COMODO
Creating Trust Online®

COMODO DOME
FIREWALL

Comodo One

Software Version 3.8

Dome Cloud Firewall Administrator Guide

Guide Version 1.1.120318

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1 Introduction to Dome Cloud Firewall

Comodo Dome Cloud Firewall is an enterprise class unified firewall solution for networks and provides a secure VPN service. Dome Cloud Firewall module is an integrated application in Comodo One and can be placed as gateway of Dome premium services such as Dome Data Protection.

Key Features

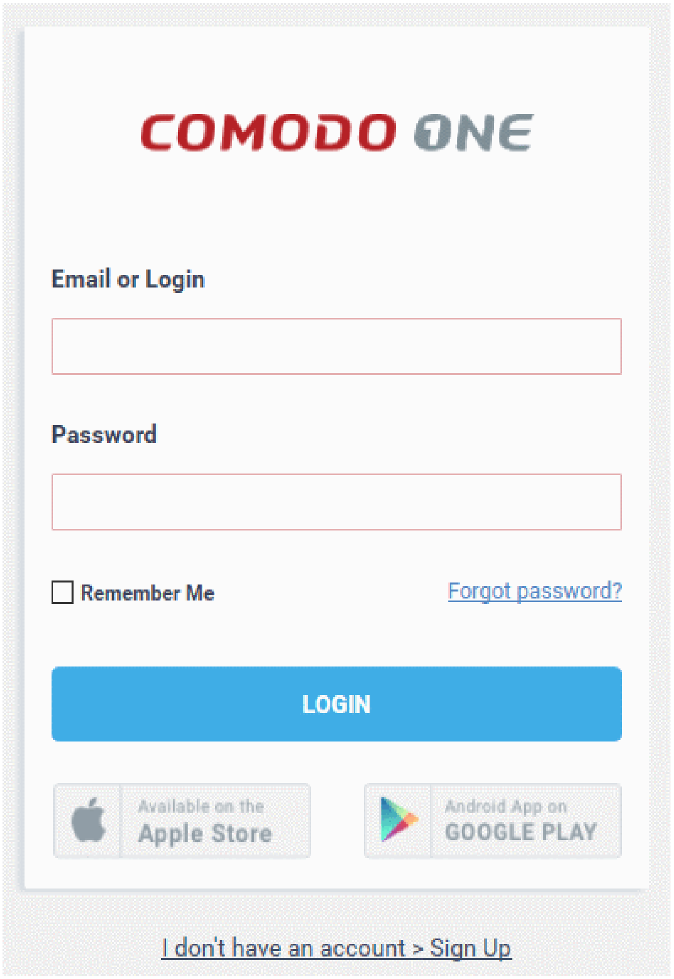
- Stateful Packet Inspection Firewall
- Source, Destination, IP, Service, Port and Schedule Based Rule Management
- VPN Firewall
- Virtual IP, DNAT,SNAT and ICAP Support
- IPSec, L2TP, SSLVPN Support
- Client-to-site and Site-to-Site VPN Tunnels
- Logs and Monitoring
- Add-on Module for Dome Premium

Guide Structure

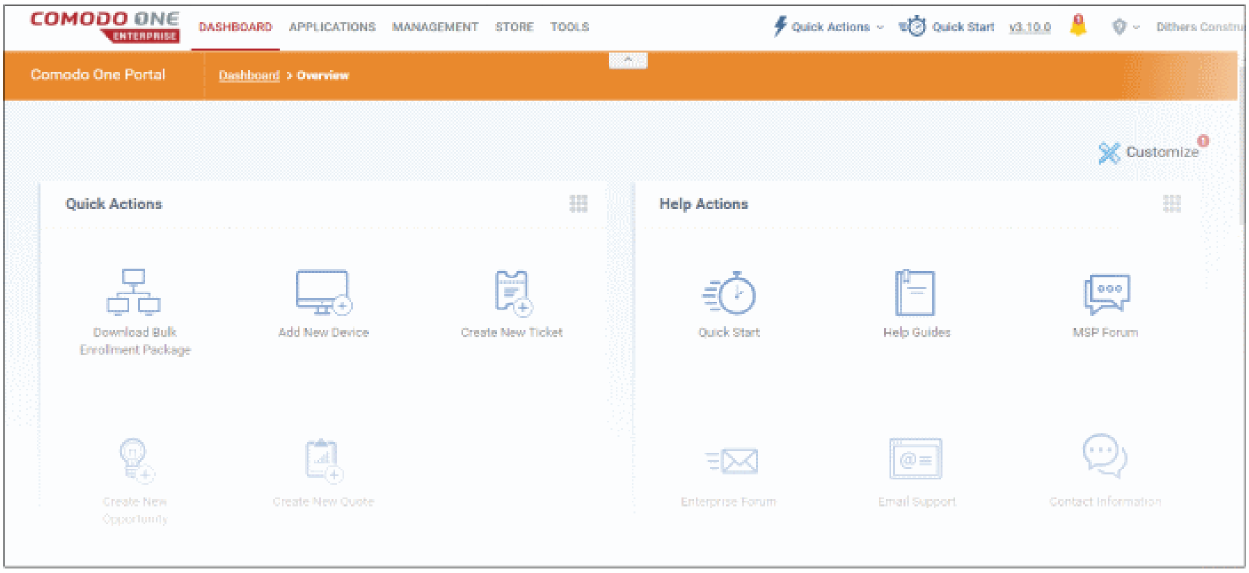
This guide is intended to take you through the configuration and use of Comodo Dome Cloud Firewall.

1.1 Logging-in to the Dome Cloud Firewall Module

To access the Dome Cloud Firewall module, login to C1 with your user name and password at **https://one.comodo.com/app/login**.

