/Range: *	127.100.100.1 - 127.100.100.21
Mapped IP Address/Range: *	192.168.10.1 - 192.168.10.21
Protocol:	● TCP ○ UDP ○ SCTP
External Service Port: *	7005 - 7006
Map to Port: *	7005 - 7006

- Enter the parameters for the new rule as shown below:

Name - Enter a name to identify the rule.

Comment - Enter a short description of the rule'.

Interface - Specify the interface through which the traffic is forwarded.

External IP Address/Range - Specify the External IP address(es) to which the connection request is received. You can enter a single IP address or a range.

- If the traffic is directed to a single IP address, enter the address in both the fields.
- If the traffic is directed to a range of IP addresses, enter the start and end addresses in the respective fields.

Mapped IP Address/Range - Specify the IP address(es) of the destination to which the traffic has to be redirected. You can enter a single IP address or a range.

- If the traffic is to be redirected to a single IP address, enter the address in both the fields.
- If the traffic is to be redirected to a range of IP addresses, enter the start and end addresses in the respective fields.

Protocol - Choose the protocol used by the service

External Service Port - Specify the port/port range to which the traffic is directed.

- If the traffic is directed to a single port, enter the port number in both the fields.
- If the traffic is directed to a port range, enter the start and end port numbers in the respective fields.

Map to Port - Specify the port/port range to which the traffic is to be redirected.

- If the traffic is to be redirected to a single port, enter the port number in both the fields.
- If the traffic is to be redirected to a port range, enter the start and end port numbers in the respective fields.

- Click 'Add' to save the rule. The rule will take effect immediately.

Virtual IP rule management activities are logged. Items logged include date, time, type of event, subject id, component name and event outcome.

8.4 Configure System Access

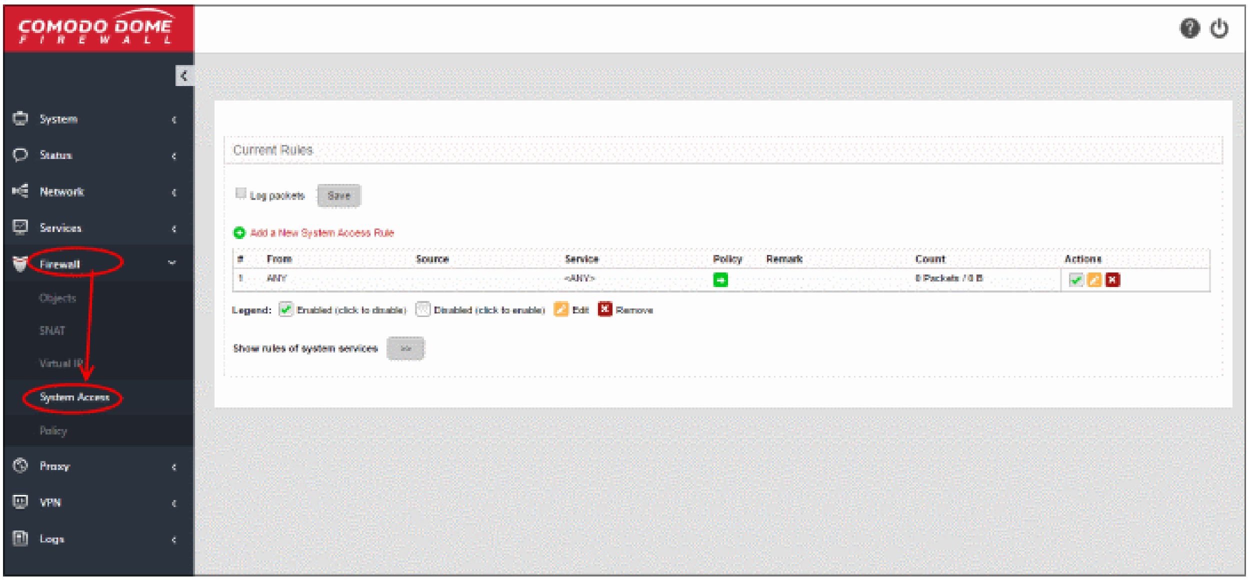
The system access firewall rules manage the access to the Comodo Dome Firewall DFW virtual appliance from the hosts in various internal network zones and external networks.

Comodo Dome Firewall is pre-configured with firewall rules that allow the hosts in different network zones to access the DFW virtual appliance for selected services like: DNS (through port 53); administrative interface (through port 10443); and DHCP service (through port 67) hosted by it. These rules are required for the hosts and clients to receive the essential services and for correct functioning of the virtual appliance. Whenever a new service is enabled in the virtual appliance, rules are auto-created to provide the service to hosts in the required network zones. The administrator can view the rules but can edit or remove the rules. See **Show rules of system services** for more details on how to view the rules.

The administrator can create and manage new rules to provide/block access to the virtual appliance from the internal hosts for specific services and to allow/block access from external networks or specific external IP addresses.

The system access firewall rules can be viewed and managed from the 'System access' interface.

To open the 'System Access' interface, click 'Firewall' > 'System Access' from the left hand side navigation.



Current Rules

□ Log packets Save

Add a New System Access Rule

#	From	Source	Service	Policy	Remark	Count	Actions
1	ANY		<ANY>	➡		0 Packets / 0 B	✓ ✎ ☒

Legend: ✓ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

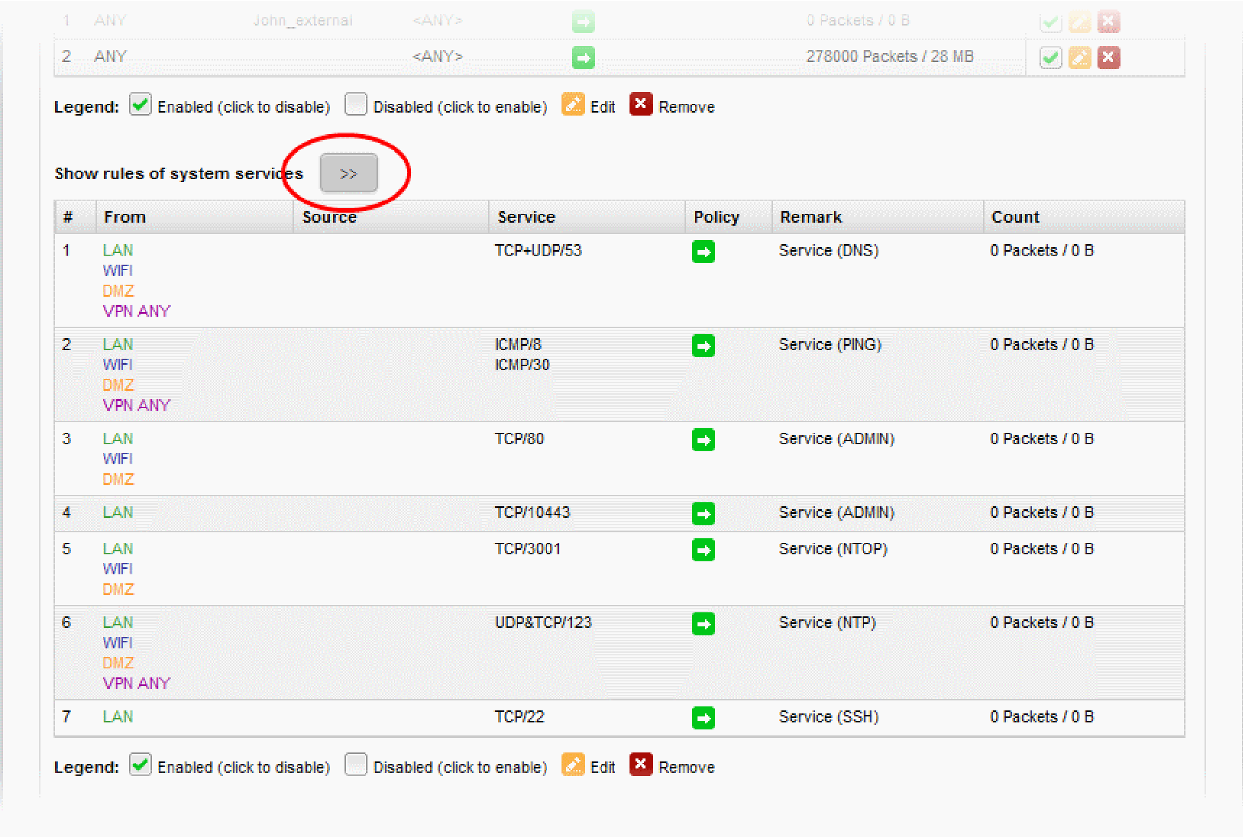
Show rules of system services >>

The interface displays a list of system access firewall rules and enables the administrator to create new rules.

System Access Firewall Rules Table - Column Descriptions	
Column	**Description**
#	ID number of the rule. A packet is allowed or denied based on the first matching rule in the list, regardless of other matching rules that follow, hence the order of the rules play an important role in packet filtering.
From	The interface of the DFW device at which the traffic is received.
Source	The firewall object/object group containing the IP addresses or subnet address of the

	internal or external host(s) from which the traffic originates.
Service	The service that uses the traffic, indicated as the protocol and the port used
Policy	Indicates the allow/block policy of the rule
Remark	A short description of the rule
Count	Indicates the number of packets and size of data intercepted by the rule.
Actions	Displays control buttons for managing the rule. ☑ - The checkbox allows the administrator to switch the rule between enabled and disabled states. ✎ - Opens the 'Edit' interface and enables to edit the parameters of the rule. The Edit interface is similar to Add Rule interface. Refer to the section **Creating System Access Firewall rules** for more details. ☒ - Removes the rule.

- Clicking the right arrow button beside 'Show rules of system services' displays the list of pre-configured/auto-created firewall rules for system access. These rules cannot be modified or removed.



1	ANY	John_external	<ANY>	➡	0 Packets / 0 B	☑ ✎ ☒
2	ANY		<ANY>	➡	278000 Packets / 28 MB	☑ ✎ ☒

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Show rules of system services >>

#	From	Source	Service	Policy	Remark	Count
1	LAN WIFI DMZ VPN ANY		TCP+UDP/53	➡	Service (DNS)	0 Packets / 0 B
2	LAN WIFI DMZ VPN ANY		ICMP/8 ICMP/30	➡	Service (PING)	0 Packets / 0 B
3	LAN WIFI DMZ		TCP/80	➡	Service (ADMIN)	0 Packets / 0 B
4	LAN		TCP/10443	➡	Service (ADMIN)	0 Packets / 0 B
5	LAN WIFI DMZ		TCP/3001	➡	Service (NTOP)	0 Packets / 0 B
6	LAN WIFI DMZ VPN ANY		UDP&TCP/123	➡	Service (NTP)	0 Packets / 0 B
7	LAN		TCP/22	➡	Service (SSH)	0 Packets / 0 B

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

From this interface, the administrator can:

- **Create new system access firewall rules**

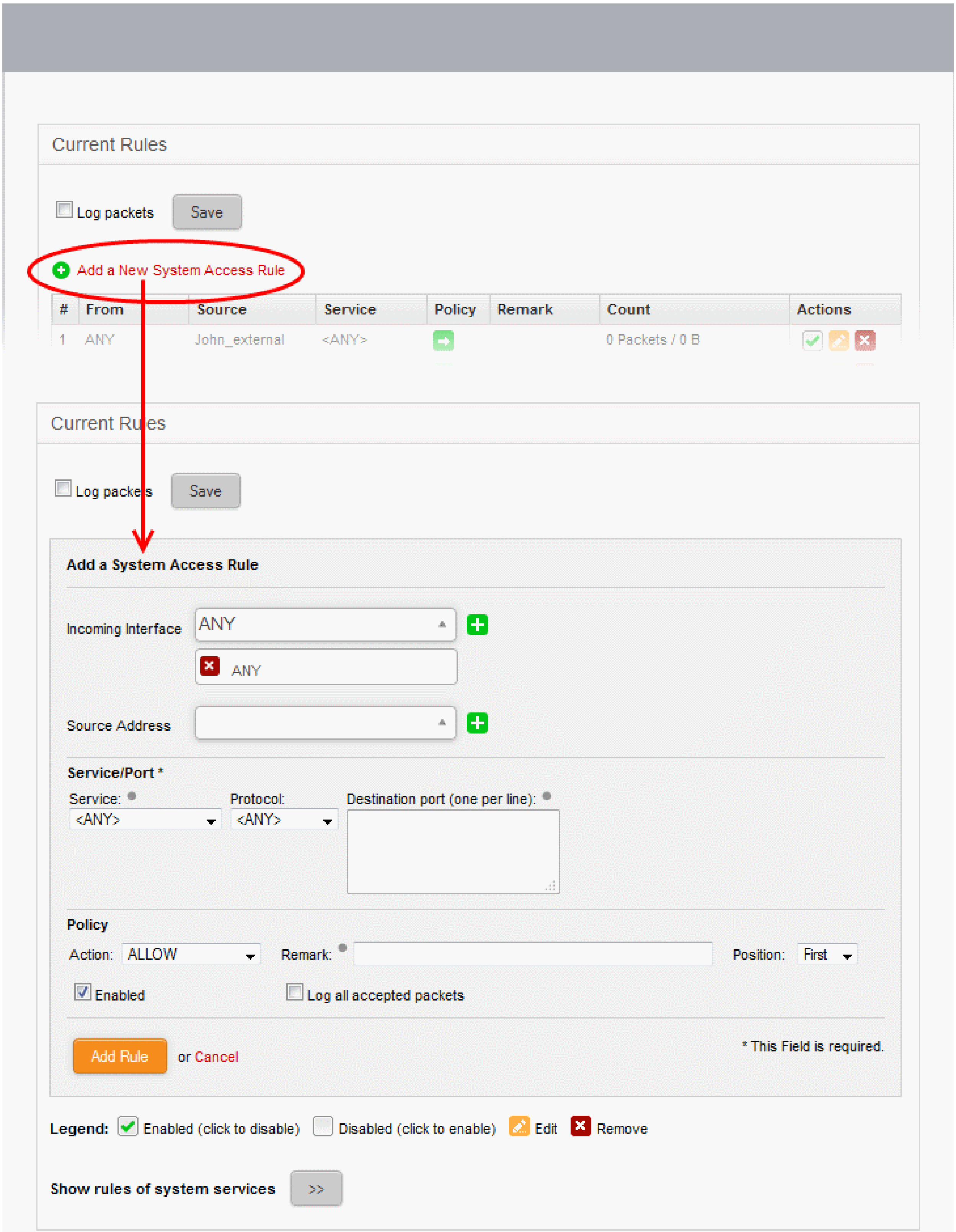
Creating System Access Firewall rules

The system access firewall rules can be created from the 'Add a system access rule' pane by defining the source, the interface of the virtual appliance at which the traffic is received and the service.

To create a new rule

- Open the 'System access configuration' interface by clicking 'Firewall' > 'System access' from the left hand side navigation.

- Click the 'Add a new system access rule' link at the top left. The 'Add a system access rule' pane will open.



#	From	Source	Service	Policy	Remark	Count	Actions
1	ANY	John_external	<ANY>			0 Packets / 0 B	

Add a System Access Rule

Incoming Interface: ANY

Source Address:

Service/Port *

Service: <ANY>

Protocol: <ANY>

Destination port (one per line):

Policy

Action: ALLOW

Remark:

Position: First

☑ Enabled

□ Log all accepted packets

* This Field is required.

Legend: ✓ Enabled (click to disable) □ Disabled (click to enable) Edit ☒ Remove

- Enter the parameters for the new rule as shown below:

Incoming Interface - Select the interface device(s) or physical ports to which the interface device(s) are connected from the drop-down, at which the traffic is received

Source Address - Specify the source of the traffic for which the rule is to be applied. The source can be an internal or external network or a specific IP address, added as a Firewall object.

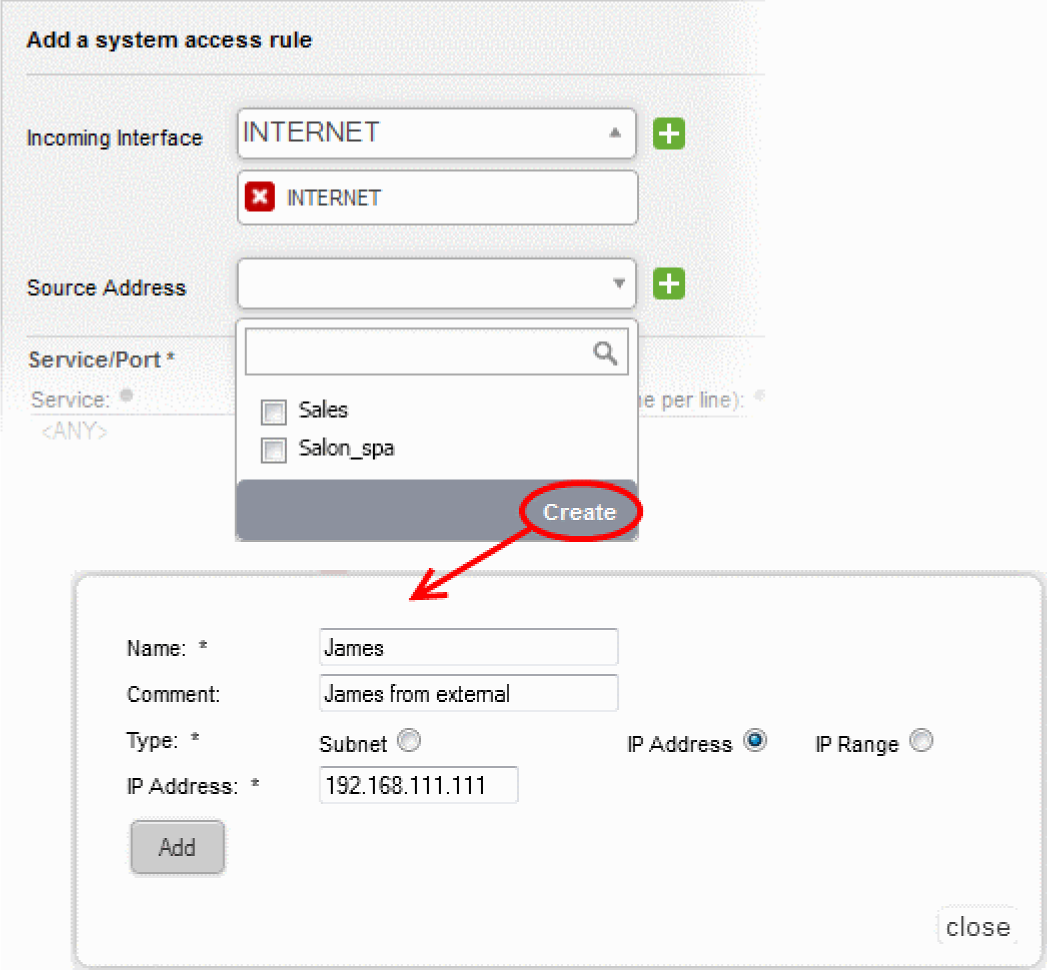
- Choose the Firewall Object(s) or Object Group(s) containing the IP address, IP Address Range or the subnet of the host(s) from the drop-down.

  If a firewall object covering the IP address/IP Address range or the subnet to be specified has not been created under the Firewall Objects interface previously, you an create a new object from this interface too.

Note: For security and operational efficiency, specify individual or narrow ranges of IP addresses/subnets rather than large subnets. For example, 10.100.150.150/32 or 10.100.150.0/24 instead of 10.100.150.0/8.

To create a new firewall object

- Click the drop-down arrow and click 'Create' at the bottom of the list. A new pane for creating a new object will appear.



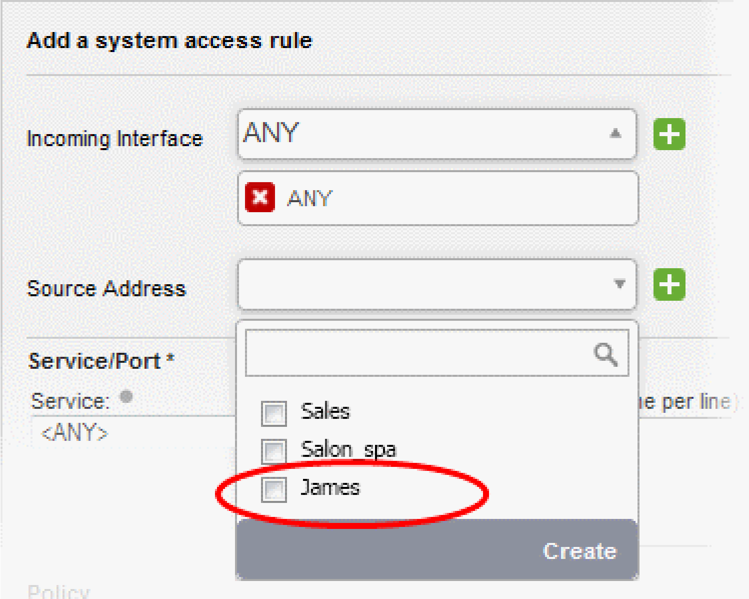
Name: * James
Comment: James from external
Type: * Subnet ○ IP Address ● IP Range ○
IP Address: * 192.168.111.111

- **Name** - Specify a name for the object (15 characters max) representing the host(s) included in the object.
- **Comment** - Enter a short description of the object.
- **Type** - Select the type by which the hosts are to be referred in the object. The available options are:
  - Subnet - Select this if a sub network of computers is to be covered by the object and enter the sub network address
  - IP address - Select this if a single host is to be covered by the object and enter the IP address of the host
  - IP range - Select this if more than one host is to be covered by the object and enter the IP

address range of the hosts

- Click 'Add'.

The new object will be added and will be available for selection from the drop-down.



The new object will also be added to the list of objects under Firewall Objects and will be available for selection for creating other firewall rules too. System access rule activities are logged, including date, time, type of event, subject id, component name and event outcome.

Service/Port - Select the type or the service hosted by the source, the protocol and the port used by the service.

- Service - Choose the type of service from the drop-down
- Protocol - Choose the protocol used by the service
- Destination port - Specify the destination port(s) of the service one by one, in the 'Destination Port' text box.

Tip: The virtual appliance is loaded with predefined combinations of service/protocol/port, like HTTP/TCP/80, <ALL>/TCP+UDP/0:65535, or <ANY>, which is a shortcut for all services, protocols, and ports. If you want to specify custom protocol/port combination, then select 'User Defined' from the service. You can also specify additional destination ports for standard combinations, for the services that run on ports different from the standard ones.

Policy - Specify whether the packets matching the rule should be allowed or denied from the Policy drop-down. The options available are:

- Allow - The data packets will be allowed without filtering
- Deny - The packets will be dropped
- Reject - The packets will be rejected, and error packets will be sent in response

General Settings - Configure the General Settings to enable/disable the rule, enable/disable logging of packets filtered by the rule, enter a short description and select a position for the rule in the list.

- Remark - Enter a short description for the rule. The description will appear in the Remark column of the respective Rules interface (Optional)
- Position - Set the priority for the rule in the list of rules in the respective rules interface. The rules in the iptables are processed in the order they appear on the list.
- Enabled - Leave this checkbox selected if you want the rule to be activated upon creation.

- Log all accepted packets - Select this checkbox if you want the packets allowed by the rule are to be logged. See **Viewing Logs** for more details on configuring storage of logs and viewing the logs.

- Click 'Add Rule'. A confirmation dialog will appear.
- Click 'Apply'. The firewall will be restarted with the new rule applied.

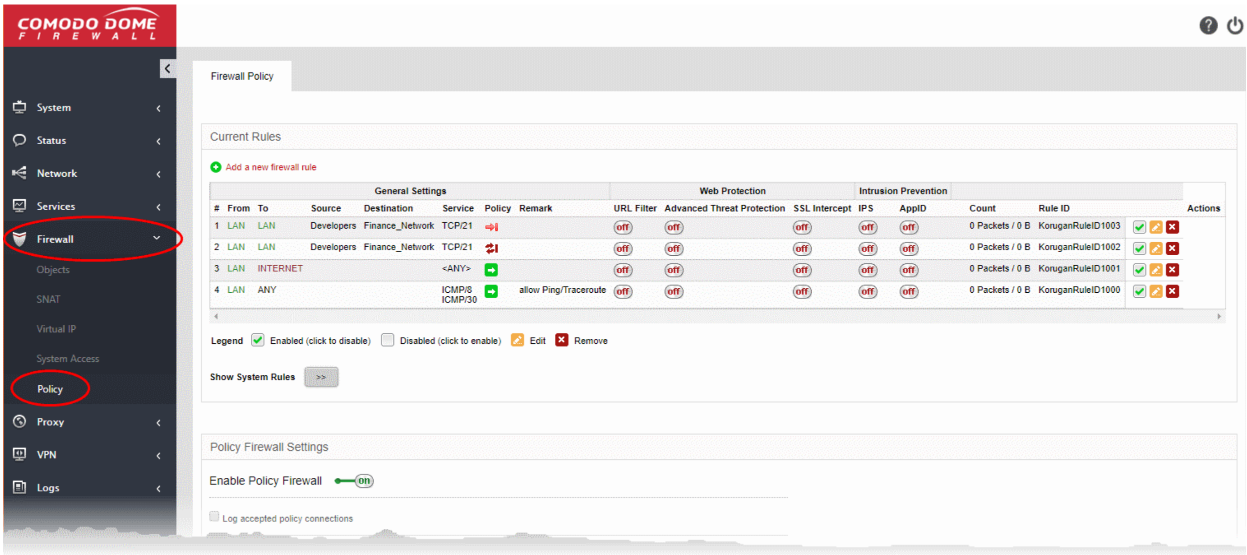
8.5 Configure Firewall Policy Rules

- Click 'Firewall' > 'Policy' in the left-hand navigation:

Comodo Dome Firewall applies a firewall 'Policy' to manage traffic flowing through your network. The policy is constructed from a series of firewall rules that are created for different types of traffic:

- Incoming traffic - Traffic from external network zones to hosts in the internal network zone
- Outgoing traffic - Traffic from internal hosts to the external network zone
- Inter-zone traffic - Traffic between network zones connected to the virtual appliance

The 'Firewall Policy' interface allows you to enable/disable firewall policy and create your own firewall rules.



Current Rules

Add a new firewall rule

General Settings								Web Protection			Intrusion Prevention				
#	From	To	Source	Destination	Service	Policy	Remark	URL Filter	Advanced Threat Protection	SSL Intercept	IPS	AppID	Count	Rule ID	Actions
1	LAN	LAN	Developers	Finance_Network	TCP/21	⇥		off	off	off	off	off	0 Packets / 0 B	KoruganRuleID1003	☑ ✎ ☒
2	LAN	LAN	Developers	Finance_Network	TCP/21	⇄		off	off	off	off	off	0 Packets / 0 B	KoruganRuleID1002	☑ ✎ ☒
3	LAN	INTERNET			<ANY>	➡		off	off	off	off	off	0 Packets / 0 B	KoruganRuleID1001	☑ ✎ ☒
4	LAN	ANY			ICMP/8 ICMP/30	➡	allow Ping/Traceroute	off	off	off	off	off	0 Packets / 0 B	KoruganRuleID1000	☑ ✎ ☒

Legend ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Show System Rules >>

Policy Firewall Settings

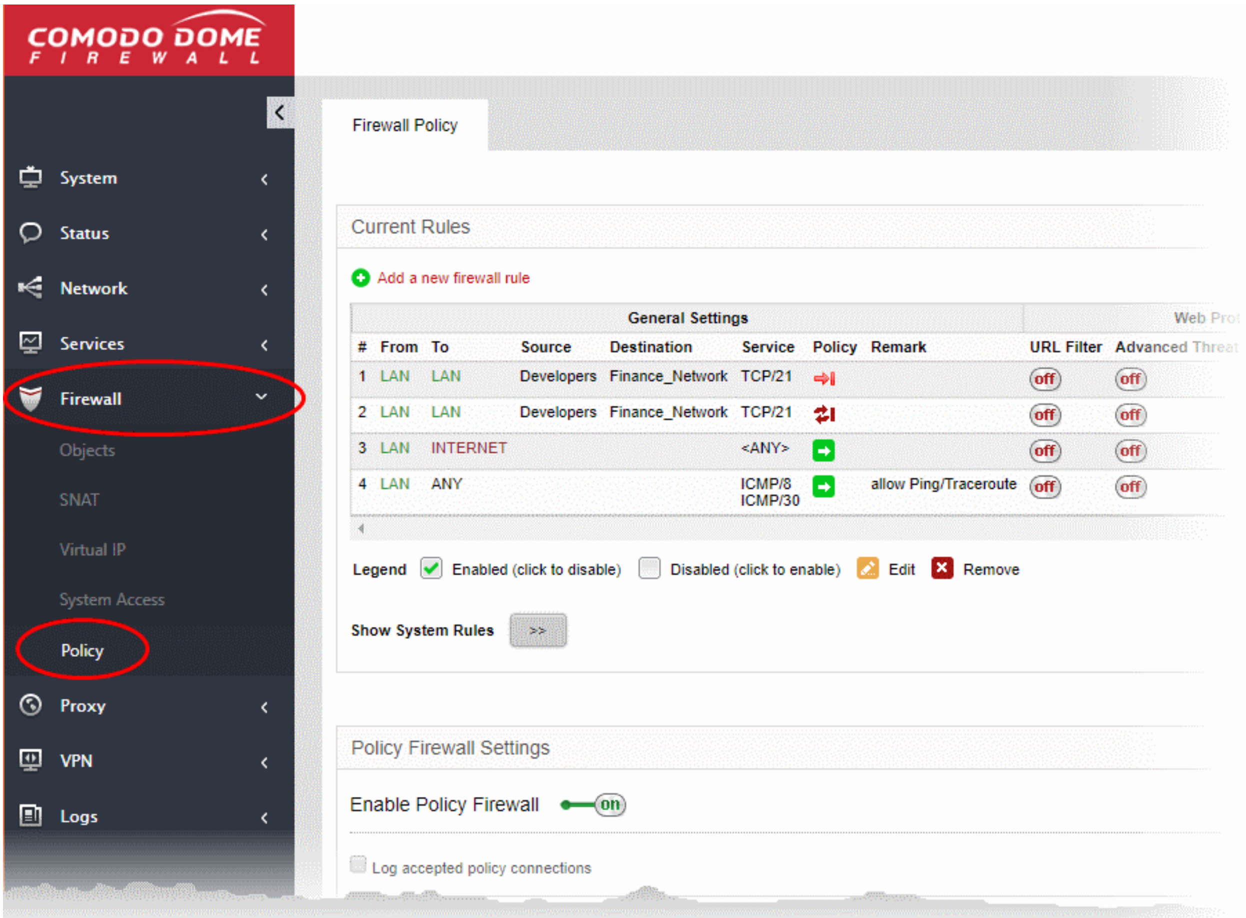
Enable Policy Firewall on

□ Log accepted policy connections

- See the next section, **Manage Firewall Policy Rules** for help with this area:

8.5.1 Manage Firewall Policy Rules

- Click 'Firewall' > 'Policy' in the left hand menu to open the firewall policy interface.
- The interface lets you define and manage firewall rules for outgoing, incoming and inter-zone traffic.
- If you haven't done so already, you will need to create firewall objects to define source and destination addresses. See **8.1.Firewall Objects** for help to do this.



Current Rules

Add a new firewall rule

General Settings								Web Prot	
#	From	To	Source	Destination	Service	Policy	Remark	URL Filter	Advanced Threat
1	LAN	LAN	Developers	Finance_Network	TCP/21	⇒		off	off
2	LAN	LAN	Developers	Finance_Network	TCP/21	⇄		off	off
3	LAN	INTERNET			<ANY>	➡		off	off
4	LAN	ANY			ICMP/8 ICMP/30	➡	allow Ping/Traceroute	off	off

Legend ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Show System Rules >>

Policy Firewall Settings

Enable Policy Firewall on

□ Log accepted policy connections

The interface contains two panes:

- **Current Rules** - The upper, 'Current Rules', pane lists all active rules and allows you to add and edit rules. See **Managing Firewall Rules** for more details on viewing and managing the rules.
- **Policy Firewall Settings** - The lower ' Policy Firewall Settings' pane displays the current enabled/status of the policy firewall, allows the administrator to change the status and to configure the policy firewall log. See **Configure Policy Firewall Settings** for more details.

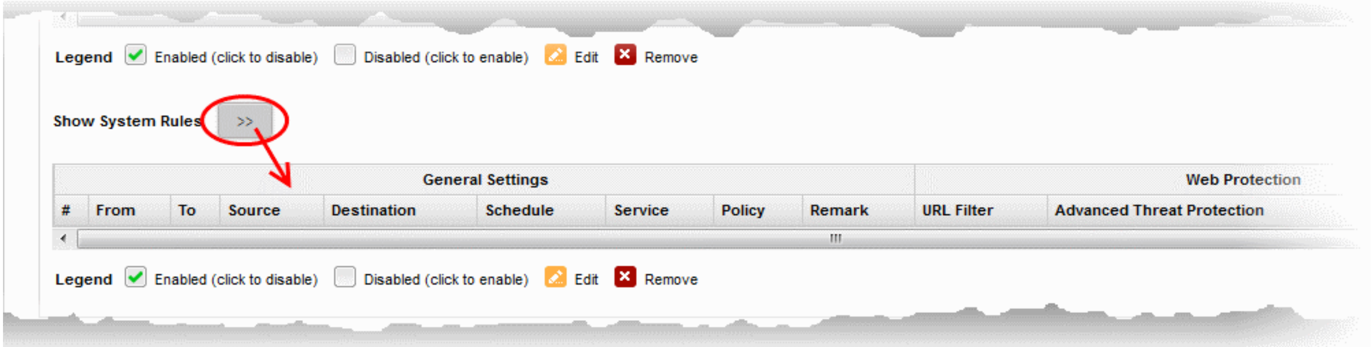
The Firewall Rules

The 'Current Rules' pane displays a list of rules in action with their configuration parameters and allows the administrator to manage them and to create new rules.

	Policy Firewall Rules Table - Column Descriptions	
Category	**Column**	**Description**
General Settings	#	Serial number of the rule.
	From	The interface or network zone from which the traffic originates.
	To	The interface or network zone to which the traffic is directed.
	Source	The firewall object or object group which contains the addresses of the host(s) from which traffic originates.
	Destination	The firewall object or object group which contains the addresses of the host(s) to which traffic is sent.
	Service	Protocol and port that will be used by traffic affected by this rule.

	Policy	Indicates the action taken on the data packets intercepted by the rule • ➡ - The data packets will be allowed • ⇥ - The packets will be denied. • ⇄ - The packets will be rejected, and error message will be sent in response
	Remark	A short description of the rule
Web Protection	URL Filter	Whether or not the 'Web Filter' security profile is enabled for the rule. If enabled you will see the name of the profile.
	Advanced Threat Protection	Whether or not the 'Advanced Threat Protection' component is enabled for the rule.
	SSL Intercept	Whether or not the 'HTTPS Intercept Web Filter security profile' is enabled for the rule. If enabled you will see the name of the profile.
Intrusion Prevention	IPS	Whether or not the 'Intrusion Protection System (IPS)' security profile is enabled for the rule.
	AppID	Whether or not the the 'Application Filter' rule is enabled for the policy.
	Count	Indicates the number of packets and size of data intercepted by the rule.
	Rule ID	Identity number of the rule. This is determined by the order in which the rules were created for the device/organization. Traffic is allowed or denied based on the first matching rule in ascending order of ID numbers. This is regardless of the order of the rules as shown in the table.
	Actions	Controls for managing the rule. ☑ - Enable or disable the rule ✎ - Modify the rule. The 'Edit' interface is similar to the 'Policy Firewall Rule Editor' interface used to create new rules. See **Creating Policy Firewall rules** for more details. ☒ - Remove the rule.

- Clicking the right arrow button beside 'Show system rules' displays a list of firewall rules auto generated by the DFW virtual appliance. These rules cannot be modified or removed.



Legend ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Show System Rules >>

General Settings									Web Protection	
#	From	To	Source	Destination	Schedule	Service	Policy	Remark	URL Filter	Advanced Threat Protection

Legend ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Create Policy Firewall rules

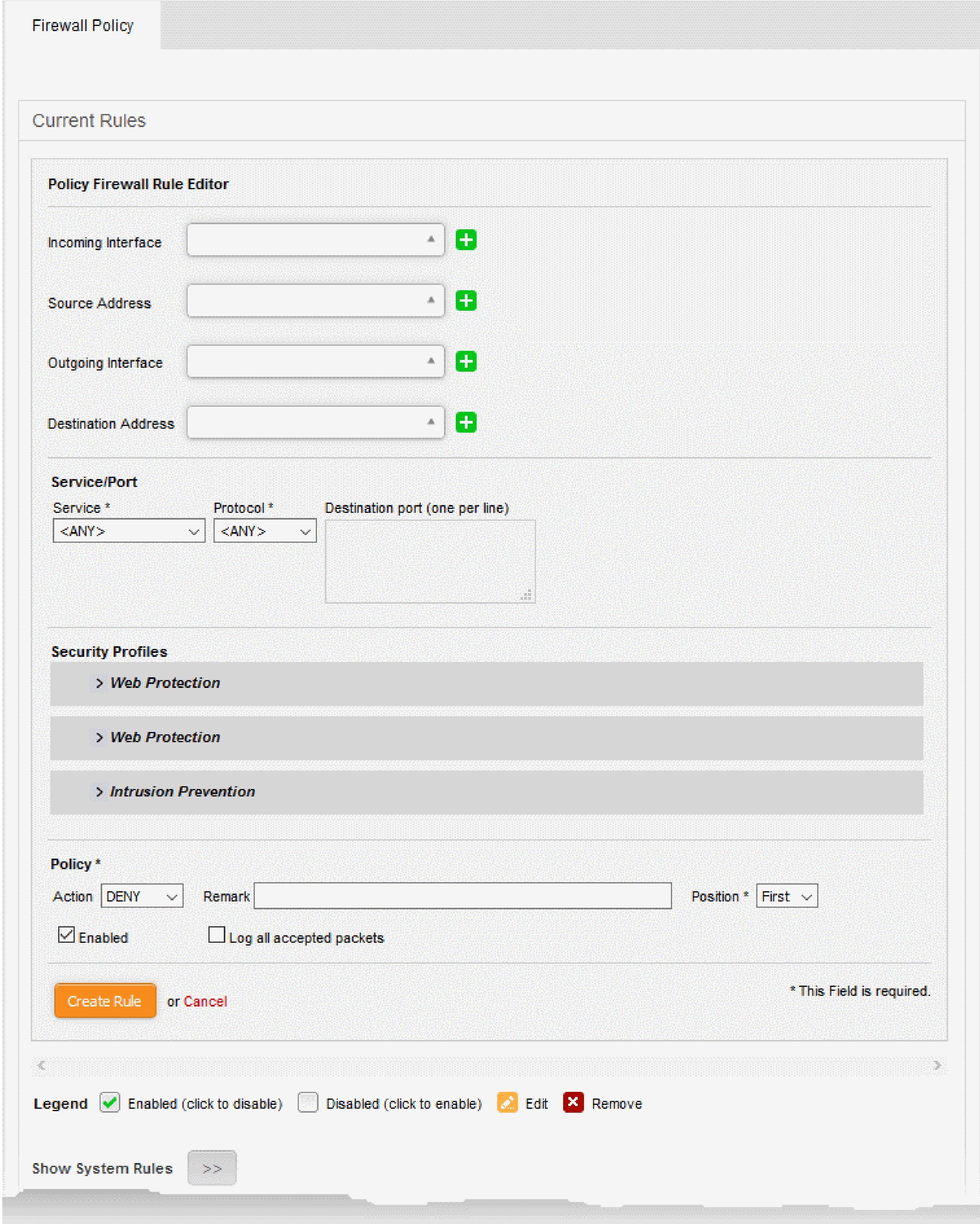
Each Firewall rule contains three components:

- General Settings - Specify source and destination addresses and the service/protocol of packets to be intercepted by the rule. You can specify the firewall address objects and object groups as source and destination addresses. See **Firewall Objects** for more details on adding firewall address objects.
- Web Protection - Enable or disable URL filtering, Advanced Threat Protection (ATP) and SSL Interception. You can also choose pre-configured profiles for them. See **Advanced Threat Protection**, and **HTTP/HTTPS Proxy Server** for help to create these profiles.
- Content Flow Check - Enable or disable Intrusion Prevention and Application Detection settings for the rule. You can configure the default intrusion prevention and application detection profile to be used in the rules. See **Intrusion Prevention** for more details.

You can create different rules for different configurations for each of these components and specify the action to be applied on the data packets intercepted by them. The rules will be applied to the inbound and outbound packets in order.

To create a new firewall rule

- Click 'Firewall' > 'Policy' from the left hand side navigation
- Selecting the 'Firewall Policy' tab.
- Click the 'Add a new firewall rule' link at the top left. The 'Policy Firewall Rule Editor' will open.



The 'Policy Firewall Rule Editor' interface is divided into four areas for specifying the different components of the rule:

- **Address Settings** - Choose the source and destination of the traffic to be intercepted by the rule
- **Service/Port** - Specify the service pertaining to the traffic to be intercepted by the rule
- **Security Profiles** - Configure settings for intrusion prevention and web protection such as URL filtering, Advanced Threat Protection (ATP) and HTTPS intercepts.
- **Policy Settings** - Configure to allow or block the traffic intercepted by the rule

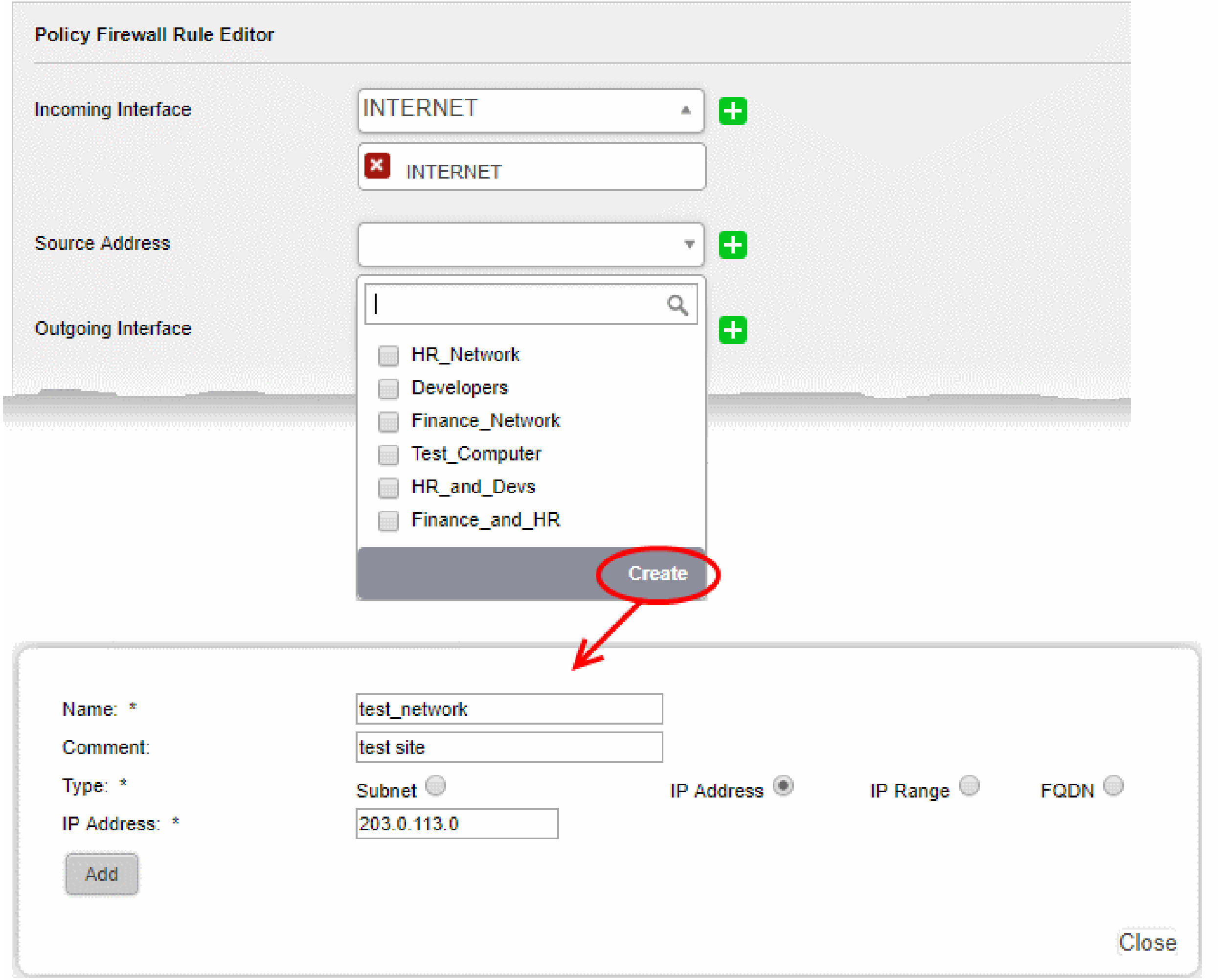
Address Settings

- **Incoming Interface** - Choose the interface device through which the traffic is received, from the drop-down.
- **Source Address** - Choose the firewall object or the object group that covers the IP address, IP address range or the subnet, on which the traffic to be intercepted by the rule, is received.

  If a firewall object covering the IP address/IP Address range or the subnet to be specified has not been created under the Firewall Objects interface previously, you an create a new object from this interface too.

  To create a new firewall object

  - Click the drop-down arrow and click 'Create' at the bottom of the list. A new pane for creating a new object will appear.



Policy Firewall Rule Editor

Incoming Interface: INTERNET

Source Address:

Name: * test_network

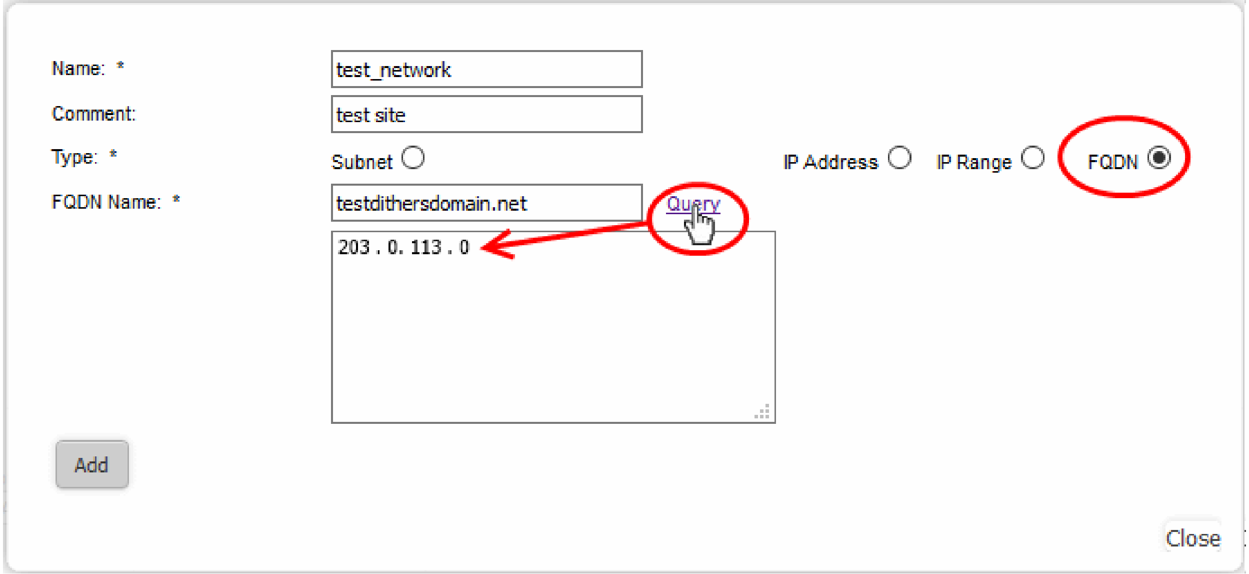
Comment: test site

Type: * Subnet ○ IP Address ● IP Range ○ FQDN ○

IP Address: * 203.0.113.0

- **Name** - Specify a name for the object (15 characters max) representing the host(s) included in the object.
- **Comment** - Enter a short description of the object.
- **Type** - Select the type by which the hosts are to be referred in the object. The available options are:
  - Subnet - Select this if a sub network of computers is to be covered by the object and enter the sub network address
  - IP address - Select this if a single host is to be covered by the object and enter the IP address of the host
  - IP range - Select this if more than one host is to be covered by the object and enter the IP address range of the hosts

- FQDN - Select this if you want to add domains by specifying their fully qualified domain name(s) (FQDN) is to be covered by the object
  - Enter the domain name (without 'http://' or 'https://') in the FQDN Name field and click the 'Query' link.


Name: * test_network

Comment: test site

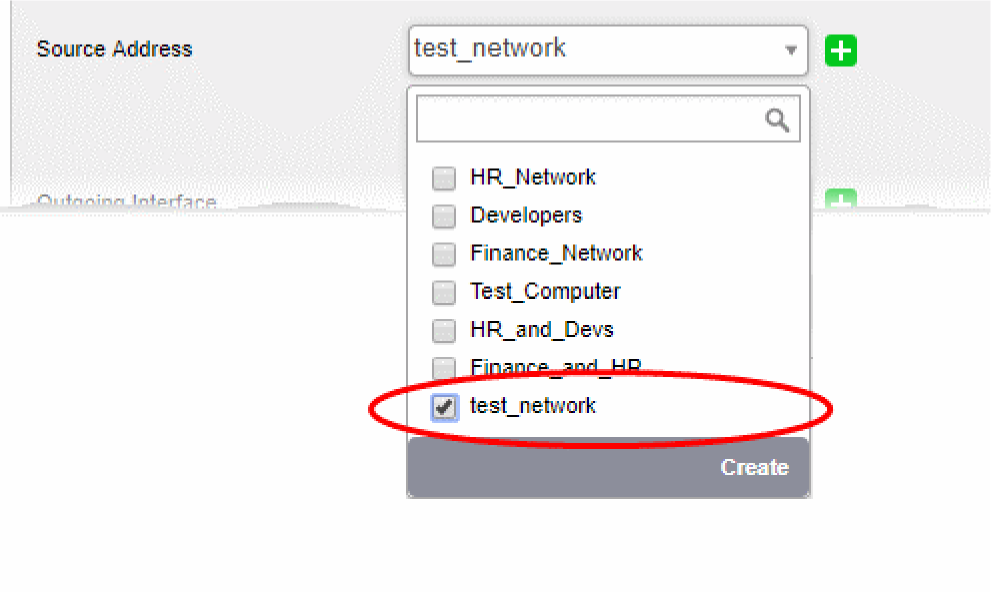
Type: * Subnet ○ IP Address ○ IP Range ○ FQDN ●

FQDN Name: * testdithersdomain.net

203 . 0. 113 . 0

  - The firewall will perform a DNS query and add the resolved IP address in the box below
  - To add more domains, enter the names one by one in the FQDN Name field and click the 'Query' link.
- Click 'Add'.

The new object will be added and will be available for selection from the Select network/IPs drop-down.


Source Address: test_network

- □ HR_Network
- □ Developers
- □ Finance_Network
- □ Test_Computer
- □ HR_and_Devs
- □ Finance_and_HR
- ☑ test_network

The new object will also be added to the list of objects under Firewall Objects and will be available for selection for creating other firewall rules too.

- **Outgoing Interface** - Choose the interface device through which the traffic is directed, from the drop-down.
- **Destination Address** - Choose the Firewall Object or Object Group containing the IP address, IP Address Range or the subnet of the host(s) to which the traffic is directed, from the drop-down.

If a firewall object covering the IP address/IP Address range or the subnet to be specified has not been created under the Firewall Objects interface previously, you an create a new object from this interface too. See **explanation above** for more details.

Service/Port

Service/Port - Select the type or the service hosted by the source, the protocol and the port used by the service.

- Service - Choose the type of service from the drop-down
- Protocol - Choose the protocol used by the service
- Destination port - Specify the destination port(s) of the service one by one, in the 'Destination Port' text box.

> **Tip**: The virtual appliance is loaded with predefined combinations of service/protocol/port, like HTTP/TCP/80, <ALL>/TCP+UDP/0:65535, or <ANY>, which is a shortcut for all services, protocols, and ports. If you want to specify custom protocol/port combination, then select 'User Defined' from the service. You can also specify additional destination ports for standard combinations, for the services that run on ports different from the standard ones.

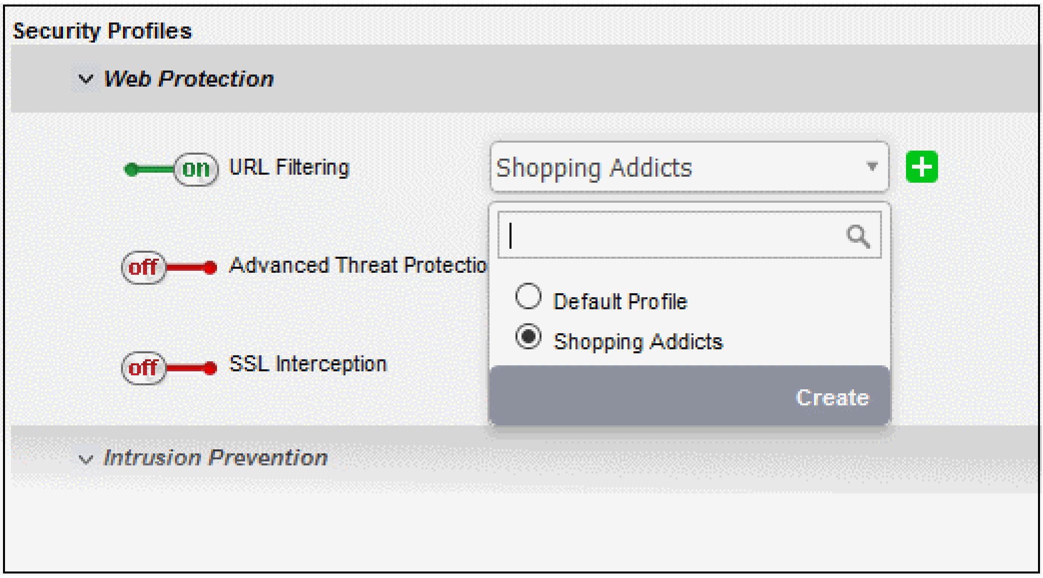
Security Profiles

The Security Profiles area allows you to enable/disable various security features for **Web Protection** and **Intrusion Prevention.**

Web Protection - Clicking the down arrow in the 'Web Protection' stripe will open the security features for web protection:

- **URL Filtering** - Allows you to enable/disable the URL filtering to be applied to the traffic intercepted by the rule.
    - To enable Web Filtering, move the toggle switch to ON position and select the URL filter profile that covers the websites to be blocked/allowed, from the drop-down.

  The rules with Web Filtering enabled and configured with a URL filter profile will be added for HTTP/HTTPS Proxy server settings. The URL Access policies for HTTP/HTTPS Proxy Server can be viewed from the 'Proxy' > 'HTTP/HTTPS' > 'URL Filter' interface. See **Configuring URL and Content Filtering Policies** for more details.



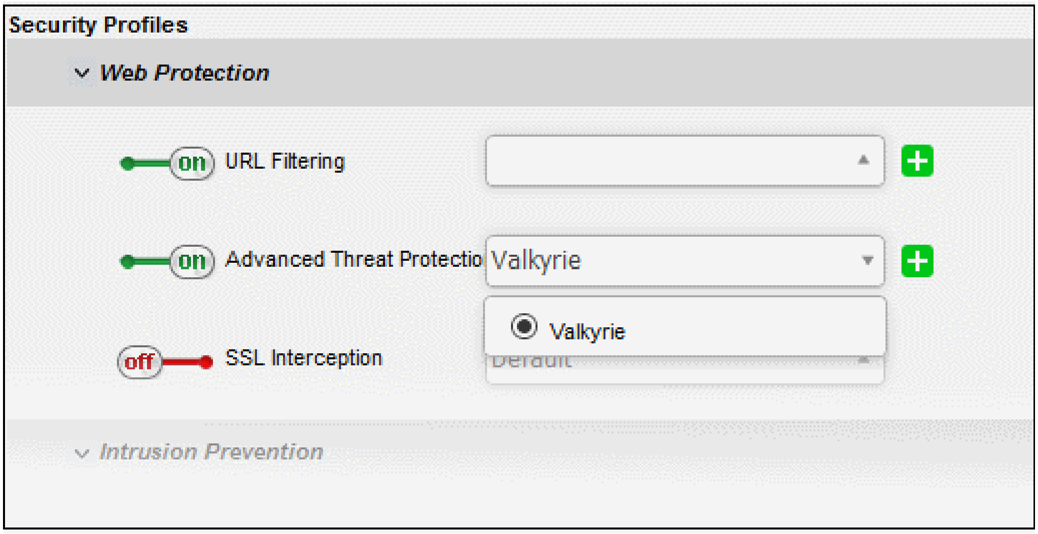
The 'URL Filtering' drop-down displays a list of profiles created and managed under the 'Proxy' > 'HTTP/HTTPS' > 'URL Filter' interface. If the profile that covers the required websites to be specified has not been created under the 'Proxy' > 'HTTP/HTTPS' > 'URL Filter' previously and hence not available in the drop-down, you can create a profile from this interface too.

- Click the drop-down arrow and click 'Create' at the bottom of the list. A new pane for creating a new profile will appear. See section **Configuring URL and Content Filtering** for more details on creating a new profile.

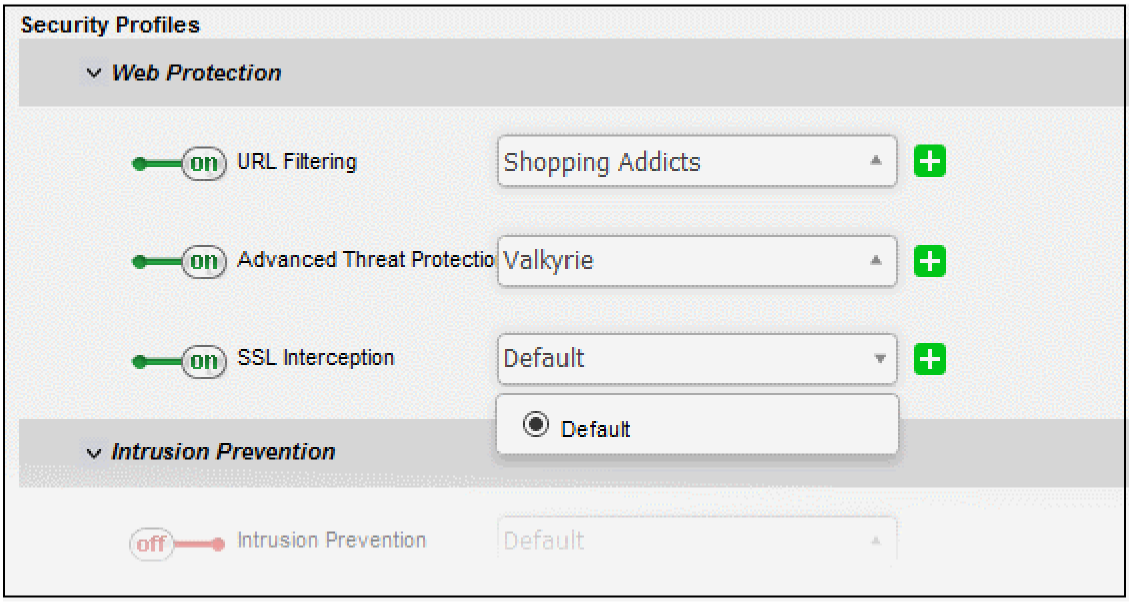
- Advanced Threat Protection - Allows you to enable/disable Advanced Threat Protection (ATP) to be applied to the traffic intercepted by the rule.

  The ATP default profile can be managed from 'Services' > 'Advanced Threat Protection' > 'Profiles' interface. For more details on managing the ATP profile, see section **Managing the ATP Profile**.

  - To enable ATP for Web Protection, move the toggle switch to ON position and select the ATP profile, from the drop-down. Please note DFW virtual appliance is configured to use Valkyrie for analysis of unknown files that is downloaded from the internet.



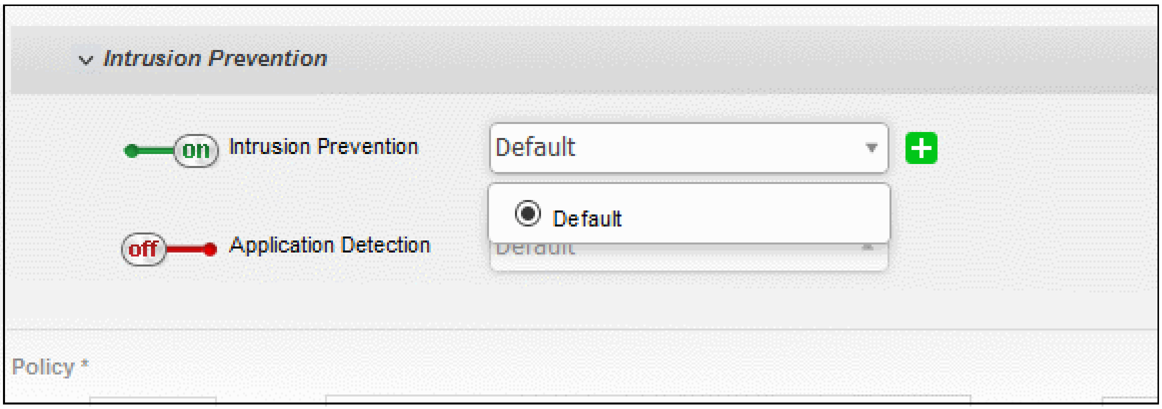
- **SSL Interception** - Allows you to enable/disable HTTPS exceptions to be applied to the traffic intercepted by the rule.
  - To enable SSL Interception, move the toggle switch to ON position and select the profile, from the drop-down.


Security Profiles
Web Protection
on URL Filtering Shopping Addicts
on Advanced Threat Protectio Valkyrie
on SSL Interception Default
Default
Intrusion Prevention
off Intrusion Prevention Default

On selecting 'Default', the HTTPS Exceptions settings as configured under the 'Proxy' > 'HTTP/HTTPS' > 'HTTPS Exceptions' interface will be applied. See **HTTPS Proxy** for more details.

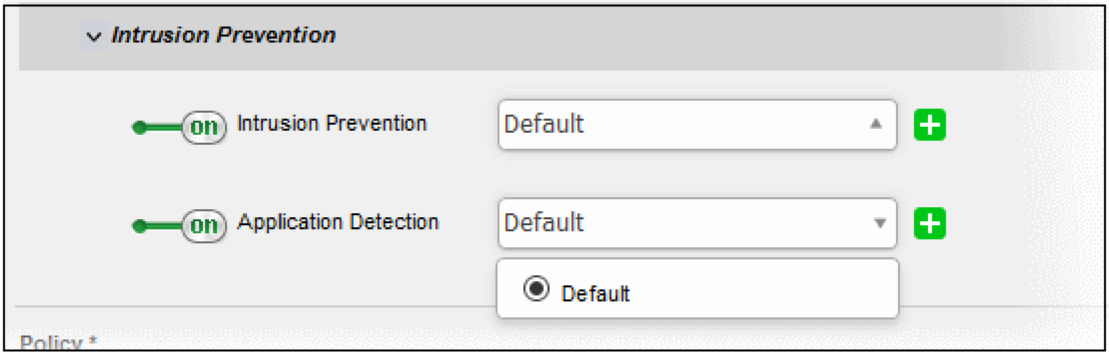
Intrusion Prevention - Clicking the down arrow in the 'Intrusion Prevention' stripe will open the security features for intrusion prevention:

- **Intrusion Prevention** - Allows you to enable/disable 'Intrusion Prevention' to be applied to the traffic intercepted by the rule.
  - To enable 'Intrusion Prevention', move the toggle switch to ON position and select the profile, from the drop-down.



On selecting 'Default', the rules settings as configured under 'Services' > 'Intrusion Prevention' > 'IPS Rules' interface will be applied. See '**Intrusion Prevention**' for more details.

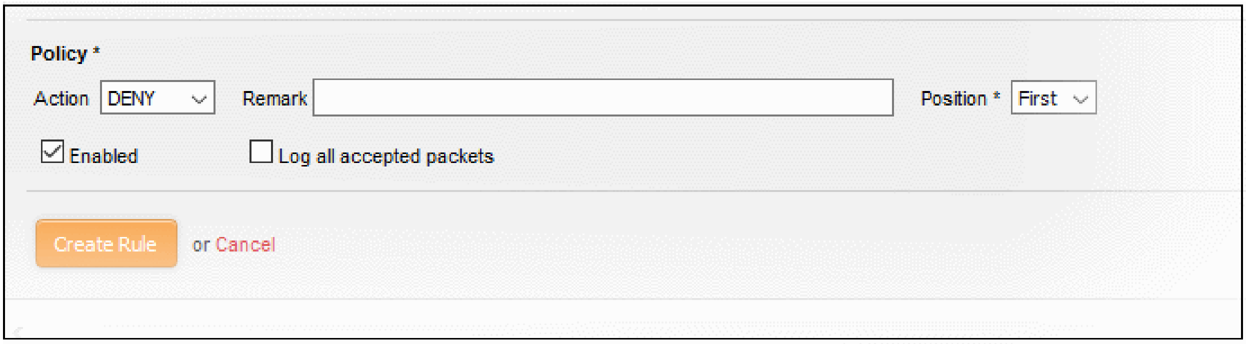
- **Application Detection** - Allows you to enable/disable 'Application Detection' to be applied to the traffic intercepted by the rule.
  - To enable 'Application Detection', move the toggle switch to ON position and select the profile, from the drop-down.



On selecting 'Default', the rules settings as configured under 'Services' > 'Intrusion Prevention' > 'Application Identification' interface will be applied. See '**Intrusion Prevention**' for more details.

Policy Settings

- **Action** - Specify whether the packets matching the rule should be allowed or denied from the Policy drop-down. The options available are:
  - Allow - The data packets will be allowed without filtering
  - Deny - The packets will be dropped
  - Reject - The packets will be rejected, and error packets will be sent in response
- **Remark** - Enter a short description for the rule. The description will appear in the Remark column of the Rules table.
- **Position** - Set the priority for the rule in the list of rules in the respective rules interface. The rules in the iptables are processed in the order they appear on the list.
- **Enabled** - Leave this checkbox selected if you want the rule to be activated upon creation.
- **Log all accepted packets** - Select this checkbox if you want the packets allowed by the rule are to be logged. See **Viewing Logs** for more details on viewing the logs.



Policy *

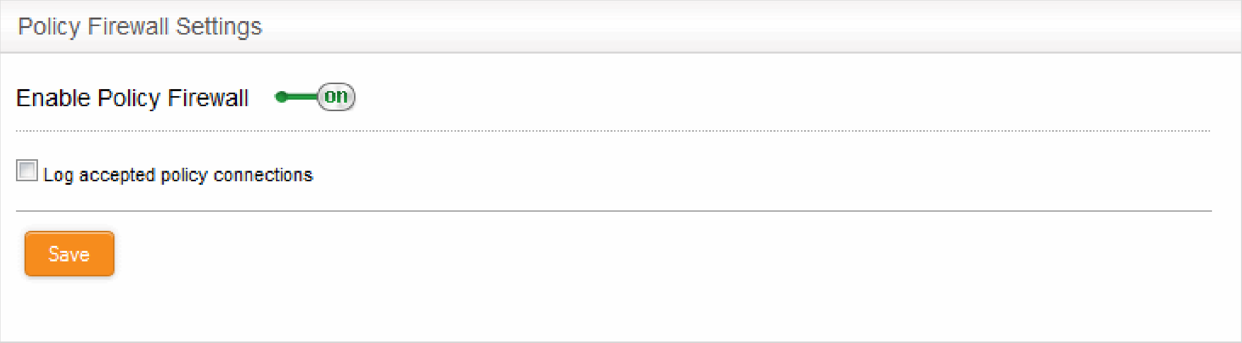
Action DENY | Remark | Position * First

☑ Enabled □ Log all accepted packets

- Click 'Create Rule'. A confirmation dialog will appear.
- Click 'Apply'. The firewall will be restarted with the new rule applied.

Configuring the Policy Firewall Settings

The lower 'Policy Firewall Settings' pane allows the administrator to enable/disable the Policy firewall rules and to opt for logging the packets that pass the rule.



Policy Firewall Settings

Enable Policy Firewall on

□ Log accepted policy connections

- Use the 'Enable policy firewall' switch to enable/disable the policy.
- Select the 'Log accepted policy connections' checkbox to log the packets that has passed the Firewall Policy. See **Viewing Logs** for more details on viewing the logs.
- Click 'Save' for your settings to take effect .

Policy firewall rule activities are logged, including date, time, type of event, subject id, component name and event outcome.

9 Configuring Proxy Services

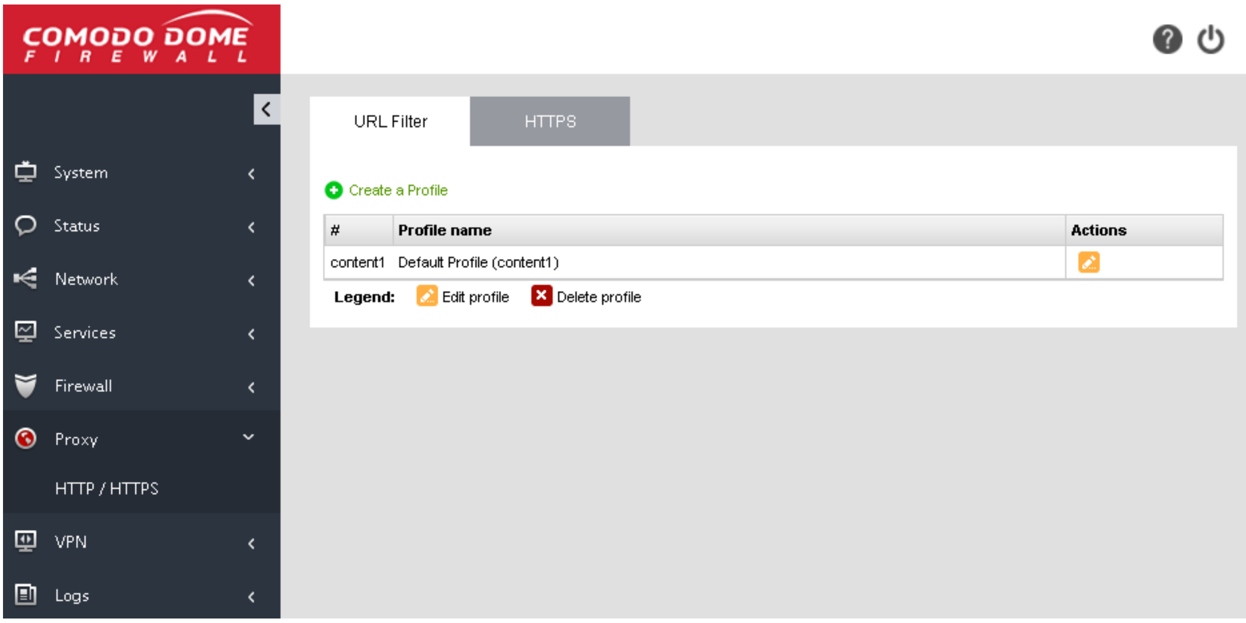
Comodo Dome Firewall has the ability to provide proxy services for HTTP/HTTPS protocols. Each proxy service can be individually and independently configured and enabled/disabled. Once configured, user traffic to the service in question will pass through the specified proxy server. The proxy will act as an intermediary between client requests and the requested external or internal resource, allowing administrators to optionally run additional services on the traffic before it is forwarded to the intended destination. Services can include URL filtering, compliance checking, virus scanning, spam filtering and more.

For each proxy to function properly, the corresponding service should be running. If a proxy service is started, the corresponding network service will also be automatically started, if not already running. Hence before configuring and starting a proxy service, the corresponding network service should have been configured according to the requirements.

- **HTTP / HTTPS** - Web proxy service for HTTP/HTTPS protocols. The administrator can configure content/url filtering, SSL support for HTTPS and HTTPS Exceptions.

The 'Proxy' interface can be accessed by selecting the 'Proxy' tab from the menu bar.

Clicking the 'Proxy' tab from the left hand side navigation opens a sub-menu containing options to access to different configuration screens to manage the proxy services.



#	Profile name	Actions
content1	Default Profile (content1)	✎

Legend: ✎ Edit profile ☒ Delete profile

The following sections provide detailed descriptions of different proxy services and their configuration:

- **HTTP/HTTPS Proxy**

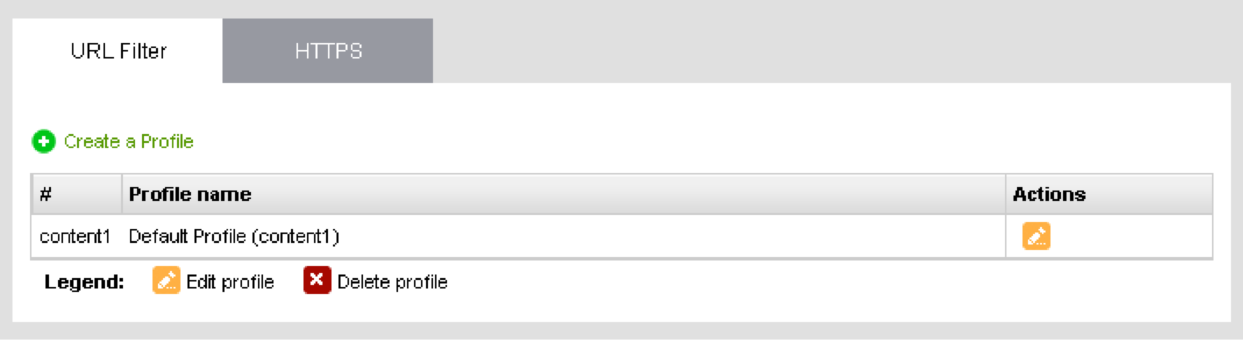
9.1 HTTP/HTTPS Proxy Server

Comodo Dome Firewall uses the HTTP proxy technology to cache a large variety of resources, such as documents, images and webpages, which have been requested by hosts connected to internal network zones. Dome Firewall will answer the initial request for a document or webpage by retrieving the resource from the original location. The cached version will then be served to answer subsequent requests for the same resource. This reduces network traffic and reduces page load time for end-users.

The HTTP Proxy server maintains logs of query parameters in requested URLs, which pages were subject to content filtering and the user agents used by browsers to identify themselves to the web servers. For more details on setting up the location for storing the logs and viewing the logs, refer to the section **Viewing Logs**.

The 'HTTP/HTTPS proxy' interface enables the administrator to configure various parameters and security features of the HTTP/HTTPS proxy service.

To access the 'HTTP/HTTPS proxy' interface, click 'Proxy' > 'HTTP/HTTPS ' from the left hand side navigation.



#	Profile name	Actions
content1	Default Profile (content1)	✎

Legend: ✎ Edit profile ☒ Delete profile

The interface contains three tabs:

- **URL Filter** - Allows the administrator to limit access to websites based on content types and specific URLs. See **Configuring URL and Content Filtering** for more details.
- **HTTPS** - Allows the administrator to configure HTTPS proxy service and certificates. See **HTTPS Proxy** for more details.

9.1.1 Configuring URL and Content Filtering

Comodo Dome Firewall uses the embedded Web Filtering technology from CYREN, to govern the websites accessed through the HTTP proxy service. The feature allows the administrator to create profiles for filtering URLs:

- by specifying webpages to be filtered based on content category.
- by specifying whitelist/blacklist of urls and domains, to be allowed/denied.

These profiles can be used as filter profiles in Firewall Policy Rules. See **Managing Firewall Policy Rules** for more details.

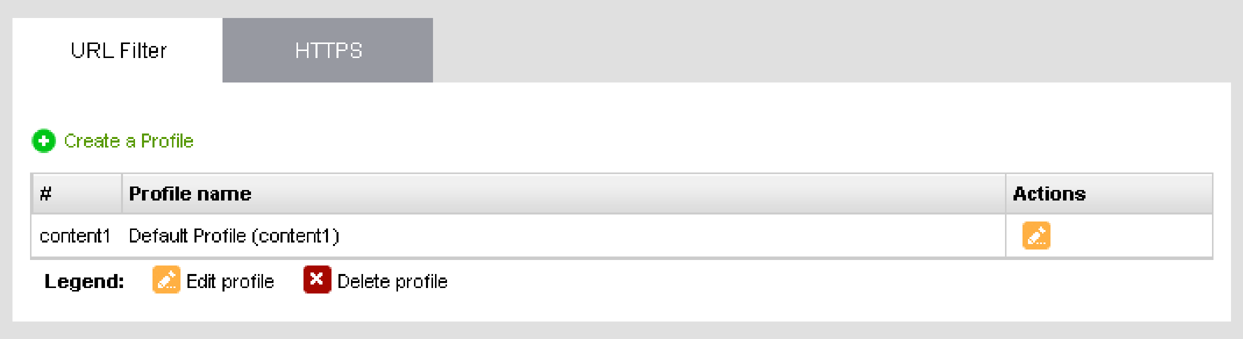
The URL/Web filtering profiles can be created for different enterprise and home network scenarios. For example, filter profiles may be applied:

- To beef security by automatically blocking malware sites to the network
- To prevent employees from visiting social networking sites during working hours.
- To imply parental control by blocking webpages with inappropriate content to juvenile users

The Web Filtering profiles can be created and managed through 'URL Filter' interface.

To configure the Web Filter

- Click 'Proxy' > 'HTTP/HTTPS' from the left hand side navigation
- Click the 'URL Filter' tab.



#	Profile name	Actions
content1	Default Profile (content1)	✎

Legend: ✎ Edit profile ☒ Delete profile

The interface displays a list of existing web filtering profiles and enables the administrator to create new profiles. The list contains 'Default Profile' which can be edited or but cannot be deleted as the first item. The default profile allows access to all the web pages, and applied to the access policies to which no filter policy is specified.

URL Filter - Column Descriptions	
Column	**Description**
#	ID number of the profile.
Profile name	The name of the profile, for easy identification
Actions	Displays control buttons for managing the profile. ✎ - Opens the 'Profile editor' interface and enables to edit the parameters of the profile. The editor interface is similar to the interface for adding a profile. See **Creating a Web Filter Profile** for more details.

	✖ - Removes the profile.

Creating a Web Filter Profile

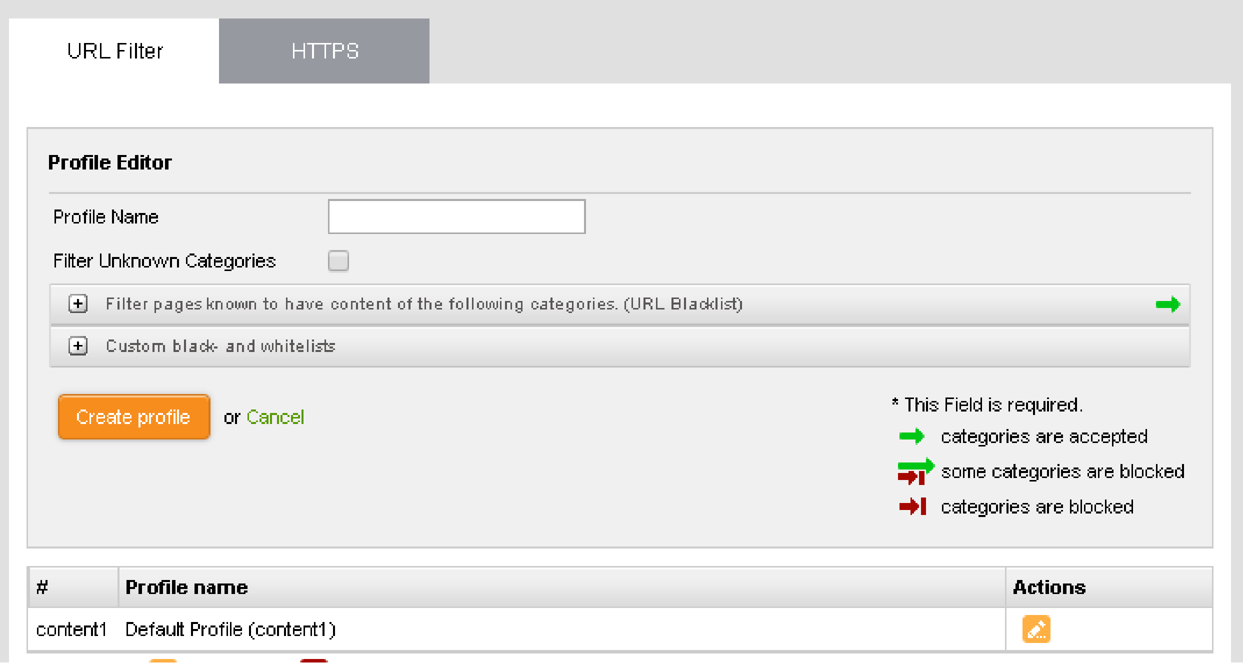
A Web Filter profile can be created by specifying the filter parameters in two ways:

- Specifying the content categories - The web pages having content falling into specified categories will be automatically blocked
- Creating custom URL Whitelist/Blacklist - The URLs and Domains specified in the whitelist will be passed without filtering and the URLs and domains in the blacklist will be blocked.

A single profile can be created with a combination of both the category filter and whitelist/blacklist.

To create a Web Filtering profile

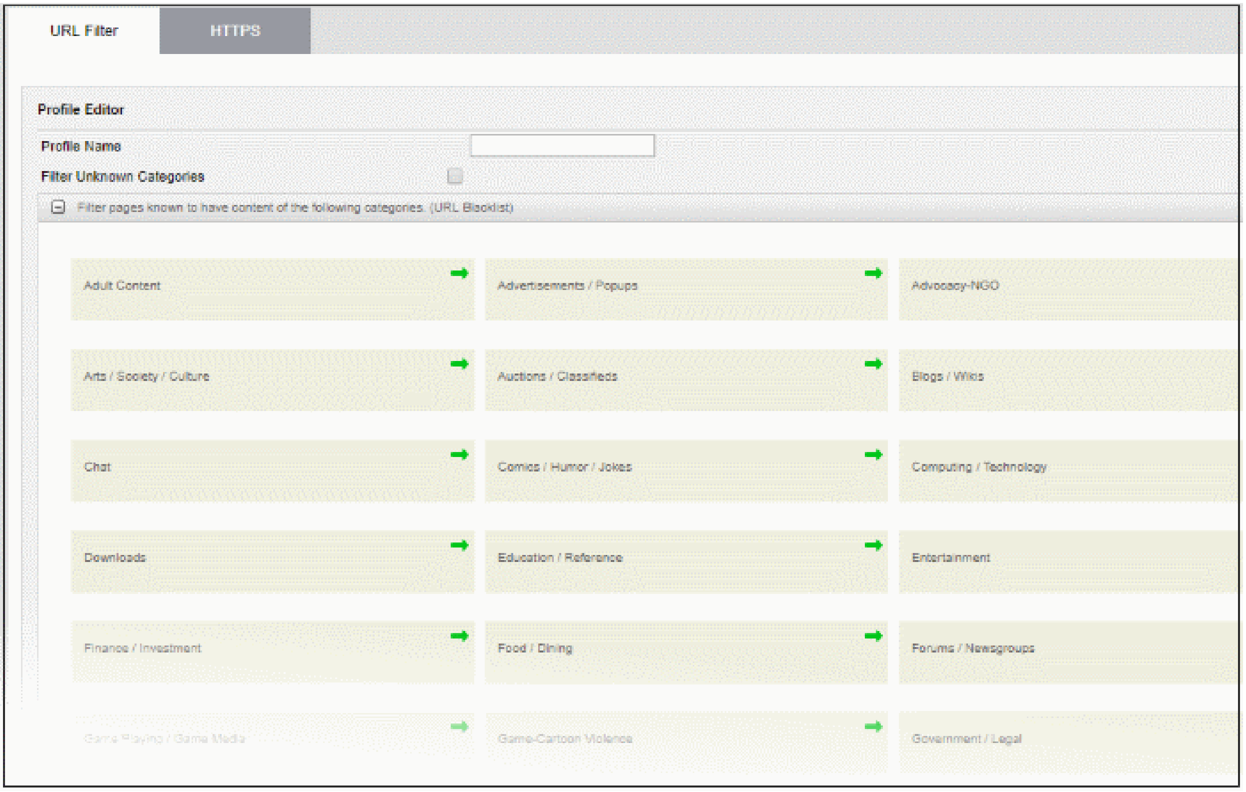
- Click the 'Create a Profile' link at the top left of the interface. The 'Profile editor' pane will open for adding a new profile.


URL Filter
HTTPS
Profile Editor
Profile Name
Filter Unknown Categories
Filter pages known to have content of the following categories. (URL Blacklist)
Custom black- and whitelists
Create profile
or Cancel
* This Field is required.
categories are accepted
some categories are blocked
categories are blocked

#	Profile name	Actions
content1	Default Profile (content1)	✎

- Profile Name - Enter a name for the profile to be created, for easy identification
- Filter Unknown Categories - Select this checkbox if you want the proxy to block all the websites that do not fall under any of the category in the built-in list of categories. The list can be viewed by clicking the ' Filter pages known to have content of the following categories' stripe below the option.

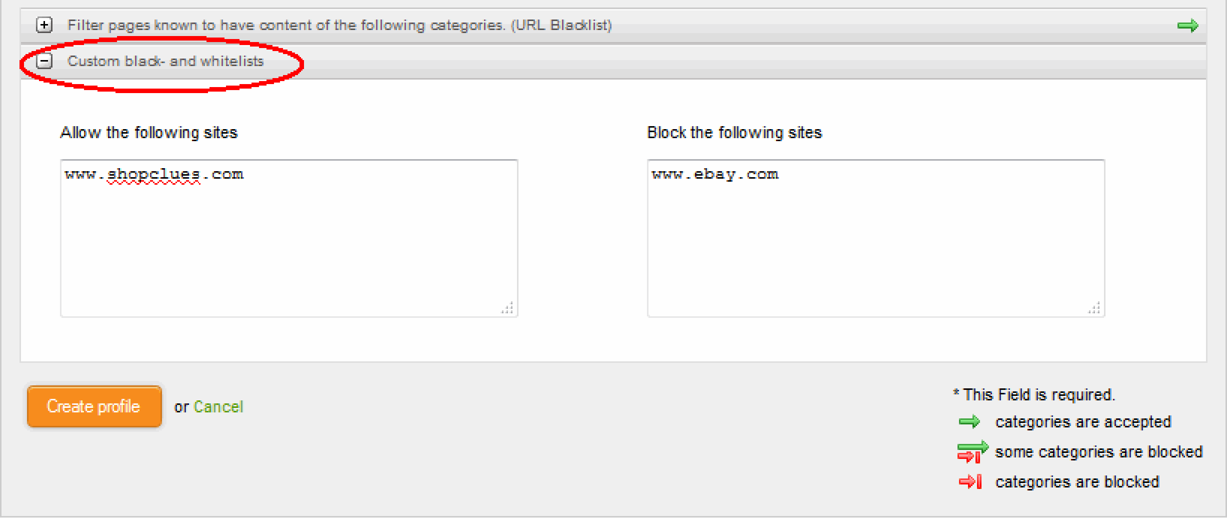
- To specify the categories for blocking the pages containing the content falling under them, click the 'Filter pages known to have content of the following categories. (URL Blacklist)' stripe.



Each main category is displayed as a tile. The arrow at the top right of each tile indicates whether the category is allowed or blocked.

➡	-	Indicates that the category is allowed
⇥	-	Indicates that the category is blocked

- To block a category, click on the green arrow. The arrow will turn red, indicating that the category will be blocked.
- To add URLs to whitelists or blacklists, click the 'Custom black-and whitelists' stripe. The text boxes for entering the whitelist and blacklist domains will open.


⊞ Filter pages known to have content of the following categories. (URL Blacklist)
⊟ Custom black- and whitelists
Create profile
or Cancel

Allow the following sites

www.shopclues.com

Block the following sites

www.ebay.com

* This Field is required.
➡ categories are accepted
⇥ some categories are blocked
⇥ categories are blocked

- Enter the URLs or domains of the websites to be allowed in the 'Allow the following sites' text box.
- Enter the URLs or domains of the websites to be denied in the 'Block the following sites' text box.

Note:

- The URLs of the websites/domains should not contain the protocols (http:// or https://)
- Wildcard characters are allowed while specifying domain(s) and sub domain(s)

- Click 'Create profile'. A confirmation dialog will be displayed at the top
- Click 'Apply' to save your profile.

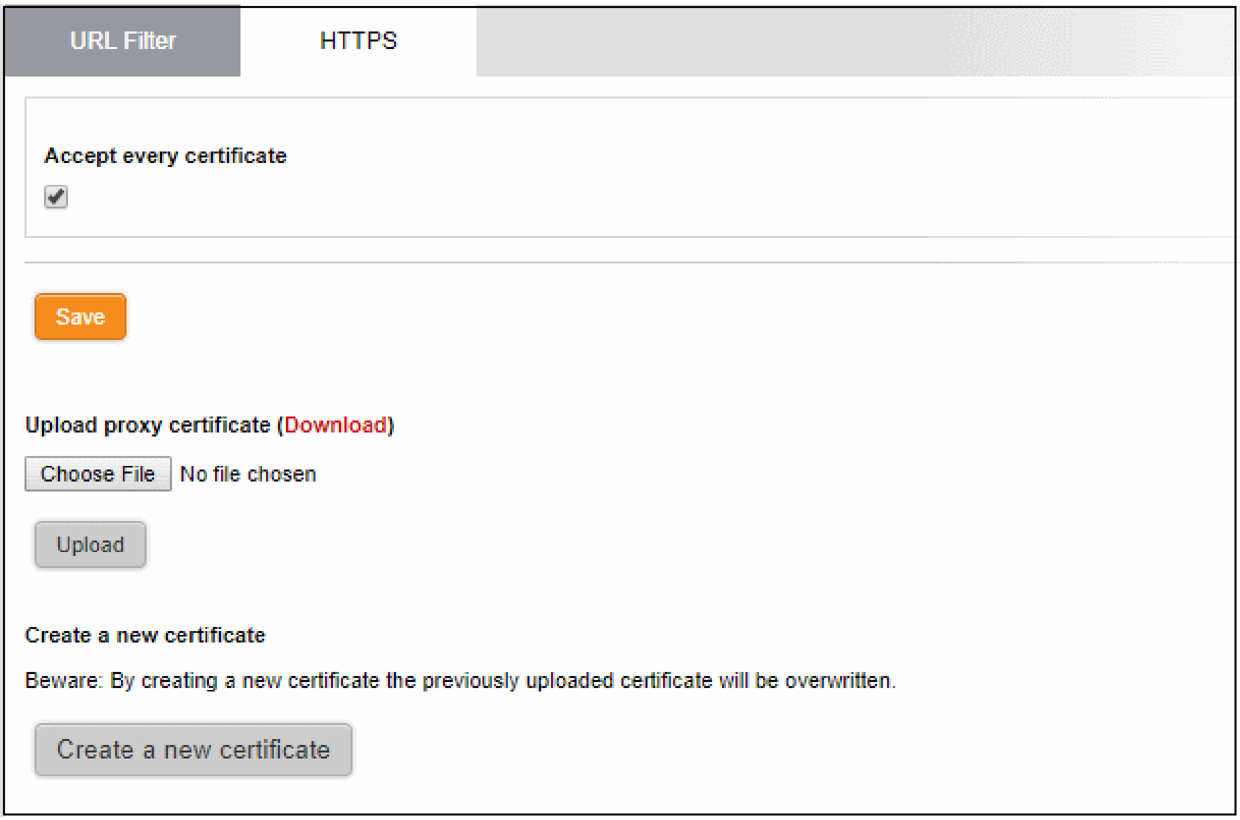
The profile will now be added to the list and will be available in the 'URL Filter' drop-down under 'Web Protection' in the Add/Edit firewall rule interface for configuring the firewall policy.

9.1.2 HTTPS Proxy

- Dome Firewall can provide a HTTPS Proxy service. The service receives requests for encrypted webpages from internal hosts, retrieves and caches the requested resources, applies any access control policies and forwards them to the requesting hosts.
- The Dome Firewall intermediate SSL certificate needs to be installed on endpoints in order to analyze SSL traffic and to authenticate themselves to the HTTPS proxy.
- Also, the administrator can specify website categories and specific URLs or domains to be exempted from the HTTPS proxy service.

To configure the service

- Click 'Proxy' > 'HTTP/HTTPS' from the left hand side navigation
- Click the 'HTTPS' tab.



Accept every certificate

☑

Upload proxy certificate (Download)

No file chosen

Create a new certificate

Beware: By creating a new certificate the previously uploaded certificate will be overwritten.

The interface enables the administrator to specify/create intermediate certificate for authentication.

Note: In order to use HTTPS Proxy service, it is mandatory to install an intermediate certificate both in the DFW virtual appliance and the client computers. The service can be enabled only after deploying the certificate in the

DFW virtual appliance. See **Certificate Settings** for more details.

  - Accept every certificate - If left unselected, the DFW virtual appliance will accept only the valid SSL certificates from the remote servers. If selected, the virtual appliance will accept all the certificates from the remote servers including outdated certificates.
- Click 'Save'. A confirmation dialog will appear.
- Click 'Apply' for your settings to take effect.

Certificate Settings

The Intermediate certificate can be deployed to the HTTPS proxy service in two ways:

- **Using an existing certificate**
- **Creating a new certificate**

In either case, the same certificate needs to be deployed on to the host computers in the network infrastructure that need access to the HTTPS proxy service.

Using an existing certificate

If you already posses an intermediate certificate, you can upload the same to the DFW virtual appliance and install in the client computers.

To upload an existing certificate

Prerequisite: Ensure that the intermediate certificate is locally stored in the computer from which you are accessing the administrative console of the Dome Firewall virtual appliance.

- Click the 'Browse' button under the 'Upload proxy certificate' option, navigate to the location where the certificate is stored and click 'Open'.
- Click 'Upload'

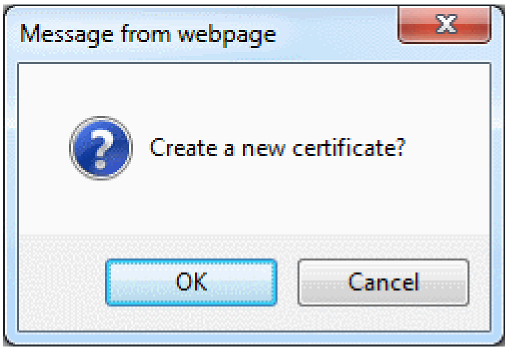
The certificate will be uploaded to the virtual appliance and deployed.

Creating a New Certificate

The Dome Firewall is capable of creating a new self signed intermediate certificate with one year validity and use it for authentication. Once a new certificate is created, the existing certificate, if any, will be replaced by the new certificate. Hence the administrator should download the certificate and install it on to the host computers in the network infrastructure that need to authenticate them to the HTTPS proxy service.

To create a certificate

- Click the 'Create a new certificate' button. A confirmation dialog will be displayed.



Create a new certificate?

- Click 'OK'

A new certificate will be created and deployed in the DFW virtual appliance.

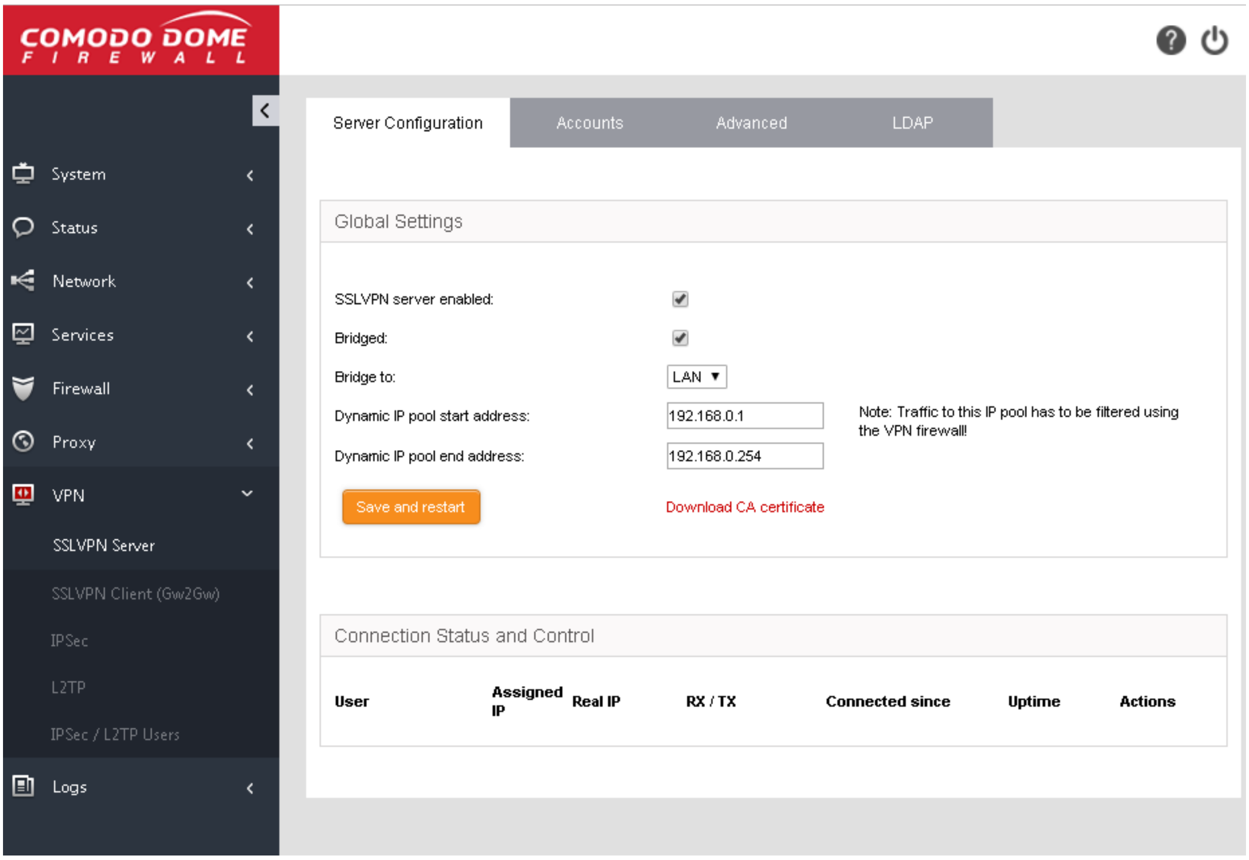
- To download the certificate for transferring to the clients in the network, click the 'Download' link within the parenthesis beside 'Upload proxy certificate'. Transfer the certificate onto the computers in the network and install it on their Intermediate Certificate Store.

10 Configuring Virtual Private Network Settings

The VPN section allows administrators to configure network and client settings in order to connect to Dome Firewall. Other settings that can be configured include user accounts, LDAP integration and more. The firewall rules for VPN traffic are configured in in the Firewall section. See **Configuring Firewall Policy Rules** for more details.

- SSLVPN Server - Allows you to configure client to site VPN connection to DFW. It also allows another DFW account and/or another VPN server configured as clients to connect in a gateway to gateway (Gw2Gw) setup.
- SSLVPN Client - DFW can act as a OpenVPN client to connect to other DFW accounts configured as SSLVPN server through Gw2Gw setup.
- IPsec - Allows you to configure and connect network and clients to DFW.
- L2TP Server - DFW can act as a L2TP server, to connect remote L2TP clients to connect to local network zones.

Clicking the 'VPN' tab on the left opens a menu which allows you to configure VPN services:



Global Settings

SSLVPN server enabled: ☑

Bridged: ☑

Bridge to: LAN ▼

Dynamic IP pool start address: 192.168.0.1

Dynamic IP pool end address: 192.168.0.254

Note: Traffic to this IP pool has to be filtered using the VPN firewall!

Save and restart

Download CA certificate

Connection Status and Control

User	Assigned IP	Real IP	RX / TX	Connected since	Uptime	Actions

The following sections provide detailed descriptions of different VPN services and their configuration:

- **SSLVPN Server**
- **SSLVPN Client**
- **IPsec Configuration**
- **L2TP Server Configuration**

- **IPsec / L2TP Users Configuration**

10.1 SSL VPN Server

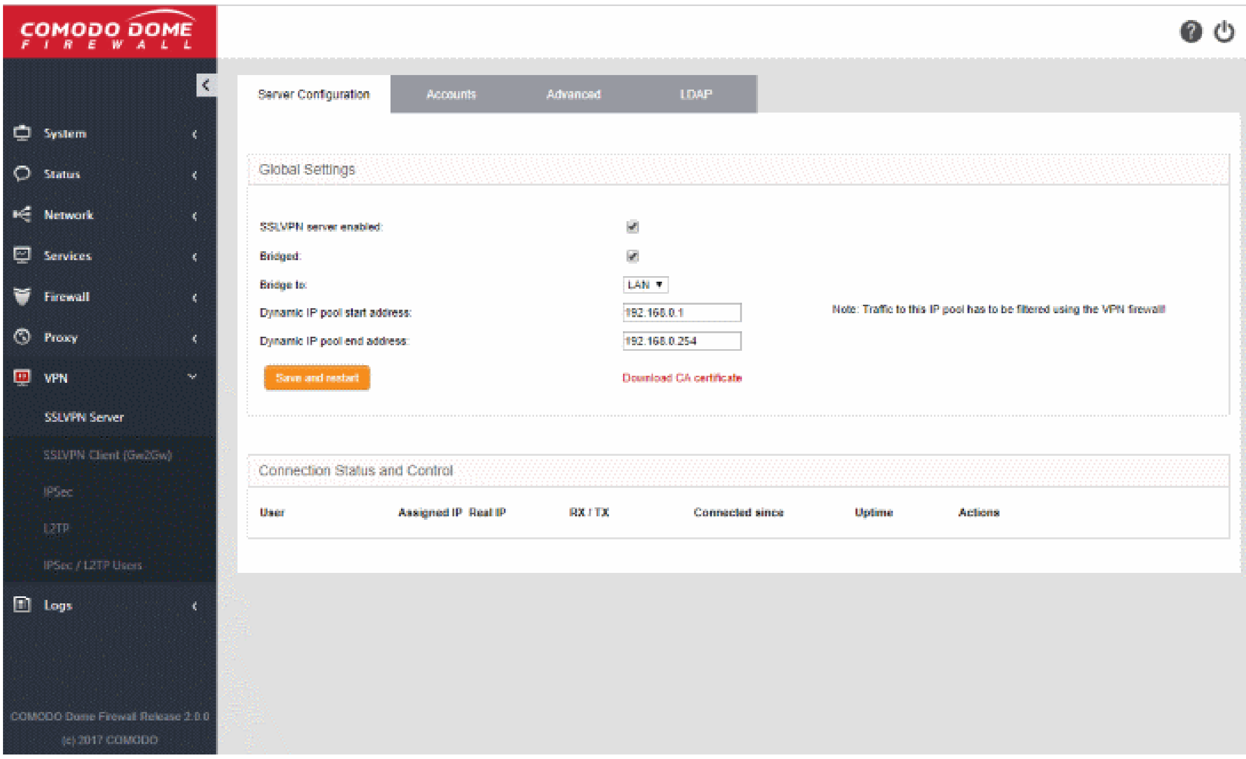
- Click 'VPN' > 'SSLVPN Server' to open this interface

The 'SSL VPN Server' area allows you to enable/disable the service, configure connection settings, manage user accounts and integrate an LDAP server.

- Dome Firewall Virtual Appliance can be configured as an SSL VPN server to allow remote clients to connect to network zones.
- This method is called 'Client-to-site VPN' and can be used to connect individual clients in your network to DFW.
- Once configured, the server allows you to download the authentication certificate and client configuration file for deployment onto remote SSL VPN clients.

The server can also accept connection requests from another DFW account configured as an SSL VPN client in a gateway to gateway connection. This allows remote networks to connect to other network zones.

To open the 'SSL VPN' interface, click 'VPN' > 'SSLVPN Server ' in the left hand menu:



Global Settings

SSLVPN server enabled: ☑

Bridged: ☑

Bridge to: LAN ▼

Dynamic IP pool start address: 192.168.0.1

Dynamic IP pool end address: 192.168.0.254

Note: Traffic to this IP pool has to be filtered using the VPN firewall

Connection Status and Control

User	Assigned IP	Real IP	RX / TX	Connected since	Uptime	Actions

The interface contains four tabs:

- **Server Configuration** - Enable/disable the SSL VPN server and configure general settings like dynamic IP address pool for assigning addresses to clients. The interface also displays a list of active client connections and allows you to download the authentication certificate for distribution to clients. See '**Configuring General SSL VPN Server Settings**' for more details.
- **Accounts** - Add and manage user accounts for clients to connect to the server. See '**Managing SSL VPN Client Accounts**' for more details.
- **Advanced** - Configure port, protocol, global push options and authentication certificate settings. See '**Configuring Advanced SSL VPN Server Settings**' for more details.
- **LDAP** - Configure LDAP server settings for user authentication. See '**Configuring LDAP Server Settings**' for more details.

The last chapter in this section describes how to configure the individual clients in order to connect to DFW. See '**Configuring Clients to Connect to DFW**' for more details.

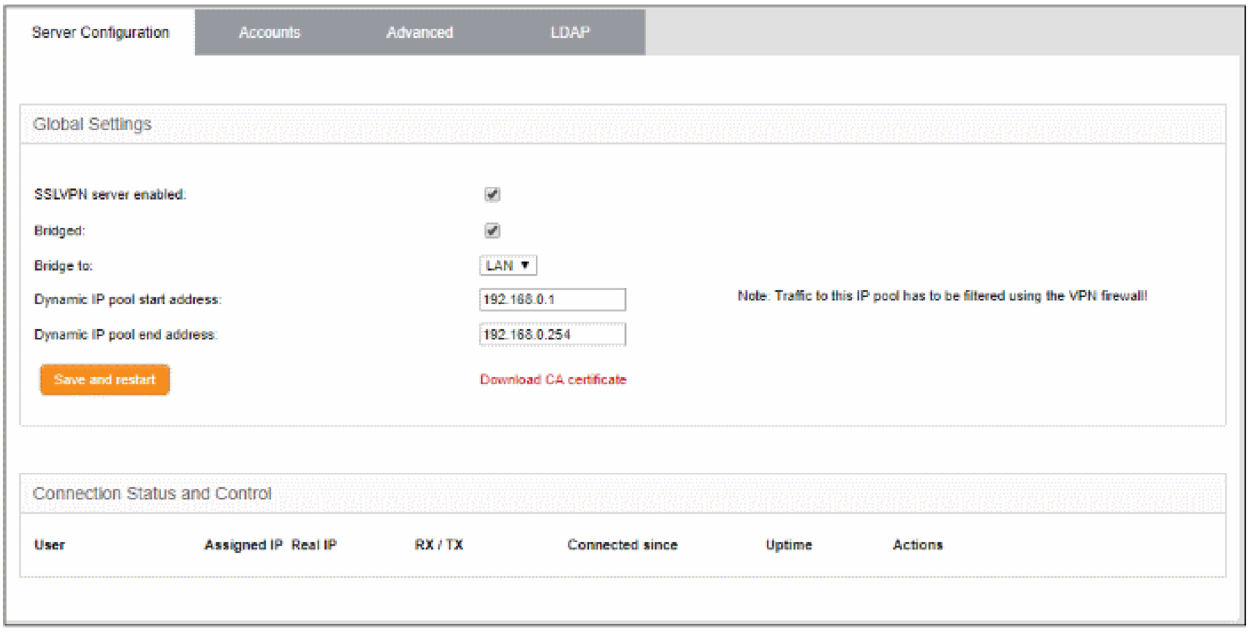
10.1.1 Configuring General SSL VPN Server Settings

This sections allows you to:

- Enable/disable the SSL VPN server
- Configure settings like the local network zone to which the connection should be bridged and settings for dynamically assigning IP addresses to clients connecting to the server.
- Download the server certificate and client configuration file for deployment to clients for authentication and connection to DFW. See '**Configuring Clients to Connect to DFW**' for more details about how to establish connection between individual clients and Dome Firewall.

To configure general settings for SSL VPN Server

- Click 'VPN' > 'SSLVPN Server' on the left-hand menu
- Click the 'Server Configuration' tab:



Global Settings

SSLVPN server enabled: ☑

Bridged: ☑

Bridge to: LAN ▼

Dynamic IP pool start address: 192.168.0.1

Note: Traffic to this IP pool has to be filtered using the VPN firewall!

Dynamic IP pool end address: 192.168.0.254

Connection Status and Control

User	Assigned IP	Real IP	RX / TX	Connected since	Uptime	Actions

- SSLVPN server enabled - Enable or disable the SSL VPN server
- Bridged - Enable or disable server bridge mode.
- Bridge to - Choose the local network zone to which the server should be bridged. This option will only appear if bridge mode is enabled.
- Dynamic IP pool start/end addresses - Enter the first and last addresses of the pool from which IP addresses are dynamically assigned to clients connecting to the server. All traffic from these addresses will pass through the firewall, if enabled. See '**Managing Firewall Policy Rules**' for more details.

- Click 'Save and Restart' to apply your changes.
- Click 'Download CA certificate' to download the server certificate for export to the clients. The certificate can also be downloaded from the '**Accounts**' interface. For more details on certificate settings, see **Configuring Advanced SSL VPN Server Settings > Authentication Settings**.

The lower pane of the interface displays a list of active SSL VPN connections to the server with their connection statistics. Admins can terminate unwanted VPN connections should they wish.

SSL VPN Server Connection status and control table - Column Descriptions	
Column	**Description**
User	The name of the user who logged-in
Assigned IP	The IP address dynamically assigned to the client from the server during the current session
Real IP	The actual, externally facing, IP address of the client
RX / TX	Amount of data sent and received during the current session
Connected since	The date and time that the session began
Uptime	The length of time that the connection has been active
Actions	Controls for terminating the session

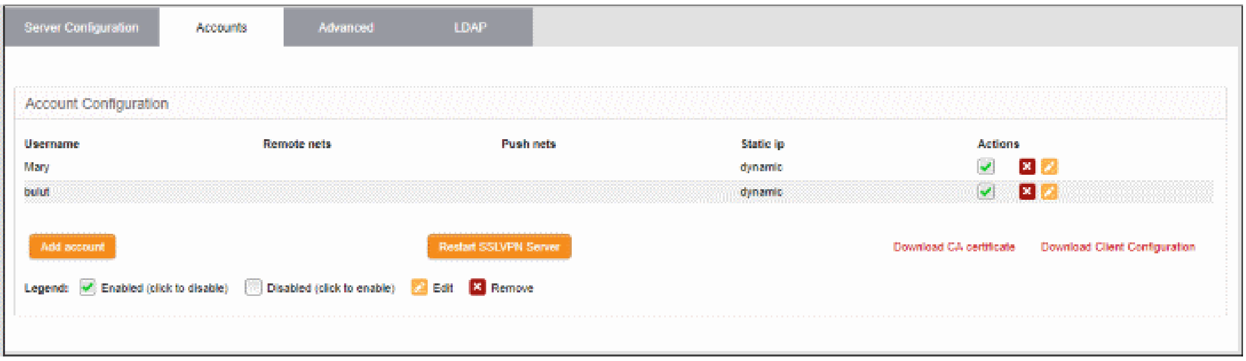
See '**Configuring Clients to Connect to DFW**' (later in this section) for more details on how to connect individual clients to DFW.

10.1.2 Managing SSL VPN Client Accounts

The 'Accounts' interface lets you add and manage user accounts for external clients to connect to the VPN server. Please note that user details should be configured before their endpoints are configured to connect to DFW. See '**Configuring Clients to Connect to DFW**' for more details on how to connect clients to DFW.

To manage user accounts

- Click 'VPN' > 'SSLVPN Server' in the left-hand navigation
- Click the 'Accounts' tab.



Account Configuration

Username	Remote nets	Push nets	Static ip	Actions
Mary			dynamic	✓ ☒ ✎
bulut			dynamic	✓ ☒ ✎

Legend: ✓ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

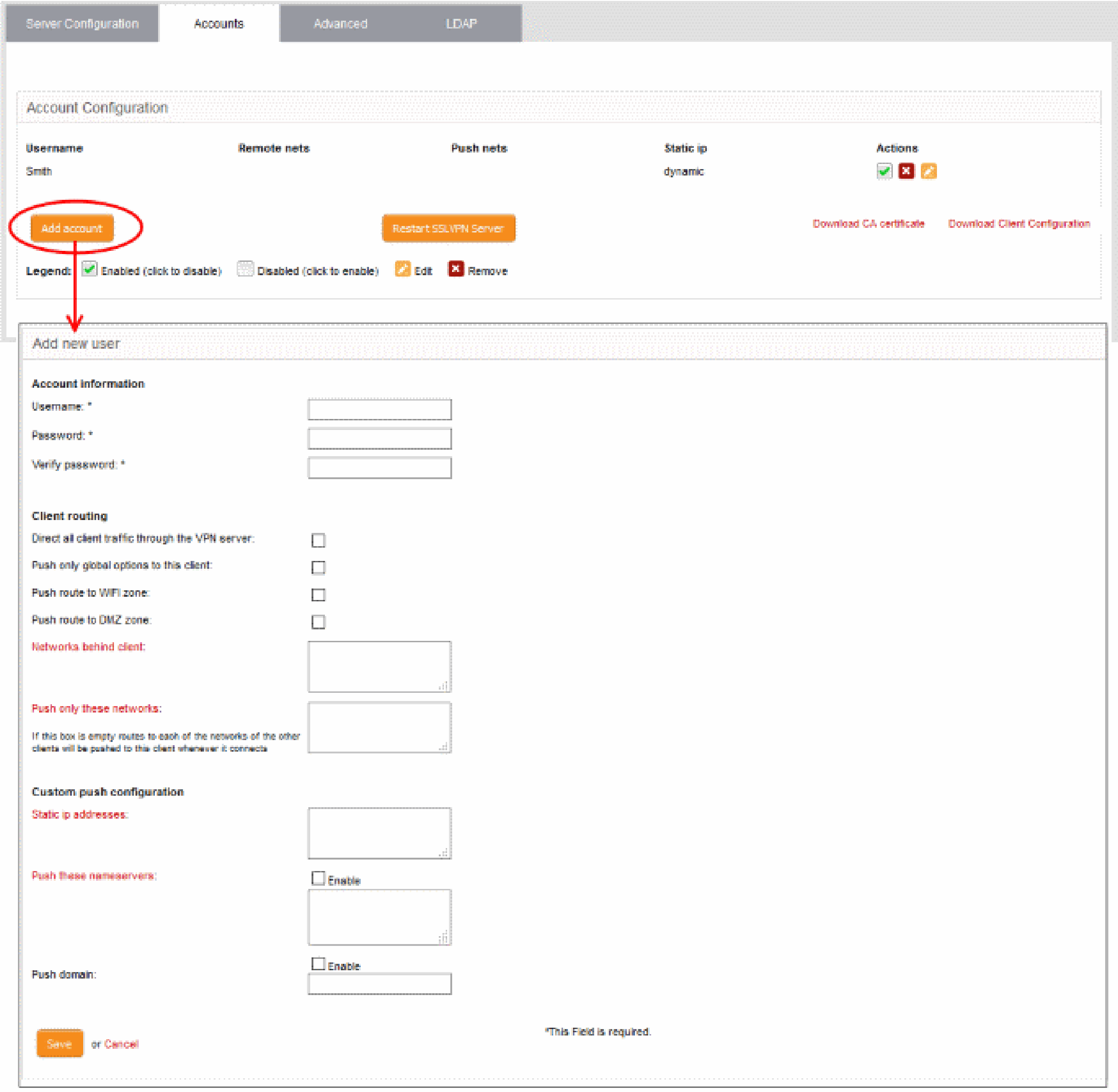
A list of existing user accounts will be displayed.

SSL VPN Server Account Configuration table - Column Descriptions	
Column	**Description**
Username	The user account authorized to log-in to the server via the external client.
Remote nets	The network subnet address of the VPN gateway server for the client to connect to VPN.
Push nets	The network(s) whose routes are pushed to the client, once it is connected
Static ip	If a static IP address is assigned to the remote client, the IP address will be displayed.

Actions	Displays controls for enabling, editing and deleting the account. ✓ - Enable or disable access for the account. ✎ - Edit account configuration. The interface for editing an account is similar to that for adding an account. See **adding a new user account** for more details. ☒ - Removes the entry.

To add a new user account

- Click the 'Add account' button. The 'Add new user' pane will open:



Account Configuration

Username	Remote nets	Push nets	Static ip	Actions
Smith			dynamic	✓ ☒ ✎

Legend: ✓ Enabled (click to disable) ▨ Disabled (click to enable) ✎ Edit ☒ Remove

Add new user

Account information

Username: *

Password: *

Verify password: *

Client routing

Direct all client traffic through the VPN server: □

Push only global options to this client: □

Push route to WIFI zone: □

Push route to DMZ zone: □

Networks behind client:

Push only these networks:

If this box is empty routes to each of the networks of the other clients will be pushed to this client whenever it connects

Custom push configuration

Static ip addresses:

Push these nameservers: □ Enable

Push domain: □ Enable

*This Field is required.

Account information

Specify the username and password of the account. These credentials are needed to authenticate the SSL VPN client to the server.

- Username - Enter a username for the account
- Password - Enter a password for the account
- Verify password - Re-enter the password for confirmation

Client routing

Configure traffic routing to the client.

- Direct all client traffic through the VPN server - Select if you want all incoming and outgoing client traffic to pass through the VPN server.
- Push only global options to this client - The server will only provide network routes, name servers and domains which have been added to 'Global Push Options' in 'Advanced Settings'. See '**Configuring Advanced SSL VPN Server Settings**' for more details.
- Push route to WIFI zone - Instructs the server to communicate the route to the internal Wi-Fi zone, so that the client can connect to hosts in the Wi-Fi zone in the local network infrastructure.
- Push route to DMZ zone - Instructs the server to push the route to the internal DMZ zone, so that the client can connect to the hosts in the DMZ zone in the local network infrastructure.
- Networks behind client - Enter the network subnet address of the VPN gateway server for the client to connect to VPN.
- Push only these networks - Allows you to push specific network routes to the client. Leave this blank if you wish to push all available routes.

Custom push configuration

- Static IP addresses - If you wish to assign static IP addresses for clients using this account, enter the IP addresses in CIDR format. To avoid IP address clashes, we advise you specify static IP addresses outside the dynamic IP address pool specified in the **Server Configuration** tab.
- Push these nameservers - If you want clients to use specific name servers for DNS resolution, enter the IP addresses of the name servers in the text field.
- Push domain - If you want clients on this account to use a specific search domain then enter it here. The search domain is used to identify servers and resources in the VPN network.

- Click 'Save'. The SSL VPN server must be restarted for the account to become active.
- Click 'Restart SSL VPN server' to instantly restart the server.

You can download the server certificate and the SSL VPN client configuration file from the 'Accounts' interface. The certificates can be installed on remote workstations to enable clients to connect. The server certificate type for authentication can be configured in the '**Advanced**' tab > **Authentication Settings**.

- Click the 'Download CA certificate' link to download the server certificate.
- Click the 'Download Client Configuration' link to download the SSL VPN client configuration file in .ovpn format.

During the configuration of the client to connect to DFW, the username and password specified for the account should be provided. By default, only one client is allowed to connect to the server per account. Select 'Allow multiple connections from one account' to enable several clients at different locations to share a single account (under the '**Advanced**' tab).

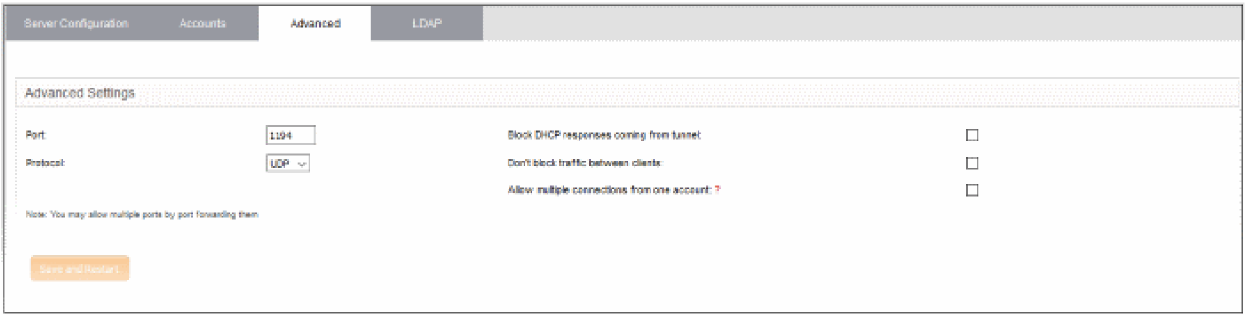
See '**Configuring Clients to Connect to DFW**' for more details about how to connect individual clients to DFW.

10.1.3 Configuring Advanced SSL VPN Server Settings

The 'Advanced' tab lets you configure the connection port and protocol for the VPN server, global push options and authentication settings.

To configure the advanced settings for the SSL VPN server

- Click 'VPN' > 'SSLVPN Server' in the left-hand menu
- Click the 'Advanced' tab.



Advanced Settings

Port: 1194

Protocol: UDP

Block DHCP responses coming from tunnel: □

Don't block traffic between clients: □

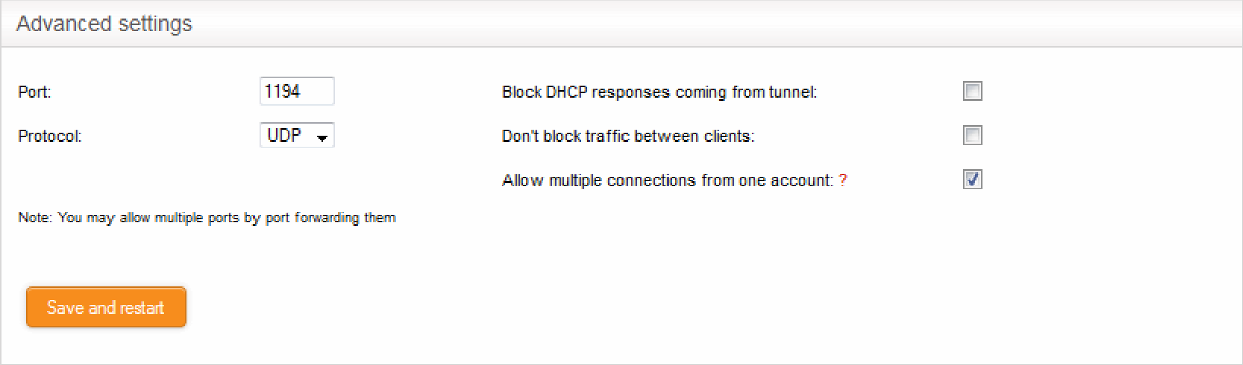
Allow multiple connections from one account: ? □

Note: You may allow multiple ports by port forwarding them

The 'Advanced' interface contains three areas:

- **Advanced Settings**
- **Global Push Options**
- **Authentication Settings**

Advanced Settings


Advanced settings

Port: 1194

Protocol: UDP

Block DHCP responses coming from tunnel: □

Don't block traffic between clients: □

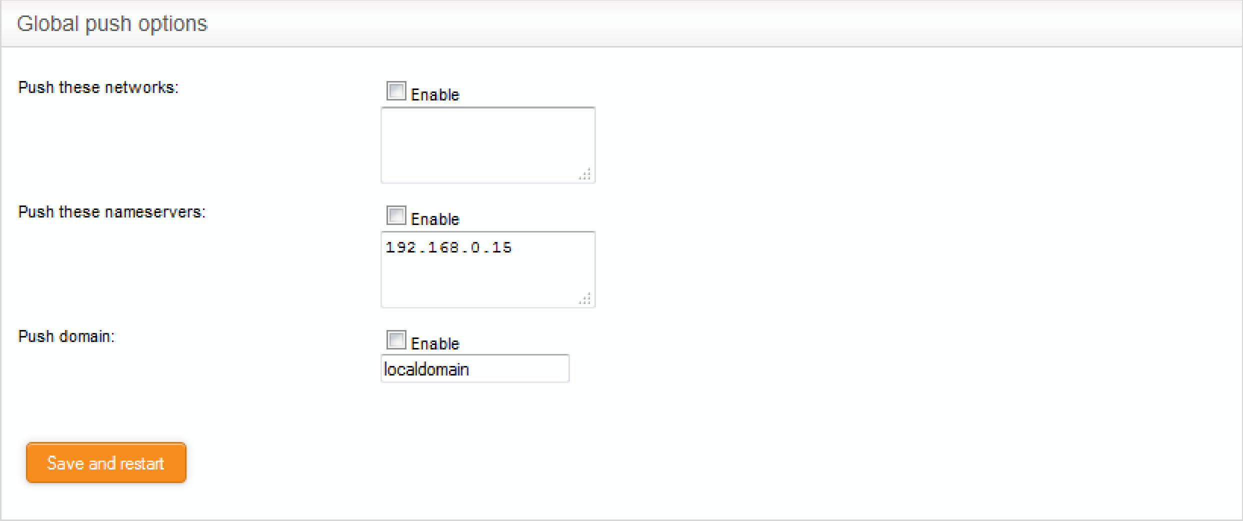
Allow multiple connections from one account: ? ☑

Note: You may allow multiple ports by port forwarding them

- Port - Specify the port for listening for VPN client requests. (***Defaul = 1194***). Admins can also create port forwarding rules under **Firewall > SNAT**, to allow multiple ports to listen for requests and forward them to the default port.
- Protocol - Choose the protocol to be used for VPN connections. (***Defaul = UDP***)
- Block DHCP responses coming from tunnel - Select if you wish to block DHCP responses from the network at the other side of the VPN tunnel that conflict with the local DHCP server.
- Don't block traffic between clients - By default, the VPN server does not allow traffic between the VPN clients connected to it. Enable this option if you wish to allow data transfer among clients.
- Allow multiple connections from one account - By default, only one client can connect to the VPN server for a single user account. Enable this option if you want to allow several clients at different locations to connect to the server using the same account. However, if several clients are using a single account, the **firewall rules** will not be applied.

- Click 'Save and restart'. The VPN server will be restarted for your configuration changes to take effect.

Global Push Options



Global push options

Push these networks: □ Enable

Push these nameservers: □ Enable

192.168.0.15

Push domain: □ Enable

localdomain

  - Push these networks - If you wish the routes to specific networks are to be pushed to all the clients that connect to the VPN server. Select the 'Enable' checkbox and enter the network addresses/subnet masks in the text field.
  - Push these nameservers - If you wish the clients to use specific name servers for DNS resolution, select the 'Enable' checkbox and enter the IP addresses of the name servers in the text box.
  - Push domain - If you wish to specify a specific search domain for all the clients, to identify the servers and network resources in the VPN network, select the 'Enable' checkbox and enter the domain name in the text box.
- Click 'Save and restart'. The VPN server will be restarted for your configuration changes to take effect.

Authentication Settings

The SSL VPN server allows three types of authentication for the clients to authenticate themselves to the server.

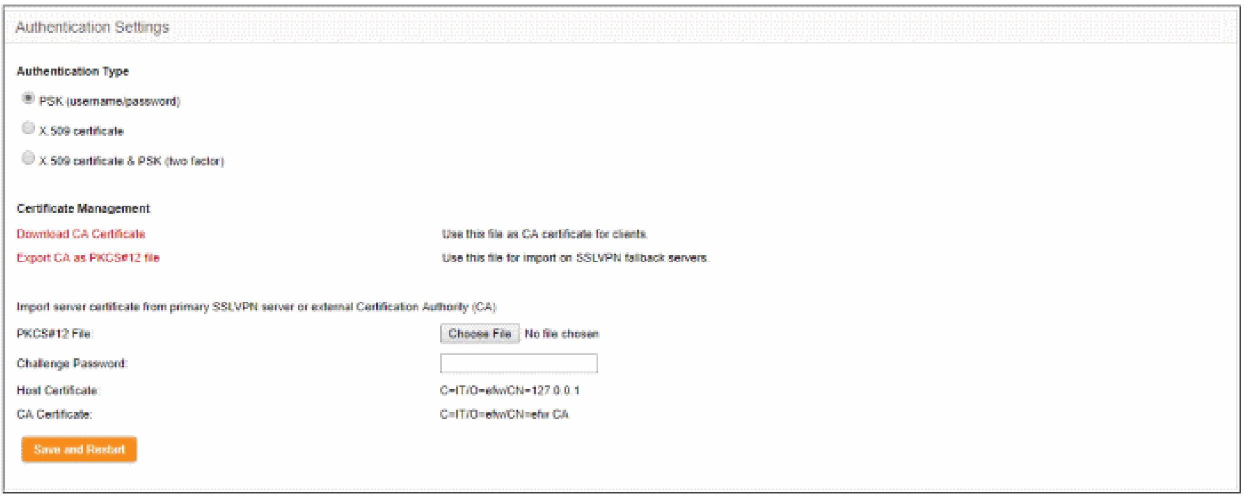
- **Pre-Shared Key (PSK)** (***Default***)
- **X.509 certificate**
- **X.509 certificate and PSK (two factor)**

PSK (username/password)

The PSK authentication type requires the CA public certificate to be installed onto the clients and entering username and password of the account created for the client under 'Accounts' tab, for the client to authenticate itself to the server.

On selecting the PSK type, the administrator can download the public certificate generated by the VPN server for deployment onto the clients. The interface also allows the administrator to export the certificate for deployment onto other SSL VPN server configured as fall back server and import the certificate from primary SSL VPN server, if this DFW virtual appliance is configured as fallback server.

- To select the PSK authentication type, select the PSK radio button.



Authentication Settings

Authentication Type

● PSK (username/password)

○ X.509 certificate

○ X.509 certificate & PSK (two factor)

Certificate Management

Download CA Certificate	Use this file as CA certificate for clients.
Export CA as PKCS#12 file	Use this file for import on SSLVPN fallback servers.

Import server certificate from primary SSLVPN server or external Certification Authority (CA)

PKCS#12 File:	Choose File No file chosen
Challenge Password:	
Host Certificate:	C=IT/O=efw/CN=127.0.0.1
CA Certificate:	C=IT/O=efw/CN=efw CA

Certificate Management

- To download the public certificate in .cer format for deployment on to the clients, click 'Download CA certificate' and save the certificate.
- To export the certificate as a PKCS#12 certificate in .p12 format, click 'Export CA as PKCS#12 file' and save the file. This file can be transferred and imported on to other SSL VPN virtual appliance configured as fallback server.

Importing the certificate

If the SSL VPN server is configured as fallback server for a different primary SSL VPN server, the administrator needs to import the public certificate generated by/issued for the primary server.

Prerequisite - The certificate needs to be exported as a PKCS#12 certificate from the server or to be downloaded from the CA that has issued the certificate and stored locally in the computer from which the DFW virtual appliance administrative console is accessed.

To import the certificate

- Click 'Browse' beside the PKCS#12 file text box and navigate to the location of the certificate stored in the local computer or the network and click Open.
- Enter the challenge password to access the certificate in the 'Challenge password' text box.
- Click 'Save and restart'.

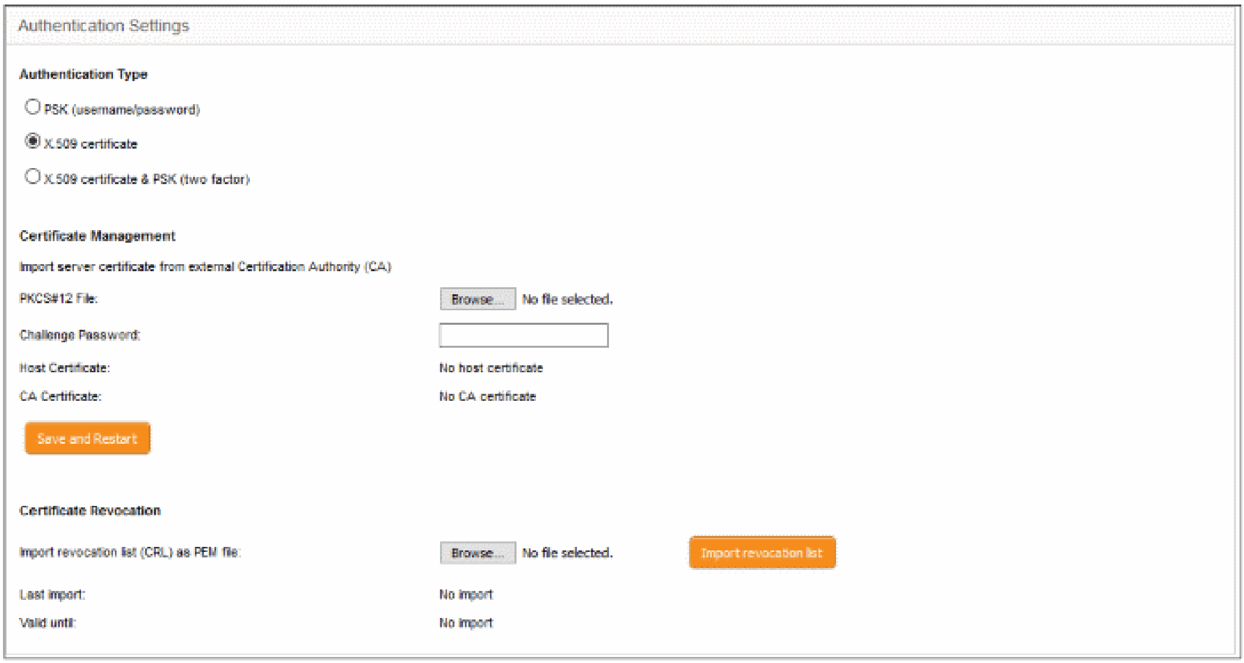
The certificate will be imported and the VPN server will be restarted for your configuration to take effect.

X.509 certificate

Comodo Dome Firewall allows the deployment of server certificate and client certificates obtained from an external CA. The X.509 authentication type requires the administrator to obtain:

- A Server certificate with the fields C = IT, O = efw and CN = 127.0.01 from an external CA for uploading to the SSL VPN server configured in the DFW virtual appliance
- A Client certificate for each client with the Common Name field = The 'username' of the client account configured under the 'Accounts' tab, for installation at the SSL VPN client.

- To select the X.509 authentication type, select the X.509 radio button.



Authentication Settings

Authentication Type

○ PSK (username/password)

● X.509 certificate

○ X.509 certificate & PSK (two factor)

Certificate Management

Import server certificate from external Certification Authority (CA)

PKCS#12 File: Browse... No file selected.

Challenge Password:

Host Certificate: No host certificate

CA Certificate: No CA certificate

Certificate Revocation

Import revocation list (CRL) as PEM file: Browse... No file selected.

Last import: No import

Valid until: No import

Certificate Management

Prerequisite - The certificate needs to be downloaded as a X.509 certificate from from the CA that has issued the certificate and stored locally in the computer from which the DFW virtual appliance administrative console is accessed.

- To import the server certificate obtained from an external CA click 'Browse', navigate to the location on your computer where the certificate is stored in X.509 format and click Open, enter the password entered for storing the private key of the certificate in the challenge password field and click 'Save and restart'. The certificate will be installed automatically and the VPN Server will restart for the installation to take effect.
- Certificate Revocation - The administrator can specify a certificate revocation list to confirm that the imported certificate is valid.

X.509 certificate and PSK (two factor)

The X.509 and PSK authentication type requires both the server and client certificates obtained from an external CA to be installed on the server and on the clients respectively and entering the username and password of the account created for the clients under 'Accounts' tab, for the client to authenticate itself to the server.

Refer to the explanations under **PSK (Username/Password)** and **X.509 certificate** above.

10.1.4 Configuring LDAP Server Settings

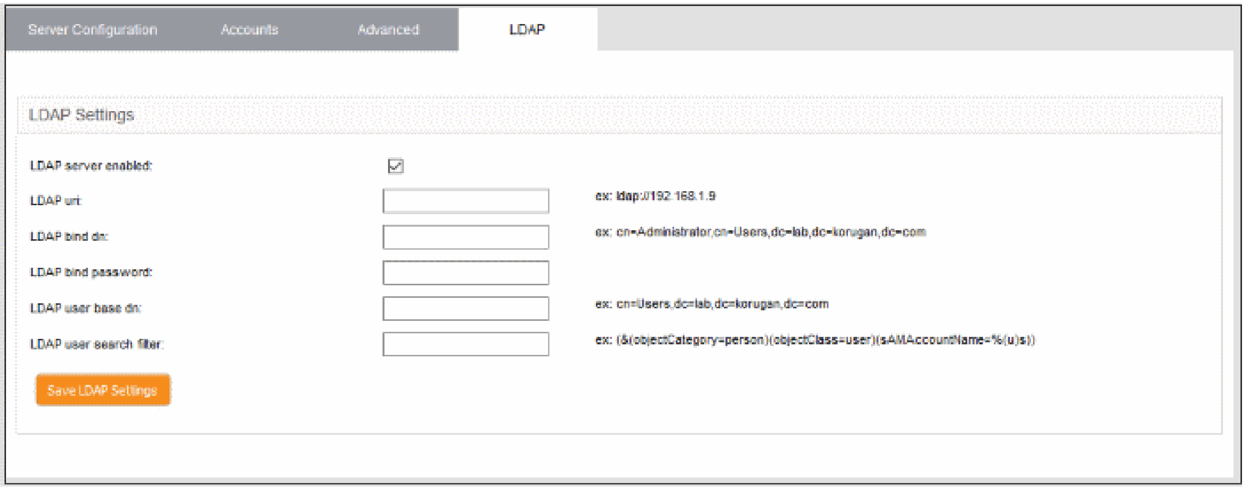
There are two ways you can configure Dome Firewall to authenticate users:

- Add users in the DFW admin console itself - Click 'VPN' > 'SSLVPN Server' on the left hand menu and then open the 'Accounts' screen. See '**Managing SSL VPN Client Accounts**' for more details.
- Configure an external LDAP server for user authentication.

The following tutorial explains how to configure an external LDAP server for user authentication.

To configure LDAP server for user authentication

- Click 'VPN' > 'SSLVPN Server' on the left menu
- Click the 'LDAP' tab.



LDAP Settings

LDAP server enabled:	☑	
LDAP uri:		ex: ldap://192.168.1.9
LDAP bind dn:		ex: cn=Administrator,cn=Users,dc=lab,dc=korugan,dc=com
LDAP bind password:		
LDAP user base dn:		ex: cn=Users,dc=lab,dc=korugan,dc=com
LDAP user search filter:		ex: (&(objectCategory=person)(objectClass=user)(sAMAccountName=%(u)s))

- LDAP server enabled - Enable or disable user authentication via LDAP
- LDAP uri - The URI of your LDAP server.
- LDAP bind dn - Bind DN of the LDAP server
- LDAP bind password - Password associated with the bind DN
- LDAP user base dn - User base DN of the LDAP server
- LDAP user search filter - Filter by user or group

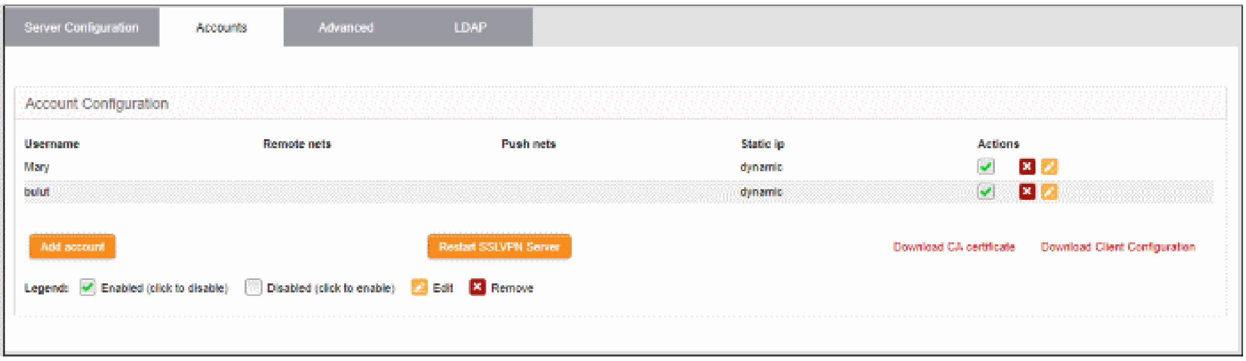
- Click 'Save LDAP Settings' for your changes to take effect.

10.1.5 Configuring Clients to Connect to Dome Firewall

This section explains how to establish a 'Client-to-site VPN' connection to DFW after configuring an SSL VPN server'. Help to configure an SSL VPN server is covered in '**Configuring General SSL VPN Server Settings**'. Help to add users is covered in '**Managing SSL VPN Client Accounts**' and '**Configuring LDAP Server Settings**'.

To configure a client to connect to Dome Firewall

- Click 'VPN' on the left then 'SSLVPN Server'
- Click the 'Accounts' tab:



Account Configuration

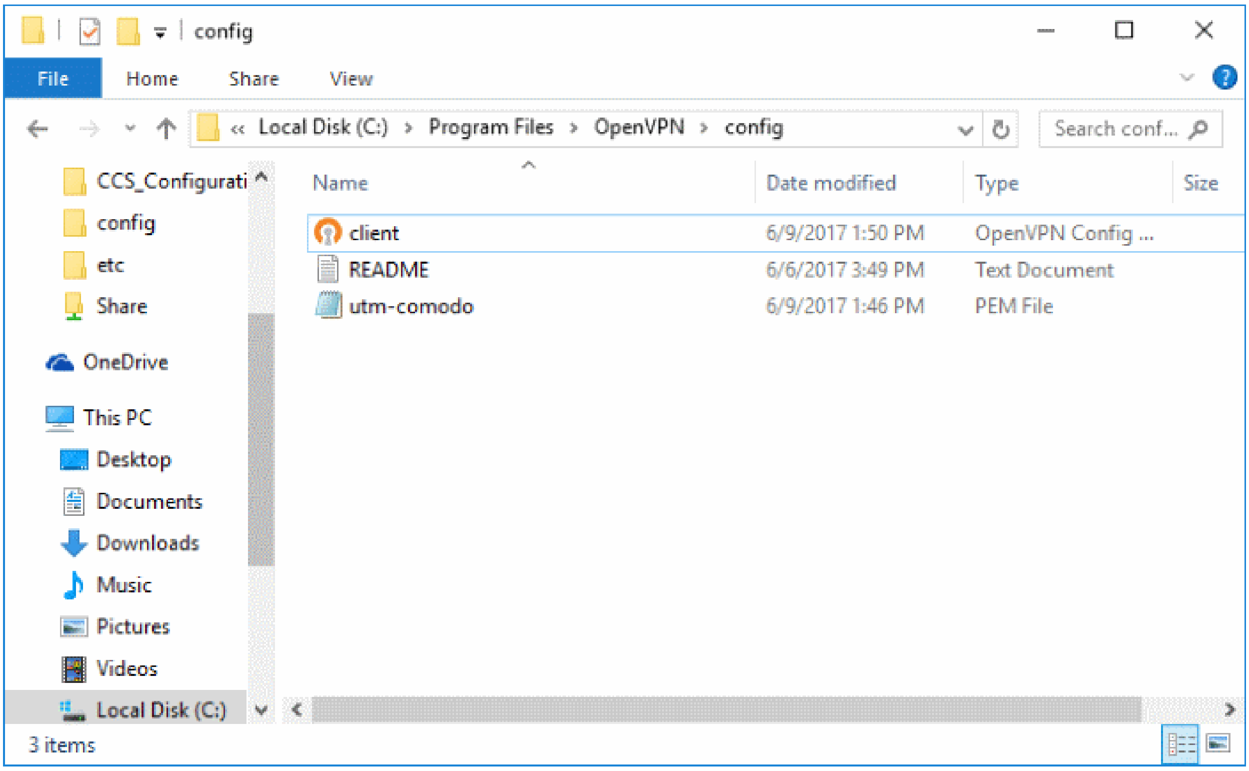
Username	Remote nets	Push nets	Static ip	Actions
Mary			dynamic	✓ ☒ ✎
bulut			dynamic	✓ ☒ ✎

Legend: ✓ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Users added via DFW will be displayed.

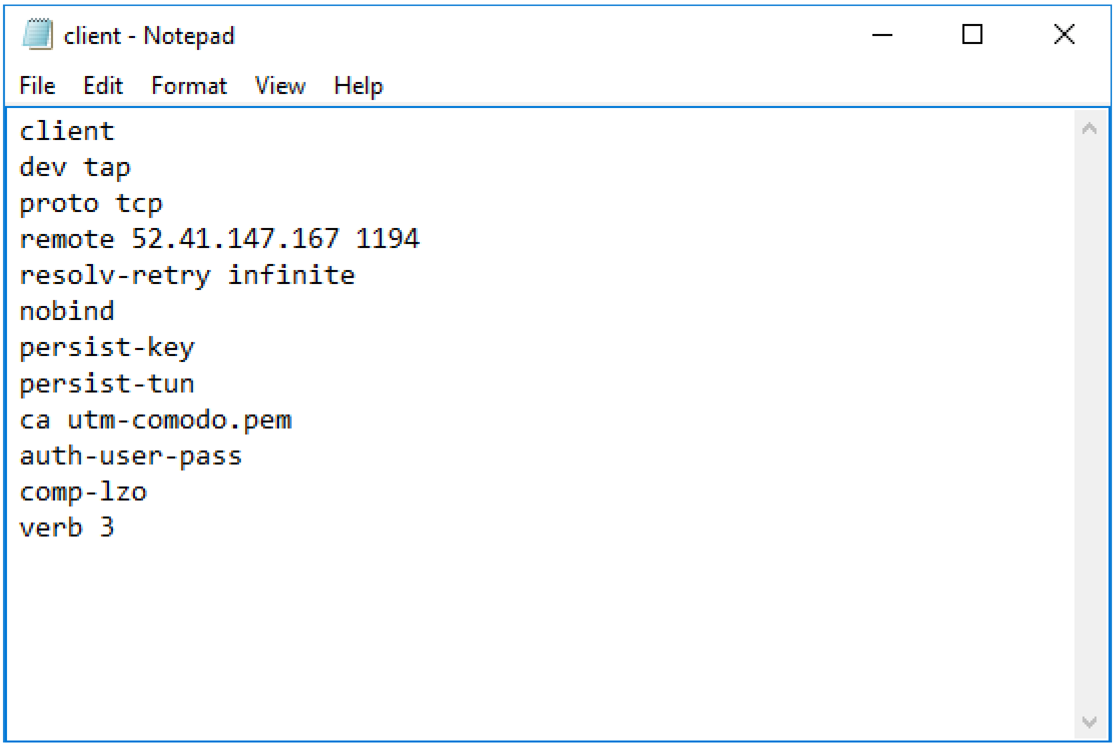
- Click the 'Download CA certificate' link to download the server certificate.
- Click the 'Download Client Configuration' link to download the SSL VPN client configuration file in .ovpn format.
- Download and install OpenVPN GUI client on computers that you want to connect to DFW. You can download the OpenVPN GUI client from **https://openvpn.net/index.php/open-source/downloads.html**
- After installing the OpenVPN GUI client on the endpoint, you need to paste the downloaded CA certificate

and configuration file into the OPVN config file. The configuration file will be available in Program Files > OpenVPN > config



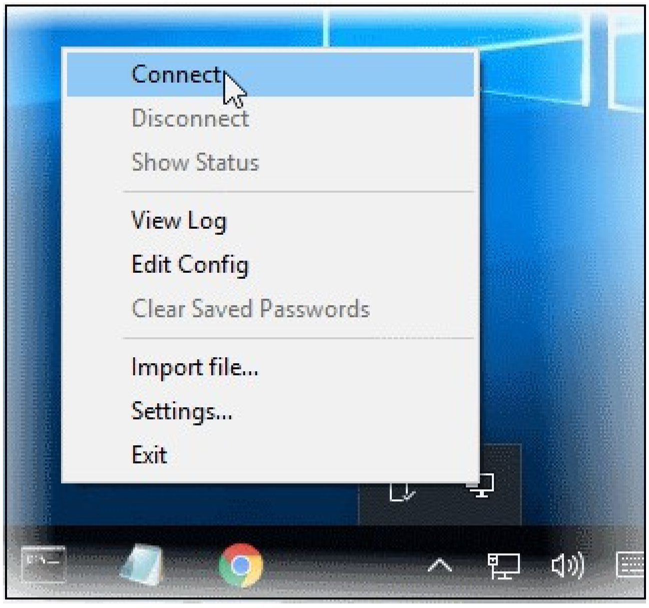
Name	Date modified	Type	Size
client	6/9/2017 1:50 PM	OpenVPN Config ...	
README	6/6/2017 3:49 PM	Text Document	
utm-comodo	6/9/2017 1:46 PM	PEM File	

- Open the configuration file and make sure the parameters are as shown below:

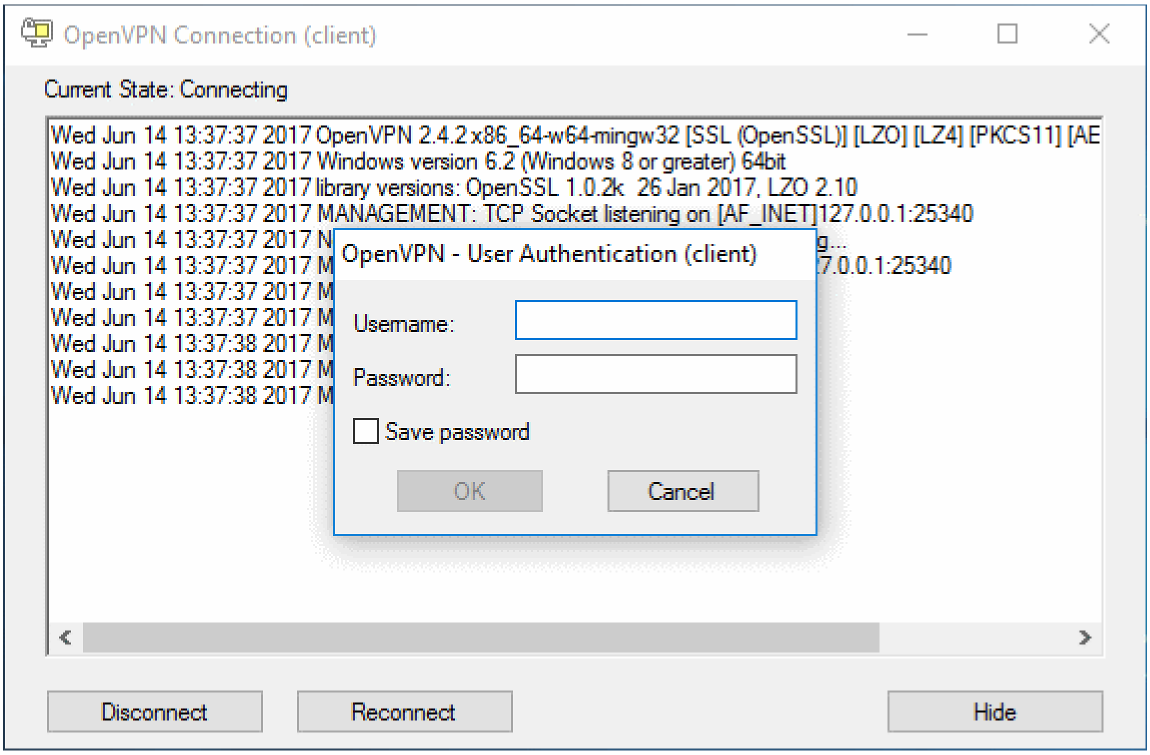


```
client
dev tap
proto tcp
remote 52.41.147.167 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca utm-comodo.pem
auth-user-pass
comp-lzo
verb 3
```

- In the third line, the protocol beside 'proto' depends on the protocol defined in '**Advanced**' section.
- In the fourth line, the IP beside 'remote' should be the IP of your DFW account and the port as configured in '**Advanced**' section. For example, if the Firewall URL is 52.41.147.187, then add '52.41.147.187' in the place of 'remote_ip'.
- To connect the client to DFW, right-click the OpenVPN GUI icon in the task bar then 'Connect'



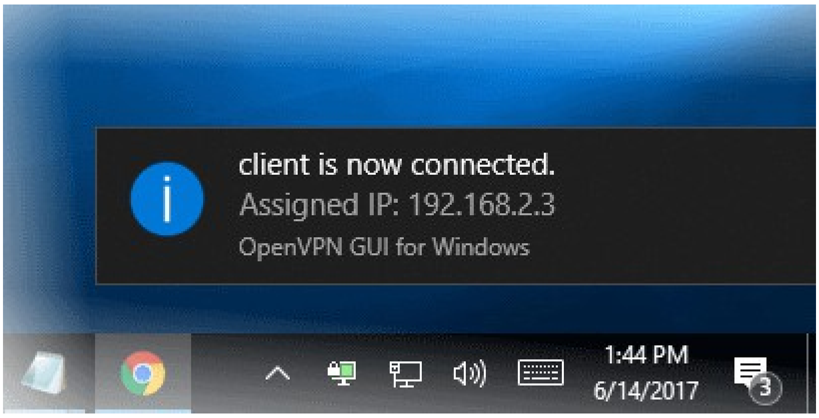
The connection process will start. You will need to provide user authentication credentials:


OpenVPN Connection (client)
OpenVPN - User Authentication (client)
Username:
Password:
□ Save password
OK
Cancel
Disconnect
Reconnect
Hide

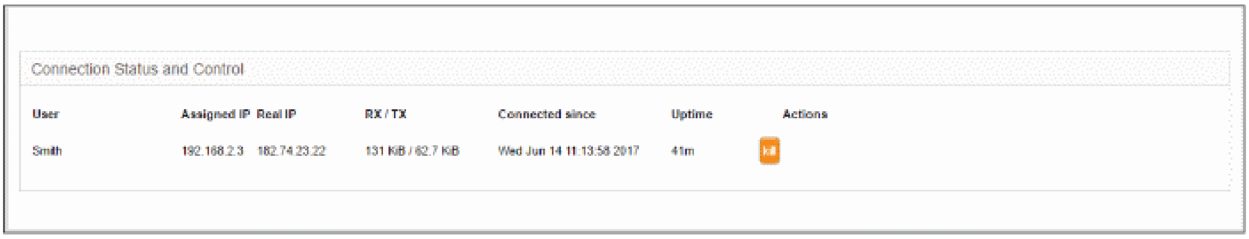
Current State: Connecting

```
Wed Jun 14 13:37:37 2017 OpenVPN 2.4.2 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11] [AE
Wed Jun 14 13:37:37 2017 Windows version 6.2 (Windows 8 or greater) 64bit
Wed Jun 14 13:37:37 2017 library versions: OpenSSL 1.0.2k  26 Jan 2017, LZO 2.10
Wed Jun 14 13:37:37 2017 MANAGEMENT: TCP Socket listening on [AF_INET]127.0.0.1:25340
Wed Jun 14 13:37:37 2017 N                                               g...
Wed Jun 14 13:37:37 2017 M                                               7.0.0.1:25340
Wed Jun 14 13:37:37 2017 M
Wed Jun 14 13:37:37 2017 M
Wed Jun 14 13:37:38 2017 M
Wed Jun 14 13:37:38 2017 M
Wed Jun 14 13:37:38 2017 M
```

- Complete the 'Username' and 'Password' fields and click 'OK'.
- After successful authentication, the client will be connected to DFW and a message will be displayed:


client is now connected.
Assigned IP: 192.168.2.3
OpenVPN GUI for Windows

The connection status of the user can also be viewed in the DFW admin console under 'Status' > 'SSLVPN Connections' and under 'VPN' > 'SSLVPN Server'.


Connection Status and Control

User	Assigned IP	Real IP	RX / TX	Connected since	Uptime	Actions
Smith	192.168.2.3	182.74.23.22	131 KiB / 62.7 KiB	Wed Jun 14 11:13:58 2017	41m	kill

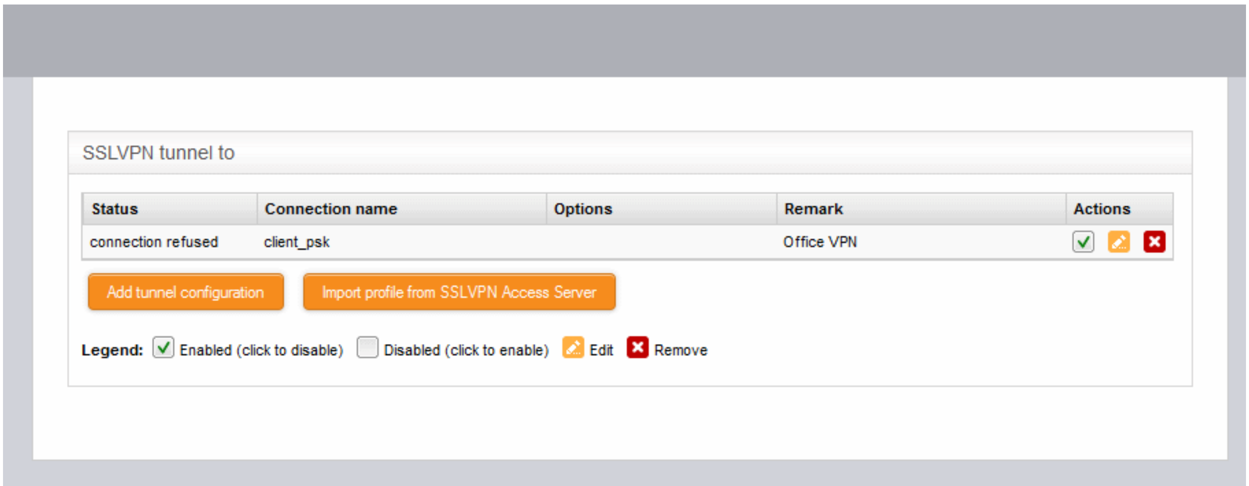
See '**IPsec Configuration**' for details about connecting networks to DFW.

10.2 SSLVPN Client

The firewall can be configured to create secure tunnels to other SSL VPN servers and/or other DFW accounts to serve as a gateway for the local network infrastructure. Each tunnel is constructed as a client to connect to different servers through Gw2Gw setup.

The 'SSLVPN Client' interface displays a list of VPN client connections and allows admins to create new tunnels.

- Click 'VPN' > 'SSLVPN Client (Gw2Gw)' in the left hand menu to open the 'SSLVPN Client' interface.


SSLVPN tunnel to

Status	Connection name	Options	Remark	Actions
connection refused	client_psk		Office VPN	☑ ✎ ☒

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

SSL VPN Clients table - Column Descriptions	
Column	**Description**
Status	Connection status of the tunnel. The possible values are:

	• Established - The connection to the external VPN server is enabled and live • Connecting - The connection is being established • Closed - The connection is terminated
Connection name	The label used to identify the connection.
Options	Additional connection options, if any, specified during creation of the tunnel.
Remark	A short description of the tunnel.
Actions	Controls to enable, edit or and delete the tunnel. ☑ - Allows administrators to switch the connection between enabled and disabled. ✎ - Edit the tunnel configuration. The pane for editing a tunnel is similar to the pane for adding a new tunnel. See '**Creating a new tunnel configuration'** for more details. ☒ - Removes the tunnel configuration.

New tunnel configurations, and hence connections to different OpenVPN servers can be configure in two ways:

- **Creating a new tunnel configuration**
- **Importing the configuration from the SSL VPN server**

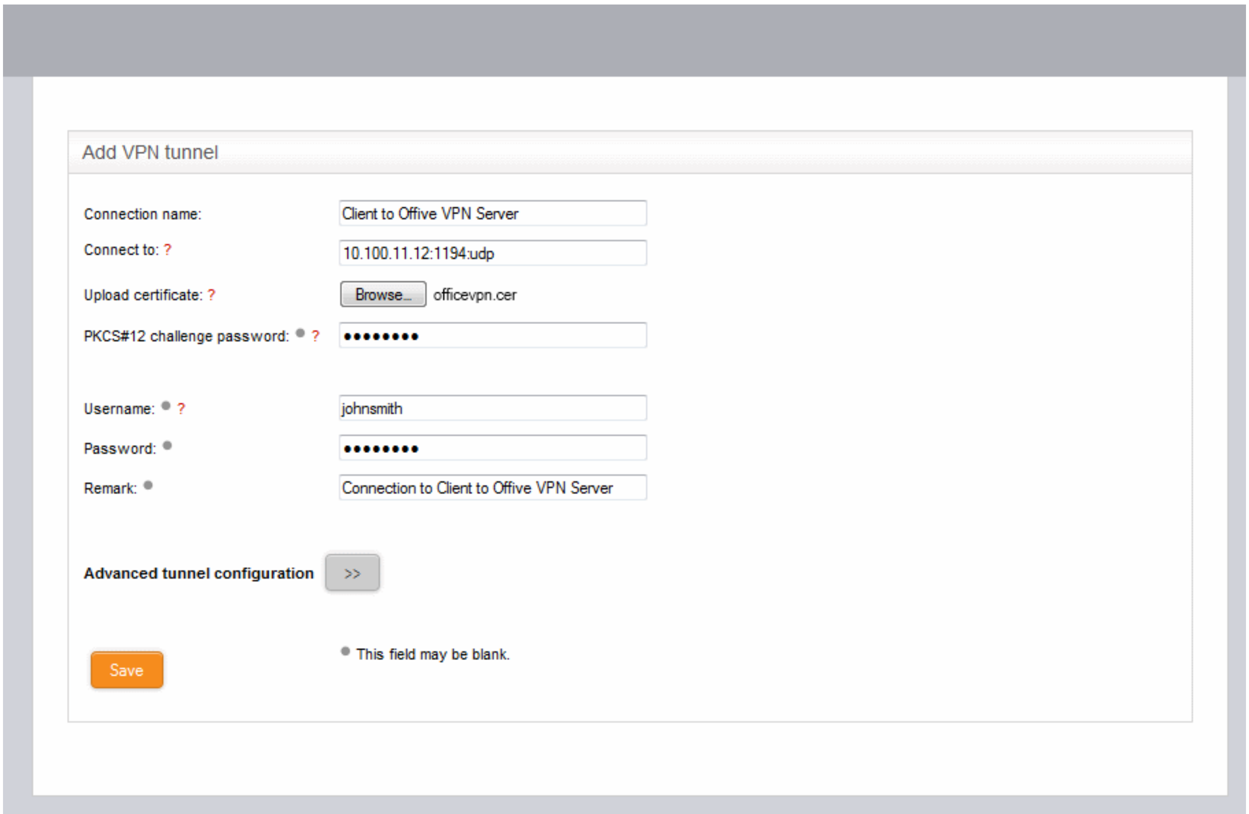
Creating a New Tunnel Configuration

A tunnel to connect to an external SSL VPN server can be added by simply specifying its hostname, uploading its server certificate and entering its access credentials. The configuration interface also allows the administrator to specify advanced tunnel configuration parameters like fallback servers, device/connection types and so on.

Prerequisite - The server certificate of the external SSL VPN server needs to be exported and installed on the client computer from which the firewall admin console is accessed.

To add a new tunnel configuration

- Click 'Add tunnel configuration'. The 'Add VPN tunnel' interface will open.



Add VPN tunnel

Connection name: Client to Offive VPN Server

Connect to: ? 10.100.11.12:1194:udp

Upload certificate: ? Browse... officevpn.cer

PKCS#12 challenge password: ● ? ••••••••

Username: ● ? johnsmith

Password: ● ••••••••

Remark: ● Connection to Client to Offive VPN Server

Advanced tunnel configuration >>

Save

● This field may be blank.

  - Connection name - Enter a name to identify the tunnel
  - Connect to - Enter the host name or IP address of the external SSL VPN server in the following format:

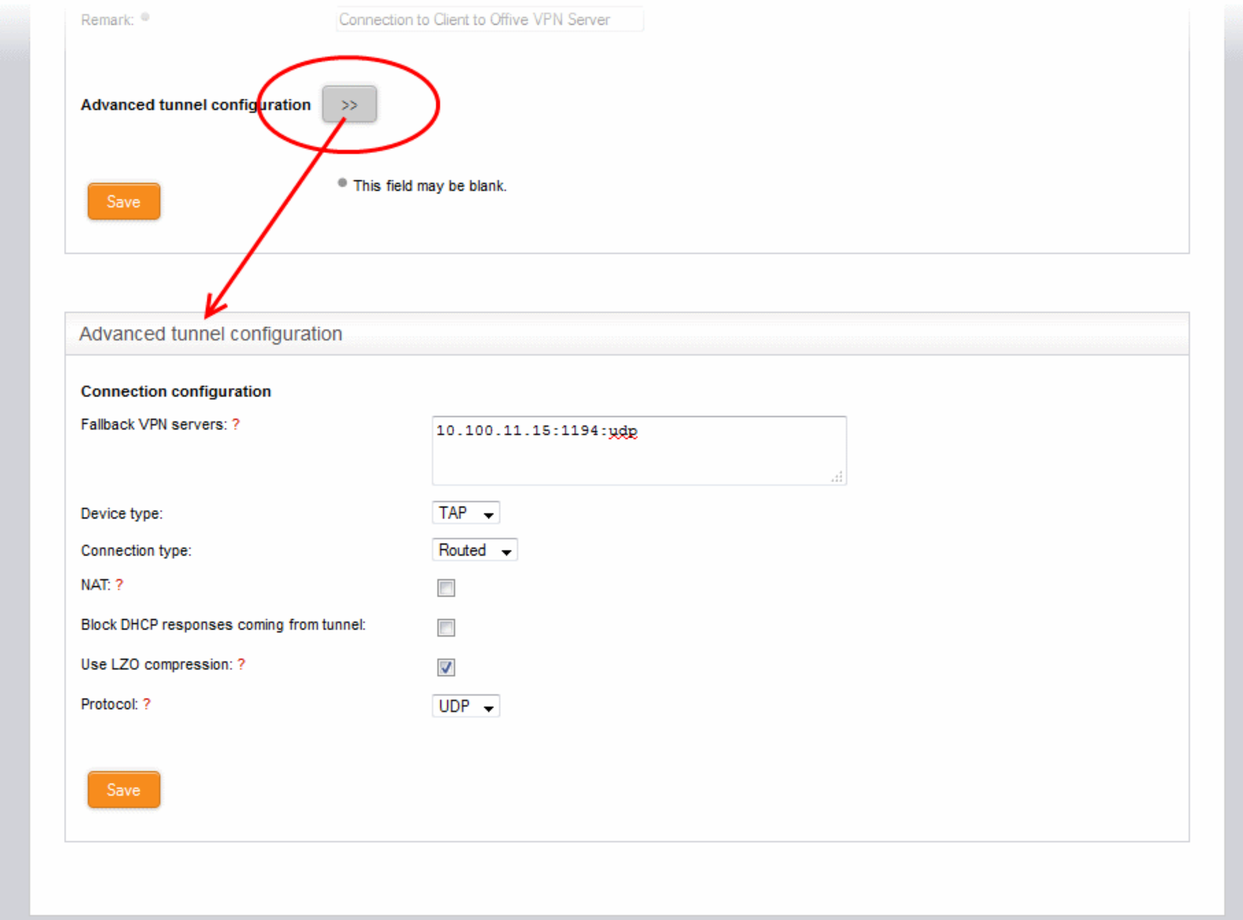
    <hostname (in FQDN format)>:port:protocol or <IP address>:port:protocol

    If the default port 1194 is to be used, you need not specify the port

    Specify the protocol in lowercase letters. If the default protocol UDP is used, you need not specify the protocol
  - Upload certificate - The server certificate of the external VPN server needs to be imported into the client.
    - If the external VPN server uses PSK type authentication, then the server's host certificate needs to be uploaded to the client
    - If the external server uses client certificate type authentication, then the client certificate for your user account, obtained from the external CA needs to be uploaded
    - Click 'Browse' beside the 'Upload Certificate' and navigate to the location of the certificate stored in the local computer or the network and click 'Open'.
  - PKCS#12 challenge password - Enter the challenge password to access the certificate in the 'Challenge password' text box.
  - Username/Password - If the external VPN server requires the username and password of your user account to be entered to connect to it, enter the username and password.
  - Remark - Enter a short description for the tunnel.
- If you wish to configure advanced configuration parameters for the tunnel, click the '>>' button beside the 'Advanced tunnel configuration'. Else click 'Save'. The SSL VPN client will be restarted and a new connection will be established to the server specified.

  Advanced Tunnel Configuration

  Clicking the >> button will open the opens Advanced Tunnel Configuration pane.



Remark: ● Connection to Client to Offive VPN Server

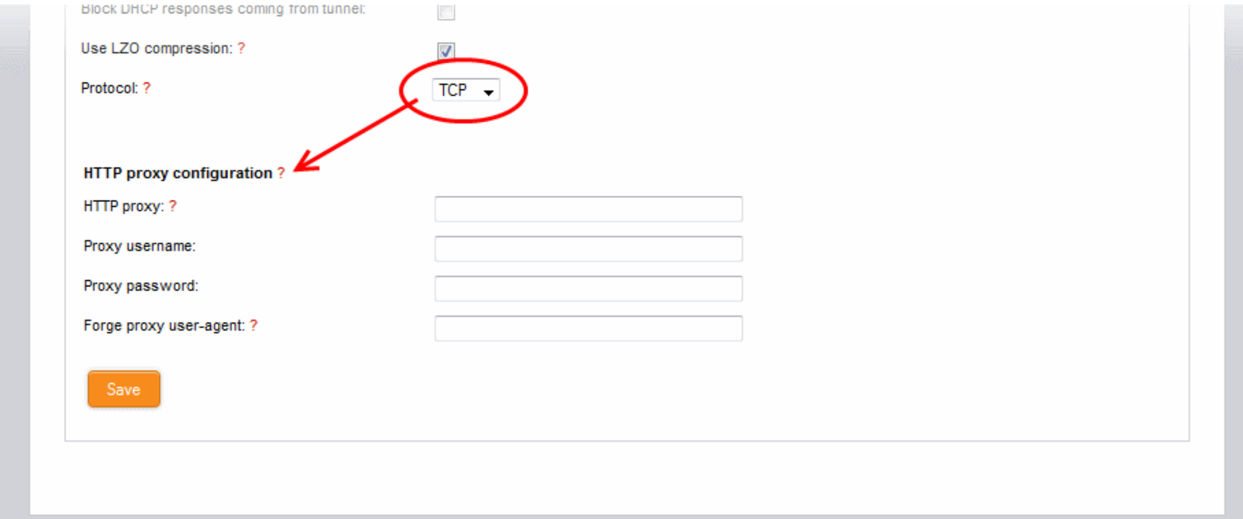
● This field may be blank.

Advanced tunnel configuration

Connection configuration

Fallback VPN servers: ?	10.100.11.15:1194:udp
Device type:	TAP
Connection type:	Routed
NAT: ?	□
Block DHCP responses coming from tunnel:	□
Use LZO compression: ?	☑
Protocol: ?	UDP

- Fallback VPN Servers - If any fallback servers are setup for the primary VPN server, specify the fallback servers in the **same format** used for the primary server.
- Device type - Choose the type of the virtual-network kernel device used by the server. The choice available are TUN and TAP.
- Connection type - Choose the connection type if TAP network device is used. The options available are 'Routed' and 'Bridged'.
- NAT - If the connection type is 'Routed', choose whether are not Network Address Translation (NAT) is to be applied. If applied, the host computers connected through this gateway client will be hidden behind the firewall's VPN IP address. This configuration will prevent incoming connections requests to the hosts.
- Bridge to - If the connection type is 'Bridged', choose the internal network zone to which the connection is to be bridged.
- Block DHCP responses coming from tunnel - Select this option, if you wish to block the DHCP responses from the network at the other side of the VPN tunnel that conflict with the local DHCP server.
- Use LZO compression - Select this option, if wish to apply lossless and high speed Lempel-Ziv-Oberhumer (LZO) data compression to the traffic passing through the tunnel. The LZO compression reduces the load on the tunnel.
- Protocol - Choose the protocol used by the external EasyVPN server. The default protocol is UDP. If the DFW virtual appliance can access the internet only through an upstream HTTP proxy then choose TCP and ensure that the external server also uses TCP protocol. Enter the HTTP Proxy parameters on choosing TCP.



Block DHCP responses coming from tunnel: □

Use LZO compression: ? ☑

Protocol: ? TCP

HTTP proxy configuration ?

HTTP proxy: ?

Proxy username:

Proxy password:

Forge proxy user-agent: ?

- HTTP proxy - specify the HTTP Proxy server in the **same format** used for the primary server.
- Proxy username / Proxy password - Enter the username/password to access the proxy server
- Forge proxy user-agent - Enter the user agent string to be used by the DFW virtual appliance to identify itself as a browser to the proxy server, This is optional, and useful if the proxy accepts connections only for some type of browsers.

- Click 'Save'.

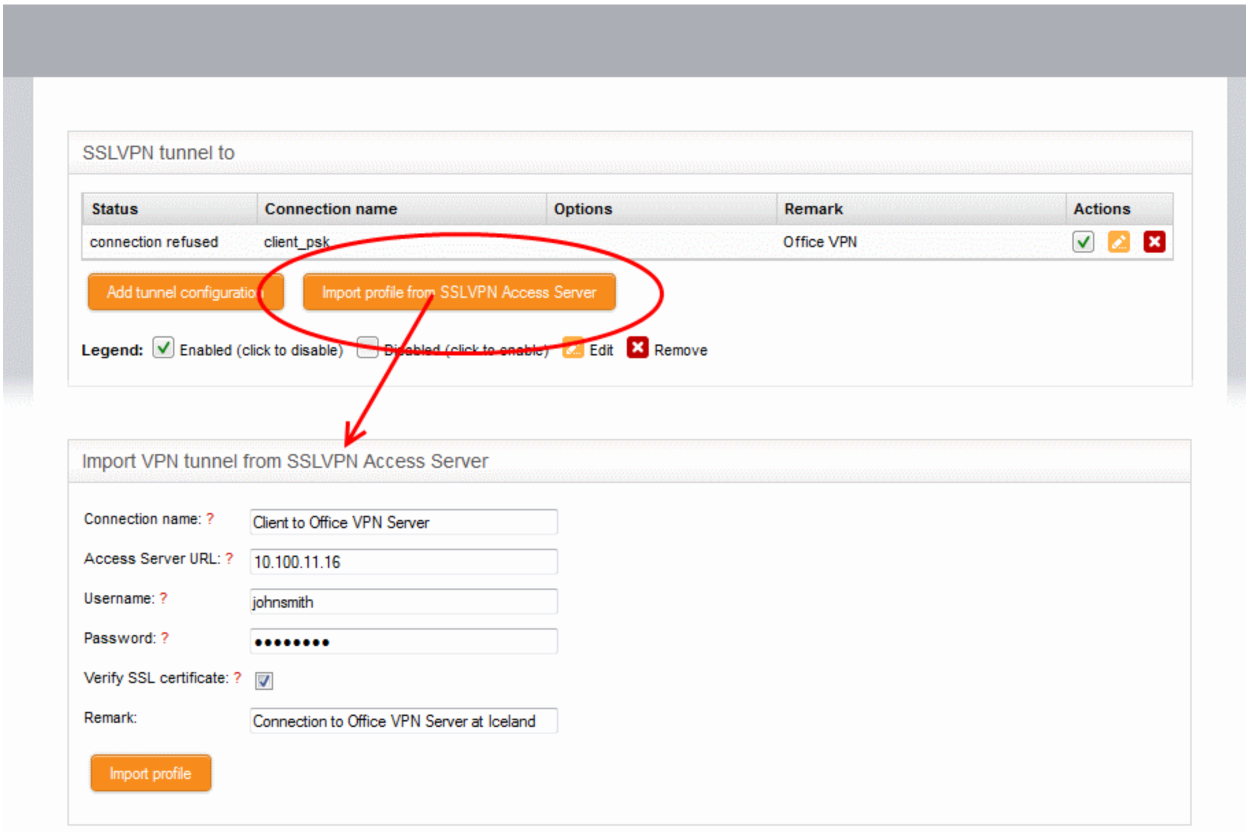
The new advanced parameters for the tunnel configuration will be saved.

Importing the Configuration from the SSL VPN Server

If the client configuration profile is available from the external VPN server for automatic configuration of the client, then the simplest way of creating a new tunnel is by directly importing the configuration from the server. Upon successful import of the configuration profile from the server, a new tunnel will be automatically created for connection to the external server.

To import the configuration profile

- Click 'Import profile from SSLVPN Access Server' from the SSLVPN Client interface. The 'Import VPN tunnel from SSLVPN Access Server' pane will open.



SSLVPN tunnel to

Status	Connection name	Options	Remark	Actions
connection refused	client_psk		Office VPN	✓ ✎ ✖

Add tunnel configuratio
Import profile from SSLVPN Access Server
Legend: ✓ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ✖ Remove

Import VPN tunnel from SSLVPN Access Server

Connection name: ?	Client to Office VPN Server
Access Server URL: ?	10.100.11.16
Username: ?	johnsmith
Password: ?	••••••••
Verify SSL certificate: ?	☑
Remark:	Connection to Office VPN Server at Iceland

  - Connection name - Enter a name to identify the tunnel.
  - Access Server URL - Enter the URL of the external SSLVPN server with the Remote Procedure Call (RPC) configuration
  - Username / Password - Enter the username and password of your user account at the server.
  - Verify SSL certificate - If the server runs on SSL encrypted channel, select this option. The client will check for the valid SSL certificate at the server in order to establish the connection. If the server is implemented with a self-signed certificate, do not select this option.
  - Remark- Enter a short description for the tunnel.

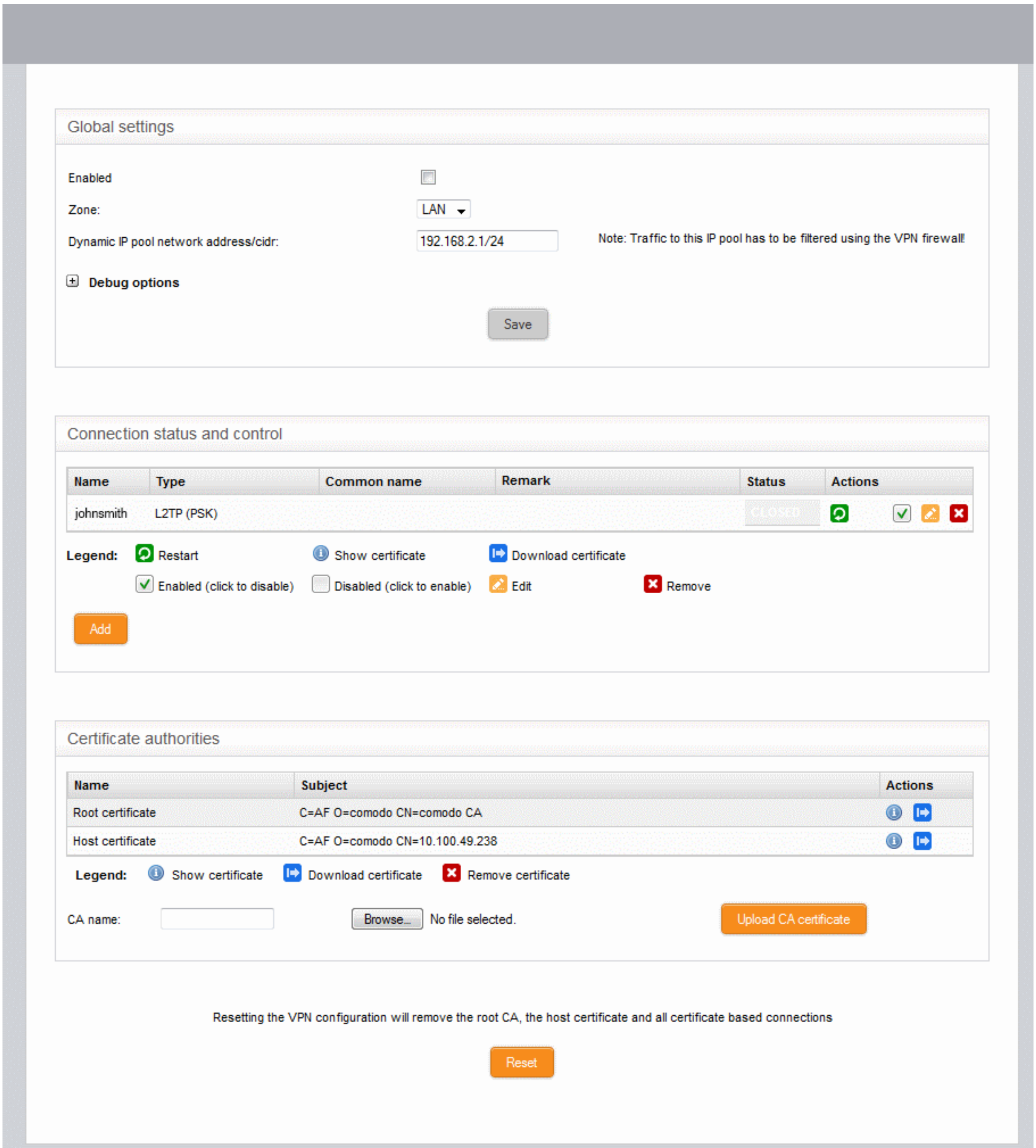
- Click 'Import Profile' after entering the details. The client will connect to the server and import the client configuration file. A new tunnel will be configured with the imported configuration profile.

10.3 IPSec Configuration

This area allows administrators to configure IPsec tunnels between different networks and sites. Dome Firewall supports the following types of connection:

- Host to Net VPN - Allows remote mobile devices, desktops and laptops to securely connect to internal networks
- Net to Net VPN - Allows network to network IPsec VPN connections (also know as Site-to-Site VPN)
- L2TP Host to Net VPN - Enables external clients using L2TP clients to connect to internal networks through an IPsec VPN

To open the 'IPSec' interface, click 'VPN' > 'IPSec' in the left menu:



Global settings

Enabled	□
Zone:	LAN
Dynamic IP pool network address/cidr:	192.168.2.1/24

Note: Traffic to this IP pool has to be filtered using the VPN firewall!

⊞ **Debug options**

Connection status and control

Name	Type	Common name	Remark	Status	Actions
johnsmith	L2TP (PSK)			CLOSED	☑ ✎ ☒

Legend: Restart · Show certificate · Download certificate · ☑ Enabled (click to disable) · □ Disabled (click to enable) · ✎ Edit · ☒ Remove

Certificate authorities

Name	Subject	Actions
Root certificate	C=AF O=comodo CN=comodo CA	
Host certificate	C=AF O=comodo CN=10.100.49.238	

Legend: Show certificate · Download certificate · ☒ Remove certificate

CA name: Browse... No file selected.

Resetting the VPN configuration will remove the root CA, the host certificate and all certificate based connections

Administrators can use the interface to create, enable, configure and monitor IPsec connections and to configure authentication preferences. Authentication between IPsec connected interfaces can be implemented via certificate-based authentication or by pre-shared key.

To access the 'IPsec' interface, select the 'VPN' tab on the menu bar and click 'IPsec' in the left-hand menu.

The interface contains three areas:

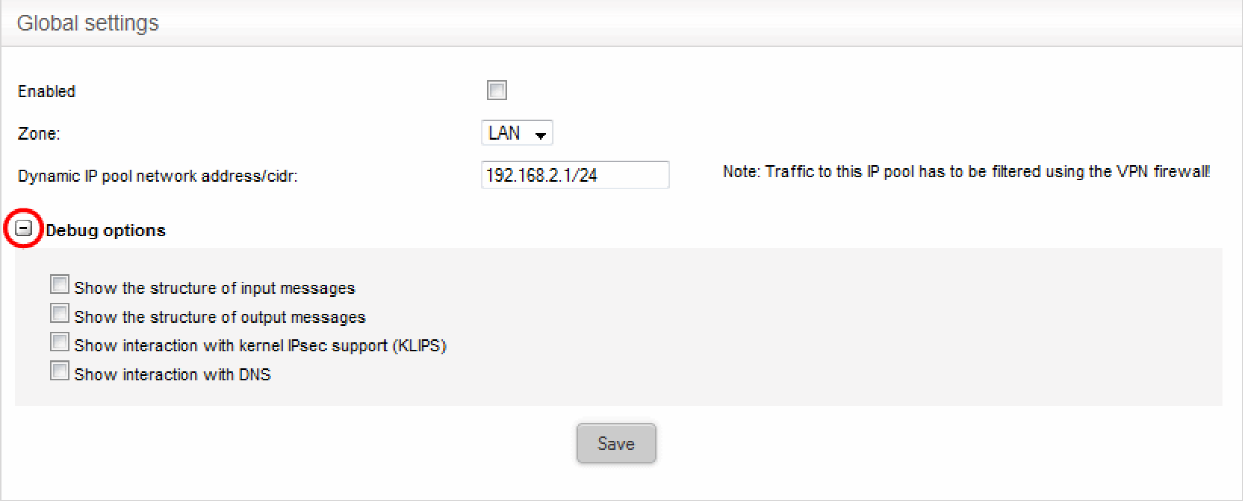
- Global Settings
- Connection status and control
- Certificate authorities

Global Settings

The 'Global Settings' area allows you to:

- Enable or disable the IPsec VPN service
- Configure which internal network zones can be accessed over IPsec
- Specify the dynamic IP address pool that should be used when assigning addresses to external clients.

The 'Debug Options' area allows you to choose how much information is included in IPsec events in debugging logs.



Global settings

Enabled □

Zone: LAN

Dynamic IP pool network address/cidr: 192.168.2.1/24

Note: Traffic to this IP pool has to be filtered using the VPN firewall!

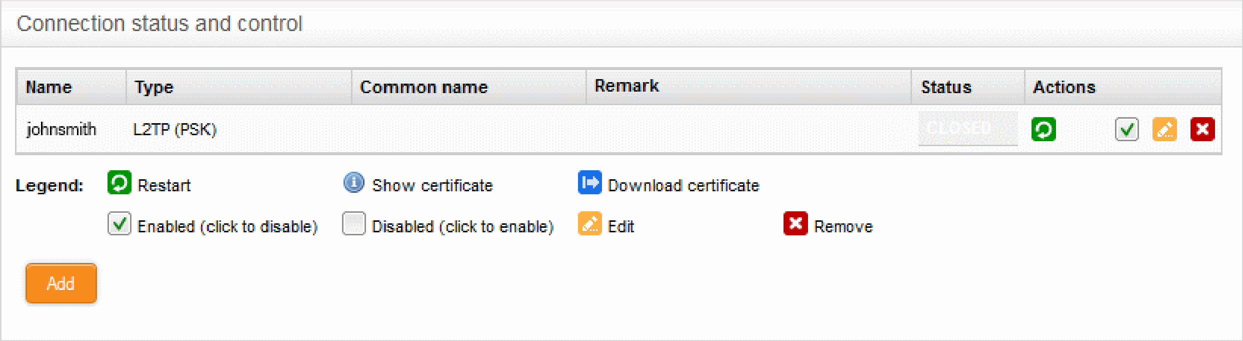
⊟ Debug options

- □ Show the structure of input messages
- □ Show the structure of output messages
- □ Show interaction with kernel IPsec support (KLIPS)
- □ Show interaction with DNS

- Enabled - Select the checkbox to enable the IPsec VPN service
- Zone - Choose the internal network zone to allow external clients and networks to access through the IPsec VPN
- Dynamic IP pool network address/cidr - Specify the IP addresses for dynamic assignment to the external clients in CIDR notation
- Debug options - Allows the administrator to configure the level of detail recorded for IPsec events in the debug log file in the event of connection failures. The log file is located at /var/log/messages in the internal storage of the virtual appliance. Click the '+' button to view the list of available options .
- Click 'Save' for your settings to take effect

Connection Status and Control

The 'Connection Status and Control' area allows you to view, edit and add IPsec tunnels.



Connection status and control

Name	Type	Common name	Remark	Status	Actions
johnsmith	L2TP (PSK)			CLOSED	⟳ ☑ ✎ ☒

Legend: ⟳ Restart ⓘ Show certificate ➡ Download certificate

☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

IPsec Connection Status and Control table - Column Descriptions	
Column	**Description**
Name	The label used to identify the connection.
Type	Indicates the type of the tunnel and the authentication type used. The IPsec service supports two types of authentication: • Pre-Shared key (PSK) - Requires username/password to be entered at the client device • Certificate - Requires an client authentication certificate to be installed on the connecting device. The certificate can be generated from the DFW virtual appliance and exported to the client device.
Common Name	If certificate authentication is used, this field shows the certificate 'Common Name'. This is usually the name of the device or the name of the user.
Remark	A short description of the tunnel.
Status	Indicates the connection status of the tunnel. The possible values are: • Established - The connection to the external client is enabled and live • Connecting - The connection is being established • Closed - The connection is terminated
Actions	Displays control buttons for managing the tunnel. ⟳ - Allows the administrator to re-establish closed connections. ⓘ - Available only for connections with certificate type authentication. Clicking this icon opens the Certificate pane that displays the client certificate. ➡ - Allows the administrator to download the client certificate for deployment on to the client machine. ☑ - Allows the administrator to switch the connection between enabled and disabled states. ✎ - Enables to edit the tunnel configuration. The pane for editing a tunnel is similar to the pane for adding a new tunnel . Refer to the section explaining **adding a new IPsec tunnel configuration** for more details. ☒ - Removes the tunnel configuration.

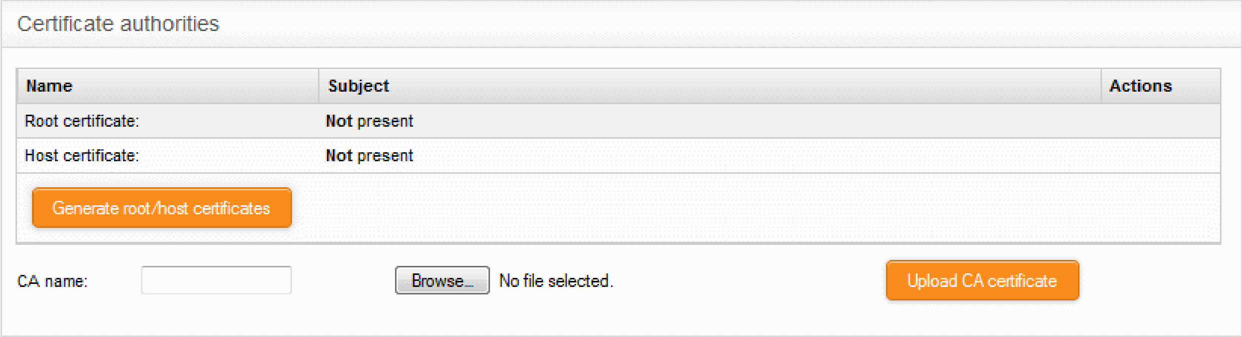
Certificate Authorities

The 'Certificate authorities' area allows the administrator to manage the Root certificate / Host certificate or the server certificate for authentication of remote clients connecting through the IPsec tunnel.

The external client/network can authenticate itself by using a client certificate:

- That was generated by the DFW virtual appliance and sent to the client ;
- Generated by the DFW virtual appliance by signing the certificate request received from the client; or
- Obtained from an external CA.

Initially, no certificate will be available with the DFW virtual appliance. If a new tunnel configuration is created with certificate type authentication, the administrator should first generate self-signed root and host certificates or upload a server certificate obtained from an external CA for deployment on to the DFW virtual appliance. This certificate will be used to generate a new client certificate for the client or to sign the certificate request received from the client.



Certificate authorities

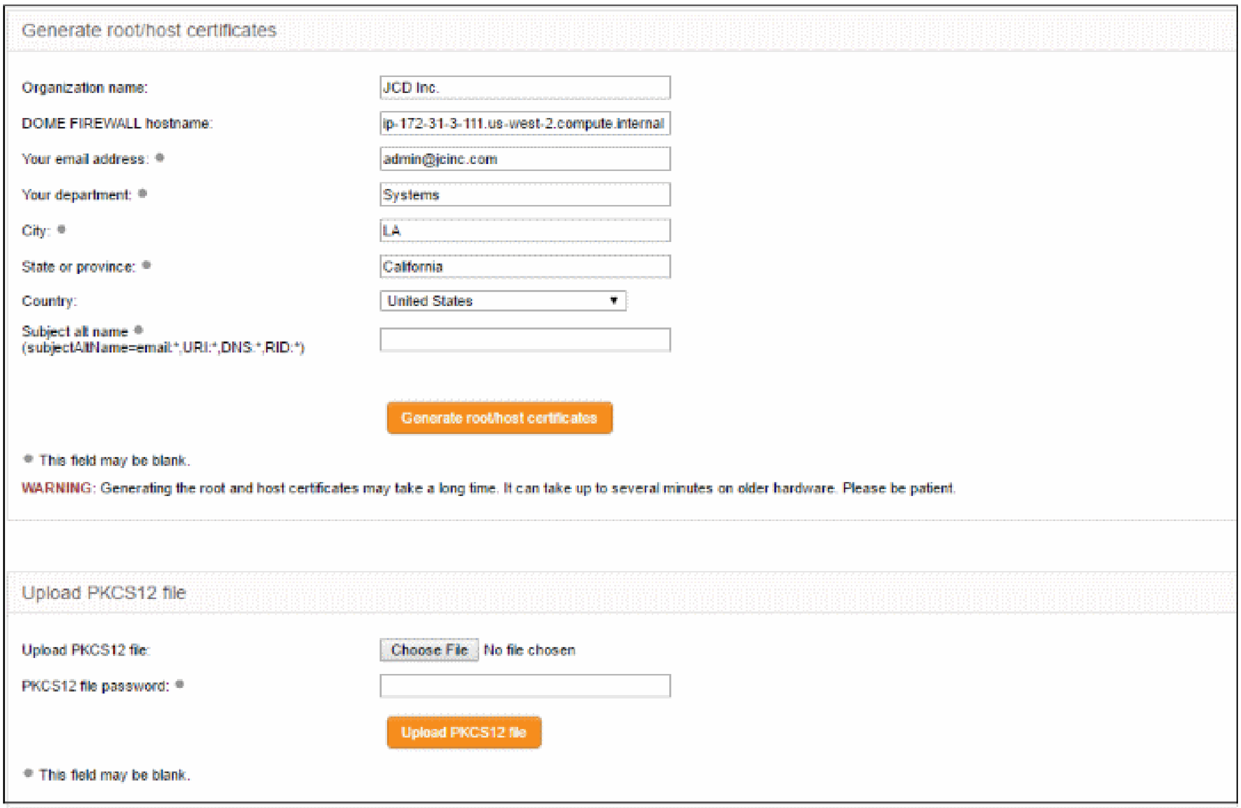
Name	Subject	Actions
Root certificate:	**Not present**	
Host certificate:	**Not present**	

The following sections explain on:

- **Generating new self-signed Root/Host certificates**
- **Uploading server certificate obtained from an external CA**

To generate new self-signed certificates

- Click 'Generate root/host certificates' . The 'Generate root/host certificates' pane will open. The pane allows the administrator to create a new certificate or upload a previously generated certificated stored locally in PKCS12 format.



Generate root/host certificates

Organization name:	JCD Inc.
DOME FIREWALL hostname:	ip-172-31-3-111.us-west-2.compute.internal
Your email address: *	admin@jcinc.com
Your department: *	Systems
City: *	LA
State or province: *	California
Country:	United States
Subject alt name * (subjectAltName=email:*,URI:*,DNS:*,RID:*)	

* This field may be blank.

WARNING: Generating the root and host certificates may take a long time. It can take up to several minutes on older hardware. Please be patient.

Upload PKCS12 file

Upload PKCS12 file:	Choose File No file chosen
PKCS12 file password: *	

* This field may be blank.

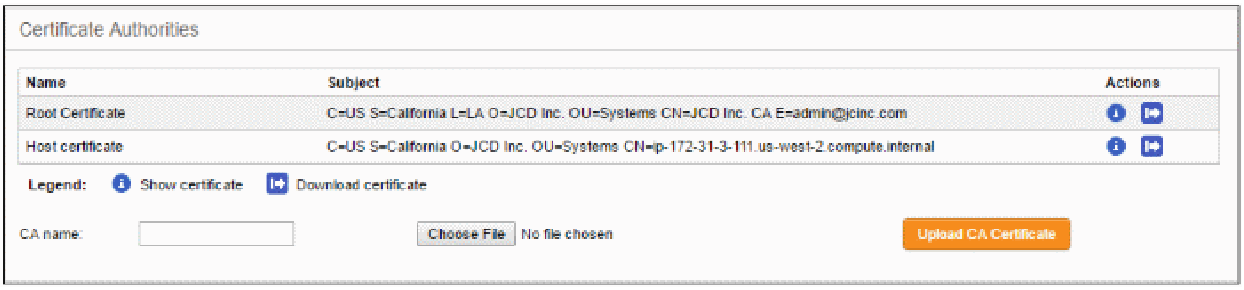
  - Organization name - Enter the name of your organization. This will appear in the 'Organization' field of your certificate
  - Dome Firewall hostname - Enter the IP address or host name of the Dome Firewall virtual appliance.
  - Your email address - Enter your email address, to be included in the certificate
  - Your department - Enter your department. This will appear in the 'Organizational Unit' (OU) field of the certificate
  - City - Enter your city
  - State or province - Enter your state or province
  - Country - Choose your country from the drop-down
  - Subject alt name - Enter the alternative host names of the DFW virtual appliance, if any.
- Click 'Generate root/host certificate'

Alternatively, if the administrator has any of the previously generated certificates stored in PKCS12 format, then the certificate can be uploaded to the virtual appliance, instead of creating new certificates.

To upload an existing certificate

- Click the 'Choose File' button beside 'Upload PKCS12 file' and locate the certificate you wish to upload.
- Enter the password which was specified when exporting the certificate
- Upload the PKCS12 certificate.

The certificates will be created and listed under 'Certificate authorities'



Certificate Authorities

Name	Subject	Actions
Root Certificate	C=US S=California L=LA O=JCD Inc. OU=Systems CN=JCD Inc. CA E=admin@jcinc.com	ⓘ ➡
Host certificate	C=US S=California O=JCD Inc. OU=Systems CN=ip-172-31-3-111.us-west-2.compute.internal	ⓘ ➡

Legend: ⓘ Show certificate ➡ Download certificate

CA name: ______ Choose File No file chosen Upload CA Certificate

Only one certificate at a time can be used for a single connection. If a new tunnel need to be configured, the existing certificate and the connection using the existing certificate can be removed by resetting the certificate store. The administrator can view the certificates by clicking the ⓘ button or download the certificate by clicking the ➡ button. The downloaded certificates can then be exported to PKCS12 format for importing into the virtual appliance in future.

To upload server certificate obtained from external CA

- Enter the CA name for identification in the CA name text field.
- Click the 'Choose File' button beside the text field and navigate to the location in the local storage or the network where the certificate is stored and click 'Open'.
- Click 'Upload CA certificate'.

The certificate will be imported into the DFW virtual appliance.

Adding a New Tunnel Configuration

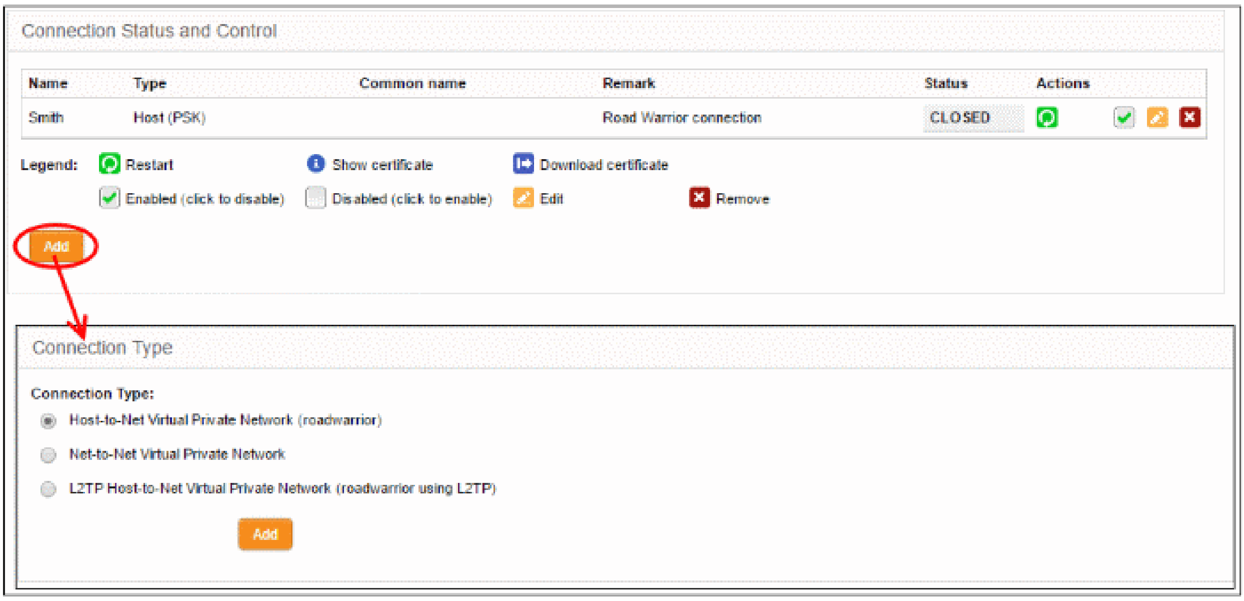
Three types of IPsec VPN Tunnels can be created in Comodo Dome Firewall:

- Host to Net VPN - Enables mobiles, desktops and portable computers (a.k.a Road Warriors) to connect to the internal networks
- Net to Net VPN - For connection from external IPsec VPN servers enabling network to network VPN connection (also called as Site-to-Site VPN)
- L2TP Host to Net VPN - Enabling external clients using L2TP clients to connect to the internal networks through IPsec VPN

Note: In order to allow L2TP Hosts to connect to the VPN, the L2TP server must be enabled and configured in the DFW virtual appliance. See '**L2TP server Configuration**' for more details. By default only one connection is allowed at a time for L2TP/IPsec connection. To enable more number to users to connect simultaneously, the L2TP/IPsec user accounts are to be added to the server. See '**IPsec / L2TP Users Configuration**' for more details.

To create a new tunnel

- Click 'Add' from the Connection Status and Control area in the 'IPSec 'interface.



Connection Status and Control

Name	Type	Common name	Remark	Status	Actions
Smith	Host (PSK)		Road Warrior connection	CLOSED	

Legend: Restart · Show certificate · Download certificate
☑ Enabled (click to disable) · □ Disabled (click to enable) · Edit · ☒ Remove

Connection Type

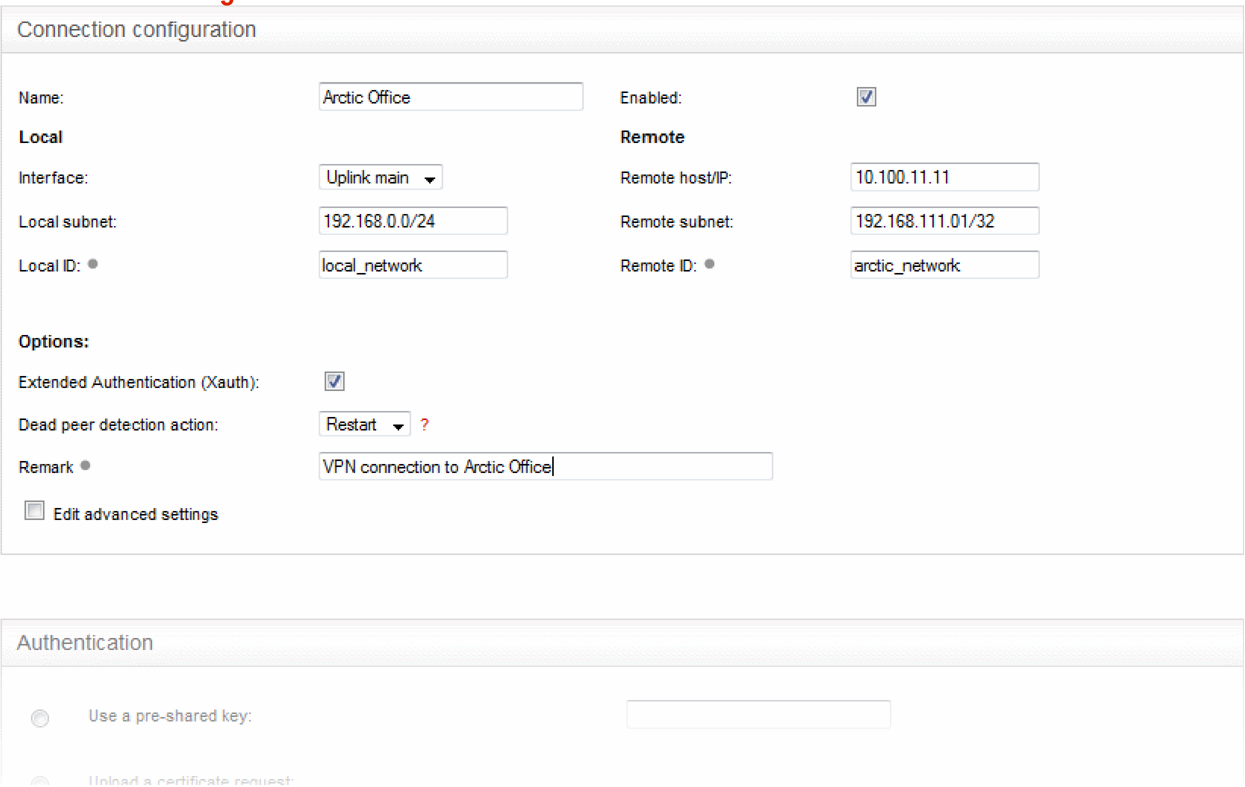
Connection Type:

- ● Host-to-Net Virtual Private Network (roadwarrior)
- ○ Net-to-Net Virtual Private Network
- ○ L2TP Host-to-Net Virtual Private Network (roadwarrior using L2TP)

The Connection type interface will open.

- Choose the connection type and click 'Add'. The interface for specifying the connection configuration parameters and the authentication parameters will open. The interface is similar for all the three types of connection, except for an additional parameter 'Remote subnet' , if you are creating Net to Net connection type. The interface contains two areas:

Connection Configuration



Connection configuration

Name: Arctic Office

Enabled: ☑

Local

Interface: Uplink main

Local subnet: 192.168.0.0/24

Local ID: ● local_network

Remote

Remote host/IP: 10.100.11.11

Remote subnet: 192.168.111.01/32

Remote ID: ● arctic_network

Options:

Extended Authentication (Xauth): ☑

Dead peer detection action: Restart ?

Remark ● VPN connection to Arctic Office

□ Edit advanced settings

Authentication

○ Use a pre-shared key:

○ Upload a certificate request:

- Name - Enter a name to identify the connection tunnel
- Enabled - Select this checkbox if you wish the tunnel to be enabled upon creation. Do not select this, if you just want to create the connection this time and enable it at a later time.

Local

- Interface - Choose the uplink interface device connected to the DFW virtual appliance, through which the external client should connect to the local network infrastructure

- Local Subnet - This field is auto populated with the local sub network of LAN. If you want to specify a different subnet, enter the address in CIDR format.
- Local ID - Enter an identification string for the local network.

Remote

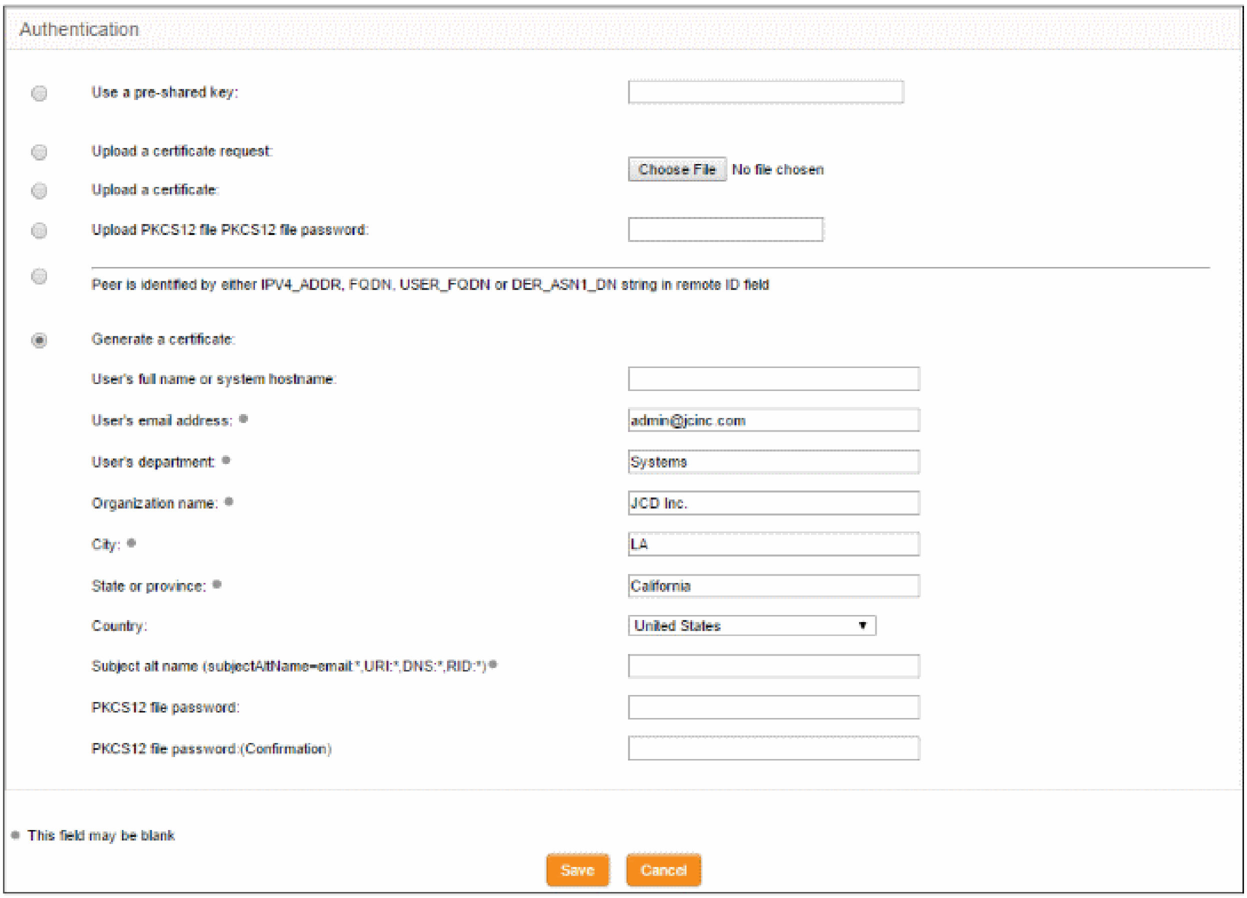
- Remote host/IP - Enter the IP address or hostname of the external host or network
- Remote subnet - The option is available only if you are creating 'Net to Net' connection type. Specify the sub network of the external network that can connect through the tunnel
- Remote ID - Enter an identification string for the local network.

Options

- Extended Authentication (Xauth) - Select this option if you wish to enable extended certificate based authentication for the remote client. You must install the client certificate on to the external client, if you select this option.
- Dead peer detection action - Choose the action to be taken by the DFW virtual appliance if the peer disconnects. The options available are:
  - Clear - Disconnect the connection
  - Hold - Wait for the peer to reconnect
  - Restart - Restart the peer
- Remark - Enter a short description for the connection
- Edit advanced settings - Select this option if you wish to edit advanced configuration parameters of the tunnel. The advanced parameters can be edited only after saving the tunnel configuration. Refer to the section explaining **editing advanced parameters of IPsec tunnel configuration** for more details

Authentication

The Authentication Settings area allows the administrator to select the authentication type. If certificate authentication type is chosen, the administrator can configure for generating the client certificate from this area. The certificate will be available for download from the **Connection status and control** area.



Authentication

○ Use a pre-shared key:

○ Upload a certificate request:

○ Upload a certificate: Choose File No file chosen

○ Upload PKCS12 file PKCS12 file password:

○ Peer is identified by either IPV4_ADDR, FQDN, USER_FQDN or DER_ASN1_DN string in remote ID field

● Generate a certificate:

User's full name or system hostname:	
User's email address: *	admin@jcinc.com
User's department: *	Systems
Organization name: *	JCD Inc.
City: *	LA
State or province: *	California
Country:	United States
Subject alt name (subjectAltName=email:*,URI:*,DNS:*,RID:*) *	
PKCS12 file password:	
PKCS12 file password:(Confirmation)	

* This field may be blank

- Select the authentication type from the options available in this interface:
  - Use a pre-shared key - Select this option if you wish to apply PSK type authentication for the remote client and enter the password to be used for authentication by the remote client.

> **Warning**: It is recommended to not to choose PSK type authentication type for 'Host to Net' connection type.

The following options are for client certificate type authentication and will be available only if Root and Host certificates are generated or a server certificate obtained from CA has been uploaded for the IPsec server in the DFW virtual appliance. Refer to the section **Certificate Authority** for more details.

- Upload a certificate request - If the IPsec tunnel implementation in the remote host does not have its own CA, a certificate request, which is a partial X.509 certificate can be generated at the host. The certificate request can be transferred to the computer from which the administrative console is accessed and uploaded to the DFW virtual appliance. The virtual appliance will sign the request using its root certificate. The signed client certificate will be available from the **Connection status and control** area, which can then be transferred to the remote host and deployed. To upload a client certificate request, select this option and click the Browse button. Navigate to the location where the request file is stored and click 'Open.'
- Upload a certificate - If the remote host already has a client certificate in X.509 format, the certificate can be transferred to the computer from which the administrative console is accessed and uploaded to the virtual appliance. To upload the certificate, select this option and click the Browse button. Navigate to the location where the certificate file is stored and click 'Open.'
- Upload PKCS12 file PKCS12 file password - If the client certificate is exported to PKCS format from the remote host, the .p12 file can be transferred to the computer from which the administrative console is accessed and uploaded to the virtual appliance. To upload the certificate, select this option and click the Browse button. Navigate to the location where the certificate file is stored and click 'Open.'
- Peer is identified by either IPV4_ADDR, FQDN, USER_FQDN or DER_ASN1_DN string in remote

ID field - Select this option if you wish the remote host is to be authenticated based on its IP Address, domain name, or by other unique information of the IPsec tunnel entered in the Remote ID field of the **Connection Configuration** area.

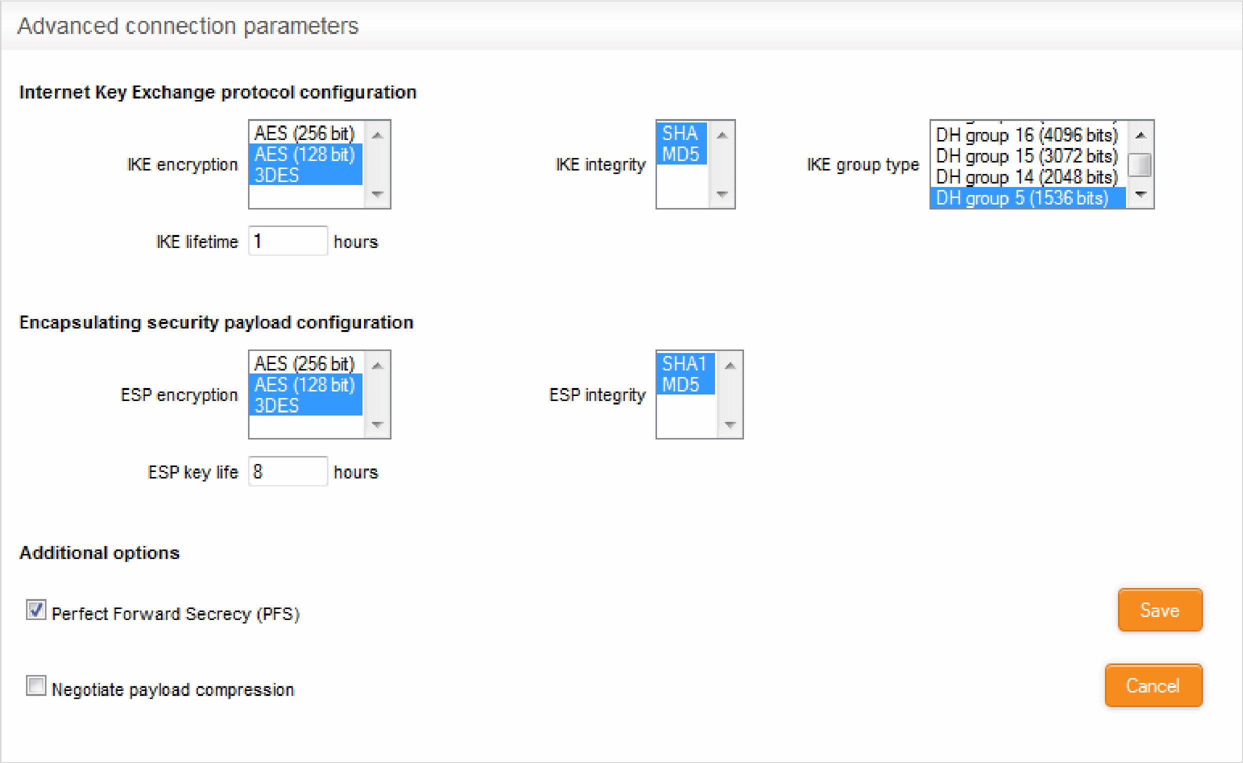
- Generate Certificate - Select this option if you wish to generate a new client certificate for the remote host signed by the Root certificate of IPsec server in the DFW virtual appliance. Enter the parametes for the certificate in the fields below. Upon generation, the client certificate will be available for download from the **Connection status and control** area. The certificate can be transferred to the remote host and deployed for authenticating itself to the server.
  - User's full name or system hostname - Enter the username or the hostname of the remote host. This name will be included in the CN field of the certificate.
  - User's email address - Enter the email address of the user of the host.
  - User's department - Enter the department to which the en-user belongs.
  - Organization name - Enter the name of the organization to which the end-user belongs.
  - City, State or province, Country - Enter the address details of the end-user
  - Subject alt name - Enter the alternative host names, if any, for the remote host.
  - PKCS12 file password - Enter the password for storing the certificate file in .p12 format and re-enter it for confirmation in the next field. This password needs to be entered while importing the certificate at the remote host.

- Click 'Save'.

If you have chosen to edit advanced settings while creating the connection, the '**Advanced Connection Parameters**' interface will open after clicking 'Save'. Else, the connection will be added to the **Connection status and control** area. The certificates generated can be downloaded and imported onto the remote host. The remote host will now be able to connect to the sub network of the internal network specified under Connection Configuration, by configuring the IPsec VPN connection at the host.

Editing Advanced Configuration Parameters of IPsec Tunnel Configuration

Warning: The Advanced connection parameters are automatically selected for optimal performance. It is recommended to leave these settings to default, unless you are an expert and understand the risk of altering encryption parameters.



Advanced connection parameters

Internet Key Exchange protocol configuration

IKE encryption: AES (256 bit), AES (128 bit) [selected], 3DES [selected]

IKE integrity: SHA [selected], MD5 [selected]

IKE group type: DH group 16 (4096 bits), DH group 15 (3072 bits), DH group 14 (2048 bits), DH group 5 (1536 bits) [selected]

IKE lifetime: 1 hours

Encapsulating security payload configuration

ESP encryption: AES (256 bit), AES (128 bit) [selected], 3DES [selected]

ESP integrity: SHA1 [selected], MD5 [selected]

ESP key life: 8 hours

Additional options

☑ Perfect Forward Secrecy (PFS)

□ Negotiate payload compression

Internet Key Exchange (IKE) Protocol Configuration

- IKE Encryption - Select the encryption method(s) to be supported by IKE.
- IKE Integrity - Select the encryption algorithms to be used for checking the integrity of IKE data packets
- IKE group type - Select the group type of IKE packets
- IKE lifetime - Specify how long the IKE packets are to be valid

Encapsulating security payload configuration

- ESP Encryption - Select the encryption method(s) to be supported for encapsulation.
- ESP Integrity - Select the encryption algorithms to be used for checking the integrity of encapsulated data packets
- ESP key life - Specify how long the encapsulated data packets are to be valid

Additional options

- Perfect Forward Secrecy (PFS) - Select this option to enable perfect forward secrecy, so that the keys exchanged during long-term connection sessions are protected from being compromised.
- Negotiate payload compression - Select this option If you wish to allow compression of payload in data packets.

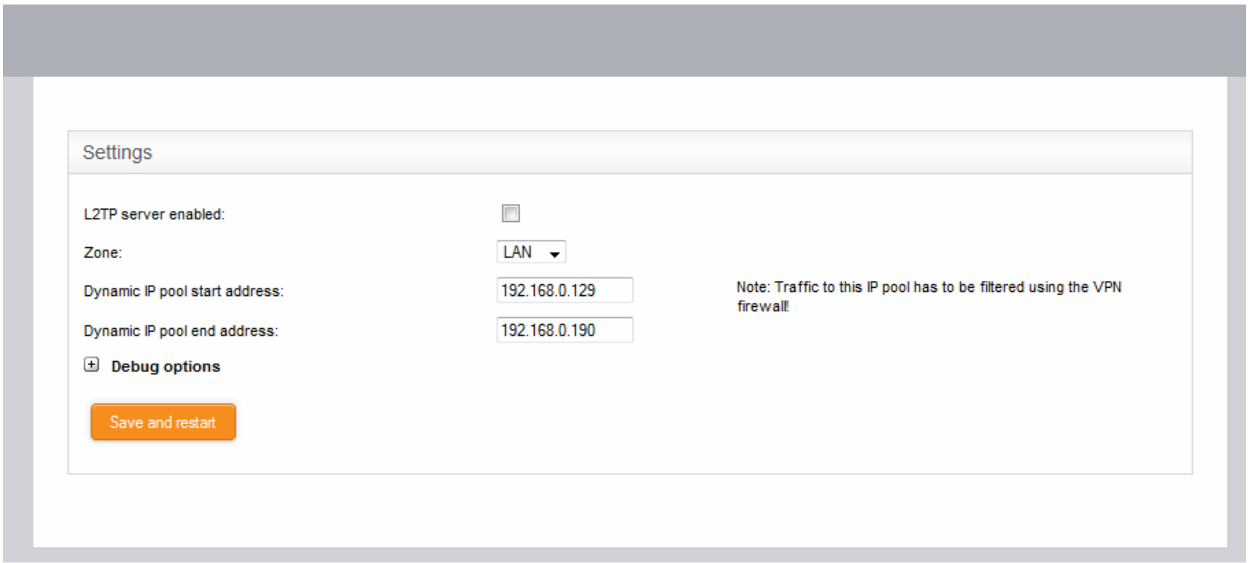
- Click 'Save' for your configuration to take effect.

The connection will be added to the **Connection status and control** area. The certificates generated can be downloaded and imported onto the remote host. The remote host will now be able to connect to the sub network of the internal network specified under Connection Configuration, by configuring the IPsec VPN connection at the host.

10.4 L2TP Server Configuration

Comodo Dome Firewall allows clients using Layer 2 Tunneling Protocol (L2TP) to connect via IPsec VPN tunnel. The L2TP service needs to be enabled and configured in order to support L2TP clients.

- Click 'VPN' > 'L2TP' in the left-menu to open the 'L2TP' interface:



Settings

L2TP server enabled: □

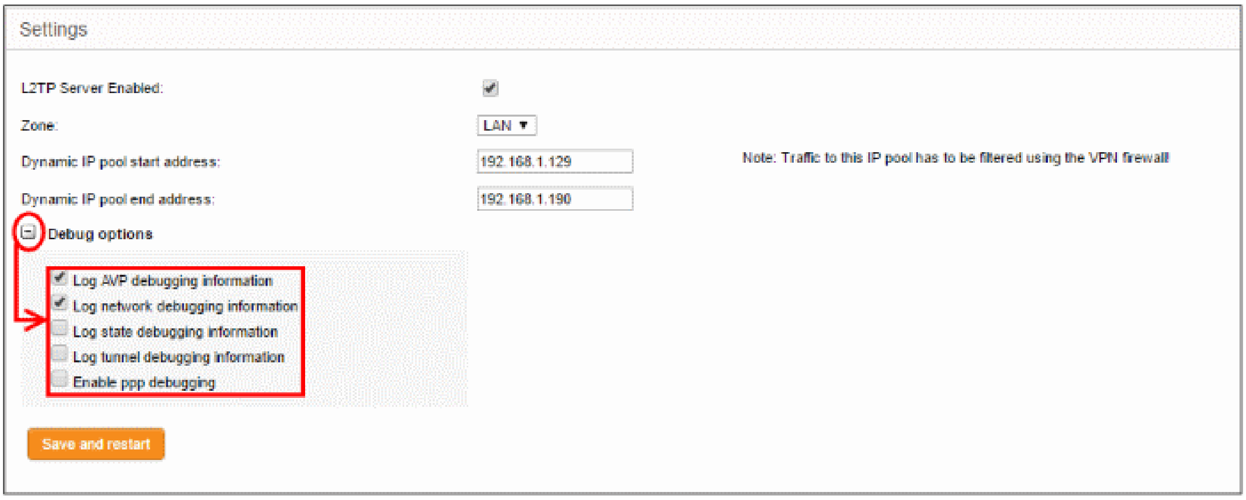
Zone: LAN

Dynamic IP pool start address: 192.168.0.129

Dynamic IP pool end address: 192.168.0.190

Note: Traffic to this IP pool has to be filtered using the VPN firewall!

- Enabled - Select the checkbox to enable the L2TP service
- Zone - Choose the internal network zone to allow external clients and networks to access through the IPsec VPN using L2TP
- Dynamic IP pool start address/end address - Specify the IP address range for dynamic assignment to the external clients that connect through L2TP
- Debug options - Allows admins to configure the level of detail recorded about L2TP connection failures in the debug log file. The log file is located at /var/log/messages in the internal storage of the virtual appliance. Click the '+' button to view the list of available options.



Settings

L2TP Server Enabled: ☑

Zone: LAN

Dynamic IP pool start address: 192.168.1.129

Dynamic IP pool end address: 192.168.1.190

Note: Traffic to this IP pool has to be filtered using the VPN firewall!

⊟ Debug options

☑ Log AVP debugging information
☑ Log network debugging information
□ Log state debugging information
□ Log tunnel debugging information
□ Enable ppp debugging

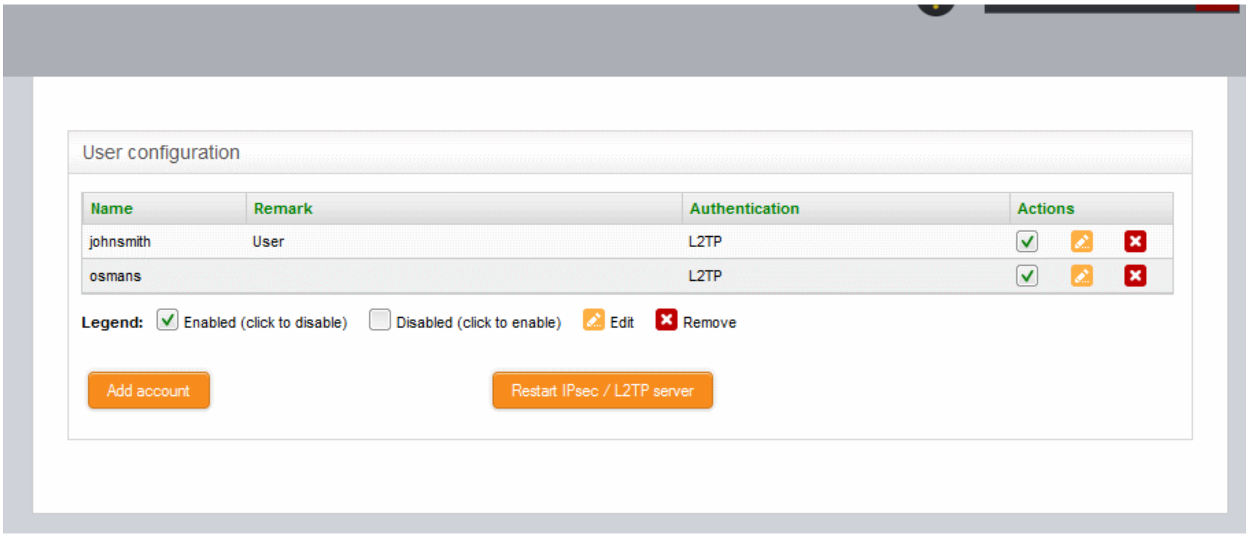
- Click 'Save and restart'. The VPN server will be restarted for your configuration to take effect.

Multiple L2TP users can connect through the IPsec tunnel. See '**IPsec / L2TP Users Configuration**' for details on creating users.

10.5 IPSec / L2TP Users Configuration

The 'IPsec / L2TP Users' area lets you add and manage user accounts for end users that connect to the IPsec VPN tunnel.

- Click 'VPN' > 'IPSec / L2TP Users' to open the 'IPSec / L2TP Users' interface:



User configuration

Name	Remark	Authentication	Actions
johnsmith	User	L2TP	☑ ✎ ☒
osmans		L2TP	☑ ✎ ☒

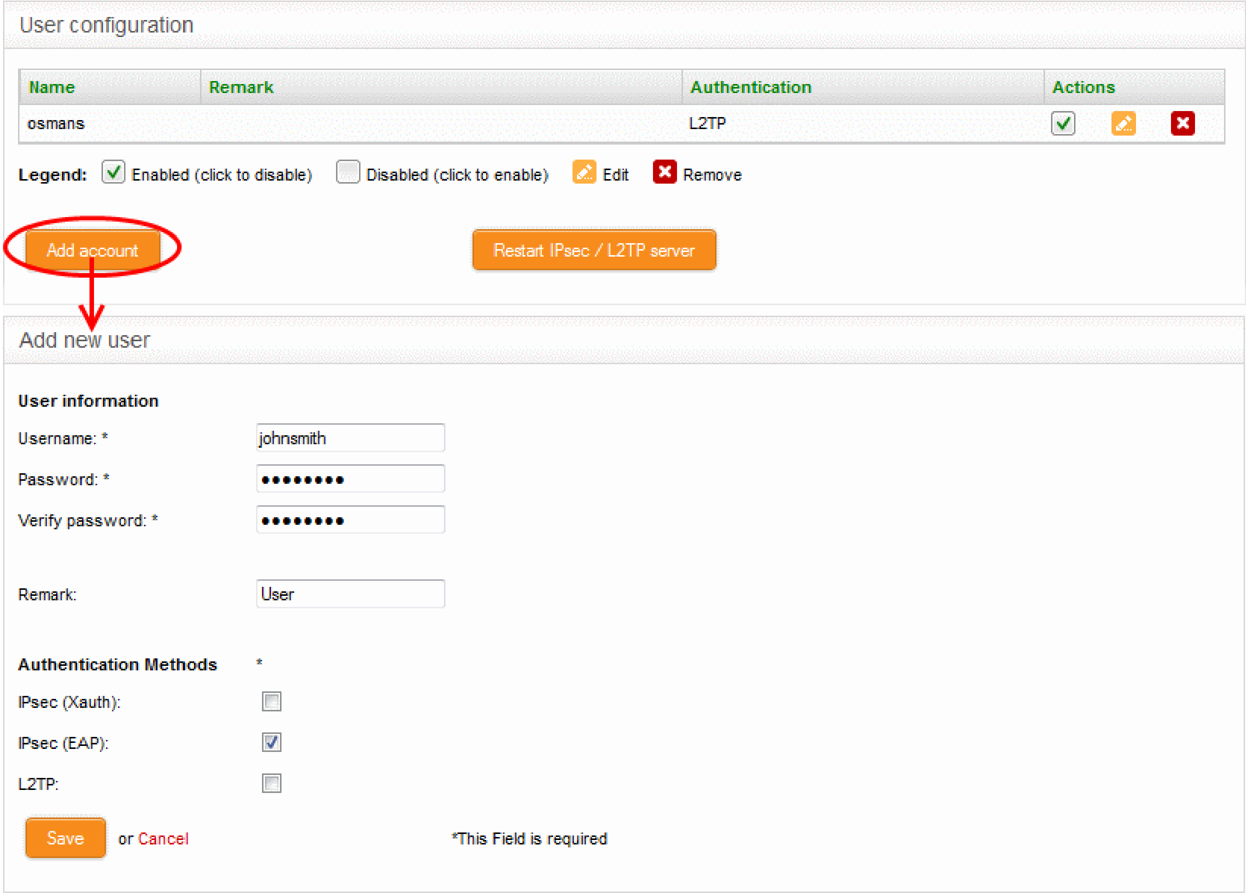
Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

A list of existing user accounts will be displayed. The following details are available for each user:

IPsec / L2TP User Configuration table - Column Descriptions	
Column	**Description**
Name	User's username.
Remark	A short description of the user account.
Authentication	The authentication method used to identify the user to the VPN service
Actions	Controls for managing the account. ☑ - Enable or disable the account's ability to connect via VPN. ✎ - Edit the user account. The editing interface is similar to to the add new account interface. See **adding a new user account** for more details. ☒ - Removes the user account.

To add a new user account

- Click 'Add account'. The 'Add new user' pane will open.



User configuration

Name	Remark	Authentication	Actions
osmans		L2TP	☑ ✎ ☒

Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Add new user

User information

Username: *	johnsmith
Password: *	••••••••
Verify password: *	••••••••
Remark:	User

Authentication Methods *

IPsec (Xauth):	□
IPsec (EAP):	☑
L2TP:	□

*This Field is required

User Information

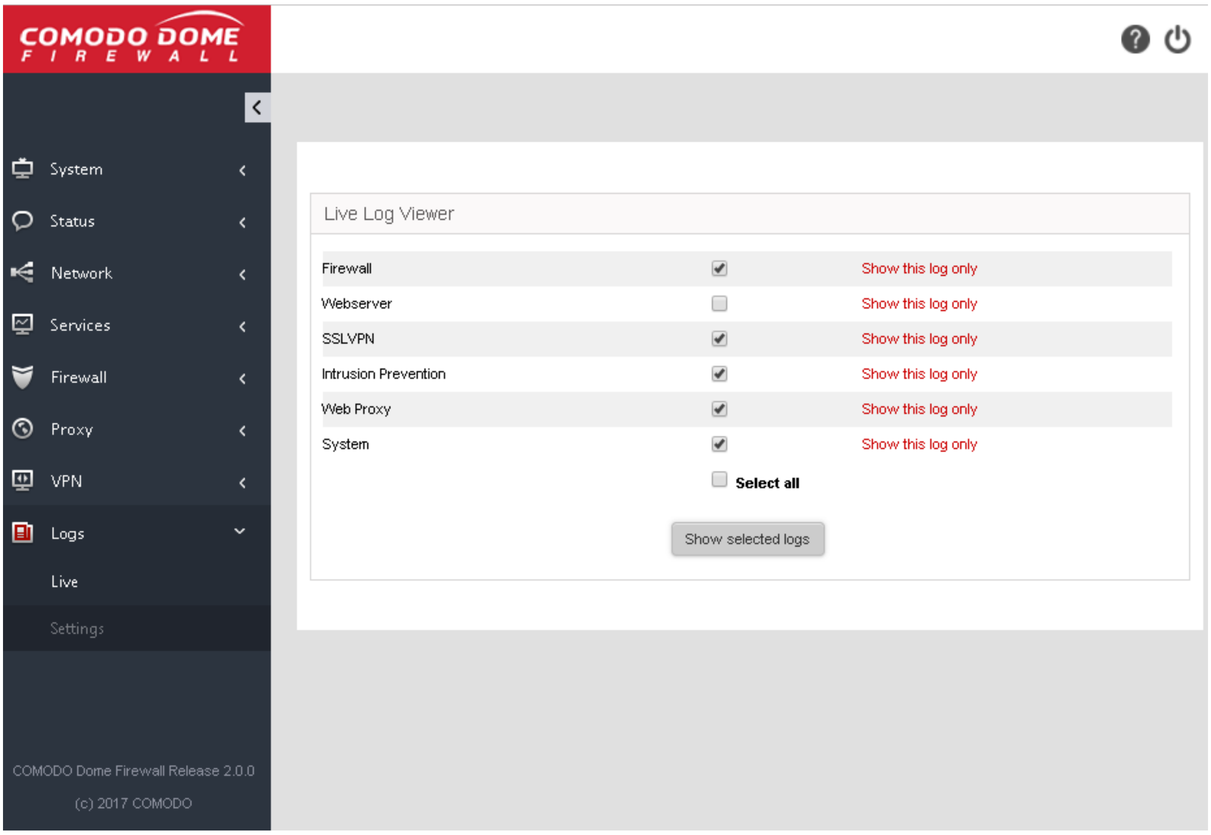
- Username - Enter the name of the user
- Password - Enter the password for the user to connect to the VPN and re-enter the password for confirmation in the 'Verify password' field
- Remark- A short description of the user account

Authentication Methods

- Select the type(s) of authentication used by the user by selecting the respective checkbox(es).
- Click 'Save' The user will be added to the list. But for the user account to take effect, the IPsec / L2TP server needs to be re-started.
- Click Restart IPsec / L2TP server for enable the user.

11 View Logs

The 'Logs' module displays events that are currently taking place across all modules, allowing administrators to effectively troubleshoot any problems and to stay informed in real time. Logs can be filtered according to date, keyword or module.



Live Log Viewer

Firewall	☑	Show this log only
Webserver	□	Show this log only
SSLVPN	☑	Show this log only
Intrusion Prevention	☑	Show this log only
Web Proxy	☑	Show this log only
System	☑	Show this log only

□ **Select all**

Show selected logs

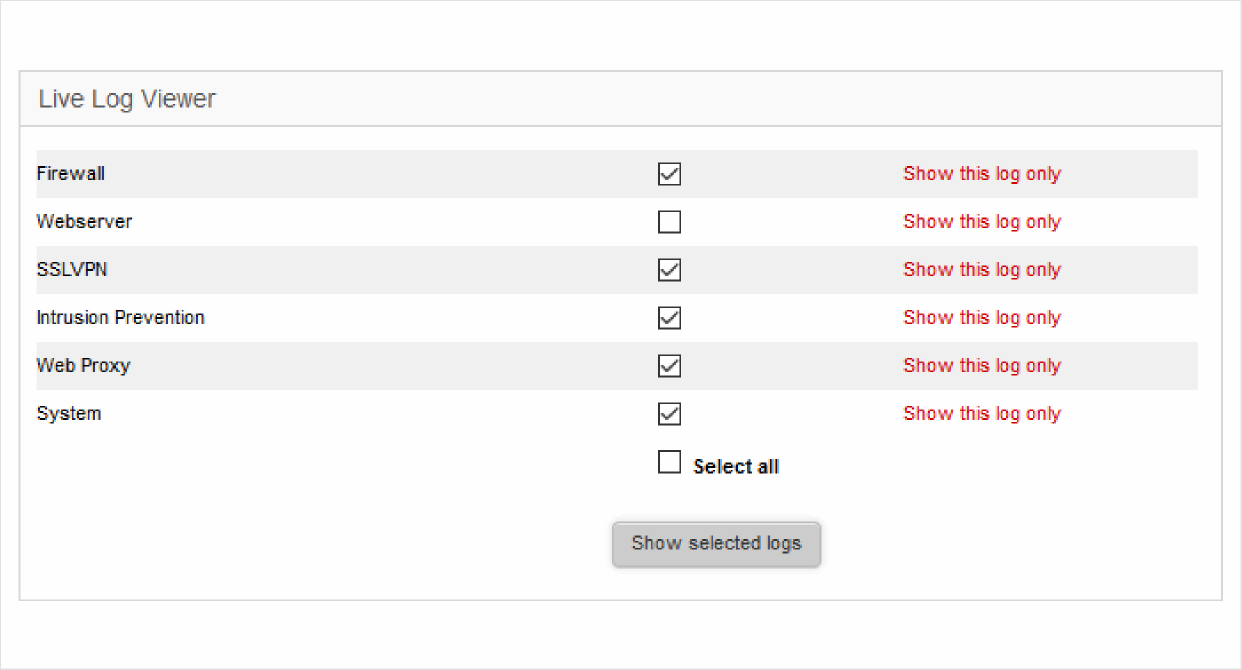
The following sections provide detailed descriptions of viewing realtime logs and configuring the 'Logs' module.

- **Realtime Logs** - View realtime logs of selected Dome features.
- **Configure Log Settings** - Set your view options, remote syslog server, life-cycle of log summaries and more.

11.1 Realtime Logs

Comodo Dome Firewall can keep realtime logs of events from selected modules. The 'Live Logs' interface displays a list of modules and their current events. Events are displayed in a scrolling window which is continuously updated. The window also allows you to filter logs according to specific criteria.

- Click 'Logs' > 'Live' to open the 'Live Logs' interface:



Live Log Viewer

Firewall	☑	Show this log only
Webserver	□	Show this log only
SSLVPN	☑	Show this log only
Intrusion Prevention	☑	Show this log only
Web Proxy	☑	Show this log only
System	☑	Show this log only
	□ Select all	

Realtime logs of the following modules are available:

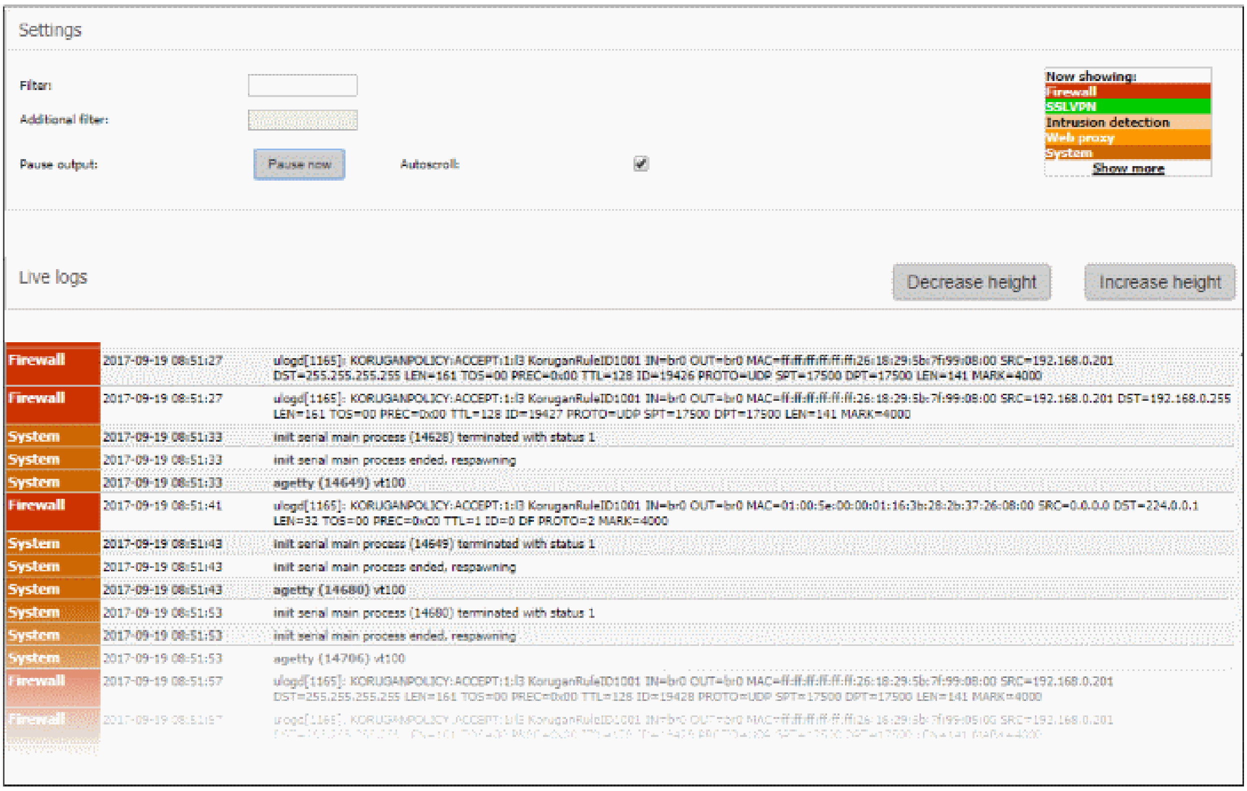
- **Firewall** - Log of connection attempts that were allowed or blocked by the Firewall. Click the '+' button to view details such as IP / Port / MAC address of the source and destination, the connection protocol and more.
- **Webserver** - List of web pages and elements that passed through the URL filter. See **Configuring URL and Content Filtering** for more details on configuring the URL filter.
- **SSLVPN** - Displays events relevant to SSL VPN connections.
- **Intrusion detection** - Displays events generated by the Intrusion Detection System (IDS) service.
- **Web proxy** - Displays events generated by the HTTP/HTTPS Proxy services.
- **System** - Shows events generated by changes to firewall settings and network configuration.

You can add or remove modules in the live log interface as required.

To view live logs

- Click 'Logs' > 'Live' on the left-hand menu
- Select the module(s) whose events you want to see.
- Click 'Show selected logs'.

The Live Log Viewer will open in a new window:



```
Firewall  2017-09-19 08:51:27  ulogd[1165]: KORUGANPOLICY:ACCEPT:1:l3 KoruganRuleID1001 IN=br0 OUT=br0 MAC=ff:ff:ff:ff:ff:ff:26:18:29:5b:7f:99:08:00 SRC=192.168.0.201
                               DST=255.255.255.255 LEN=161 TOS=00 PREC=0x00 TTL=128 ID=19426 PROTO=UDP SPT=17500 DPT=17500 LEN=141 MARK=4000
Firewall  2017-09-19 08:51:27  ulogd[1165]: KORUGANPOLICY:ACCEPT:1:l3 KoruganRuleID1001 IN=br0 OUT=br0 MAC=ff:ff:ff:ff:ff:ff:26:18:29:5b:7f:99:08:00 SRC=192.168.0.201 DST=192.168.0.255
                               LEN=161 TOS=00 PREC=0x00 TTL=128 ID=19427 PROTO=UDP SPT=17500 DPT=17500 LEN=141 MARK=4000
System    2017-09-19 08:51:33  init serial main process (14628) terminated with status 1
System    2017-09-19 08:51:33  init serial main process ended, respawning
System    2017-09-19 08:51:33  agetty (14649) vt100
Firewall  2017-09-19 08:51:41  ulogd[1165]: KORUGANPOLICY:ACCEPT:1:l3 KoruganRuleID1001 IN=br0 OUT=br0 MAC=01:00:5e:00:00:01:16:3b:28:2b:37:26:08:00 SRC=0.0.0.0 DST=224.0.0.1
                               LEN=32 TOS=00 PREC=0xC0 TTL=1 ID=0 DF PROTO=2 MARK=4000
System    2017-09-19 08:51:43  init serial main process (14649) terminated with status 1
System    2017-09-19 08:51:43  init serial main process ended, respawning
System    2017-09-19 08:51:43  agetty (14680) vt100
System    2017-09-19 08:51:53  init serial main process (14680) terminated with status 1
System    2017-09-19 08:51:53  init serial main process ended, respawning
System    2017-09-19 08:51:53  agetty (14706) vt100
Firewall  2017-09-19 08:51:57  ulogd[1165]: KORUGANPOLICY:ACCEPT:1:l3 KoruganRuleID1001 IN=br0 OUT=br0 MAC=ff:ff:ff:ff:ff:ff:26:18:29:5b:7f:99:08:00 SRC=192.168.0.201
                               DST=255.255.255.255 LEN=161 TOS=00 PREC=0x00 TTL=128 ID=19428 PROTO=UDP SPT=17500 DPT=17500 LEN=141 MARK=4000
Firewall  2017-09-19 08:51:57  ulogd[1165]: KORUGANPOLICY:ACCEPT:1:l3 KoruganRuleID1001 IN=br0 OUT=br0 MAC=ff:ff:ff:ff:ff:ff:26:18:29:5b:7f:99:08:00 SRC=192.168.0.201
                               [illegible]
```

- The 'Settings' pane at the top contains filter options and controls.
- Logs for all selected modules are shown in the lower pane.

Settings

The Settings area contains the options and controls for the following:

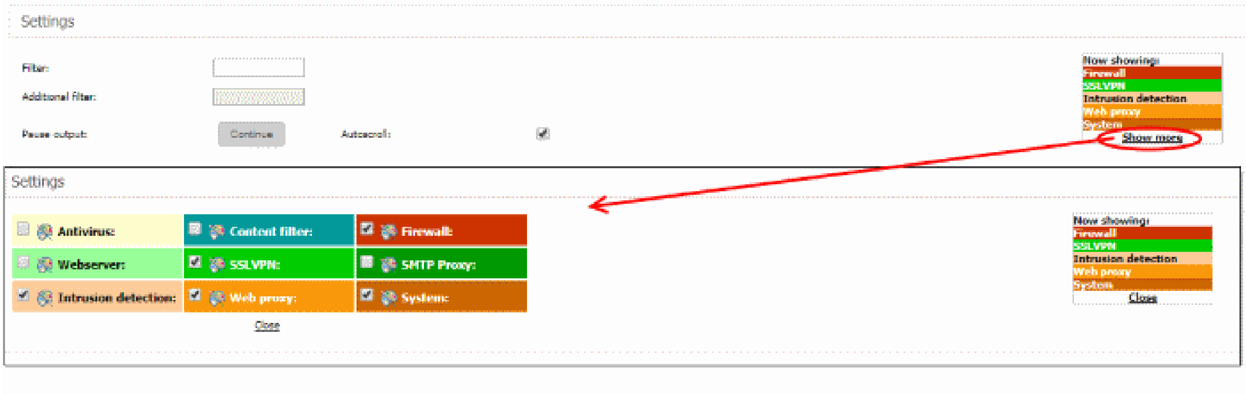
- **Select Log Modules**
- **Filter Log Entries**
- **Pause and Resume log updates**
- **Autoscroll settings**

Select Log Modules

The modules currently included in the stream are listed at the top right. Each module name is color-coded.

To add or remove modules to view the logs

- Click the 'Show More' link at the top right. A list of modules will be displayed.



Settings

Filter:

Additional filter:

Pause output: Continue Autoscroll: ☑

Now showing:
Firewall
SSLVPN
Intrusion detection
Web proxy
System
Show more

Settings

☐ Antivirus:	☐ Content filter:	☑ Firewall:
☐ Webserver:	☑ SSLVPN:	☐ SMTP Proxy:
☑ Intrusion detection:	☑ Web proxy:	☑ System:

Close

Now showing:
Firewall
SSLVPN
Intrusion detection
Web proxy
System
Close

- Select the modules for which you wish to view the live logs and deselect the modules for which you do not wish to view the live logs

The realtime log entries corresponding only to the selected modules are displayed in the lower pane.

Filter Log Entries

- Enter a keyword for the primary filter in the 'Filter' text field
- Optional. Fine-tune the filter by entering a second keyword in the 'Additional filter' field

The logs shown in the lower pane will automatically update according to your filter.

Pause and Resume log updates

- By default, the Live Log viewer is dynamically updated with the current events that are pertinent to the selected modules.
- Admins may want to temporarily stop the updates to analyze existing events.
- Click the 'Pause now' button to temporarily halt the stream..
- Click 'Continue' to resume updates.

Autoscroll settings

The dynamically updated live log viewer can automatically scroll upwards to show the chronologically added latest entries at the bottom of the list. If the autoscrolling is not enabled, the administrator can use the scroll bar at the right to move the list upwards to see the latest entries.

- To enable autoscrolling, select the 'Autoscroll' checkbox

Note: The 'Autoscroll' will be available only if the live log viewer is configured to sort the entries in chronological order, that is the latest entries added to the bottom of the list. If the live log viewer is configured to sort the entries in reverse chronological order by selecting the option 'Sort in reverse chronological order' from the Settings interface, the 'Autoscroll' option will not be available. See '**Configuring Log Settings**' for more details on configuring the log viewer.

Changing height of the Log Viewer

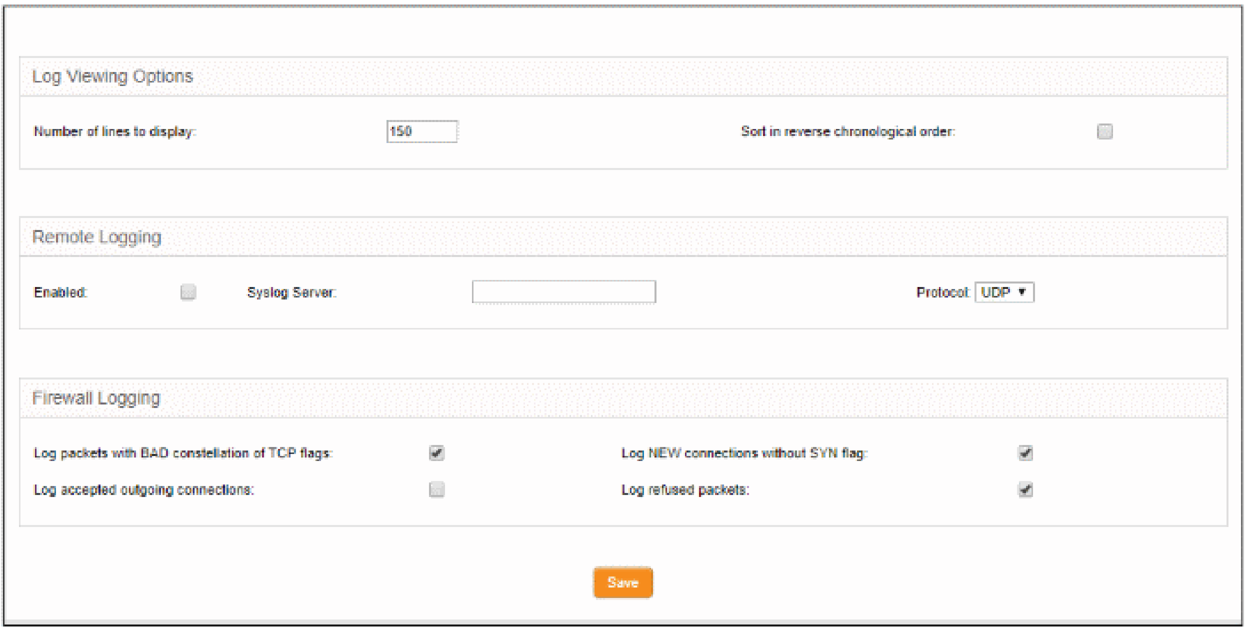
The Live Logs area displays the list of events pertaining to the selected modules and services. Each entry contains the log type, the precise date and time of the event and the message describing the event. The administrator can increase or decrease the height of the live log viewer.

- To increase the height of the log viewer in order to view large number of log entries at once, click 'Increase height' repeatedly. The height is increased by two entries for a single click.
- To reduce the height of the log viewer, click 'Decrease height'. The height is decreased by two entries for a single click.

11.2 Configuring Log Settings

The 'Log Settings' interface allows administrators to customize the log viewers of various modules.

- To open the 'Log Settings' interface, click 'Logs' > 'Settings' on the left menu:



Log Viewing Options

Number of lines to display: 150

Sort in reverse chronological order: □

Remote Logging

Enabled: □

Syslog Server:

Protocol: UDP ▾

Firewall Logging

Log packets with BAD constellation of TCP flags: ☑

Log NEW connections without SYN flag: ☑

Log accepted outgoing connections: □

Log refused packets: ☑

The interface contains three areas:

- **Log Viewing Options**
- **Remote Logging**
- **Firewall Logging**

Log Viewing Options

The 'Log Viewing Options' area allows the administrator to customize the log viewer screens of different DFW modules/services.

- Number of lines to display - Specify the number of log entries to be displayed in a single page in the log viewer
- Sort in reverse chronological order - The log entries are normally displayed in chronological order, that is the latest entries added to the bottom of the page On selecting this option, the entries will be sorted in reverse chronological order, that is the latest entries will be added to the top of each page.

Remote Logging

If the logs are to be posted on to a remote log server, the administrator can specify the remote server and the protocol to be used for the data transfer.

- Enabled - Select the checkbox to enable remote logging
- Syslog server -Specify the host name or the IP address of the remote logging server to which the logs are to be passed. Ensure that the server supports the latest IETF syslog protocol standards. If a remote syslog server is setup in the network by installing 'Dome Firewall Log Collector', specify the IP address or the hostname of the endpoint at which the log collector is installed.
- Protocol - Choose the data transfer protocol to be used for transferring the logs from the drop-down.

Tip: For Dome Firewall Log Collector, choose UDP as data transfer protocol.

Firewall Logging

The Firewall Logging area allows the administrator to specify the certain connection event types to be included in the Firewall Logs, in addition to the usually logged events.

- Select the event types from the options in this area:
  - Log packets with BAD constellation of TCP flags - Instructs the Firewall to include packets with all flags set, in the log.
  - Log NEW connections without SYN flag - Instructs the Firewall to include all the new connections without the synchronization flag, in the log.
  - Log accepted outgoing connections - Instructs the Firewall to include even the outgoing connections that pass the Firewall from the internal network zones, in the log.
  - Log refused packets - Instructs the Firewall to include even the details of the packets that were refused from the external sources, in the log.
- Click 'Save' for your configuration to take effect.

Appendix: Minimum Requirements for Software Installations

Dome Firewall is also available as software which can be installed on a PC:

- Dome Firewall Lite (**https://www.Dome Firewall.com/Dome Firewalllite.php**) - Free, feature limited version of Dome Firewall which can be installed on any PC
- Dome Firewall VM (**https://www.Dome Firewall.com/Dome Firewallvm.php**) - Fully featured version of Dome Firewall in VM format

To run one of the software versions, please ensure your PC meets the following minimum requirements:

- 1 x Intel or equivalent CPU
- 2 GB RAM
- 4 GB Storage
- 4 x 1 GbE NIC

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

The Comodo Threat Research Labs is a global team of IT security professionals, ethical hackers, computer scientists and engineers analyzing and filtering input from across the globe. The team analyzes millions of potential pieces of malware, phishing, spam or other malicious/unwanted files and emails every day, using the insights and findings to secure and protect its current customer base and the at-large public, enterprise and internet community.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets. With offices in the US, China, Turkey, India, Romania and Ukraine, Comodo secures the online and offline eco-systems of thousands of clients worldwide.

Comodo Security Solutions, Inc

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.888.266.6361

Tel : +1.703.581.6361

Email: **EnterpriseSolutions@Comodo.com**

For additional information on Comodo - visit **https://www.comodo.com**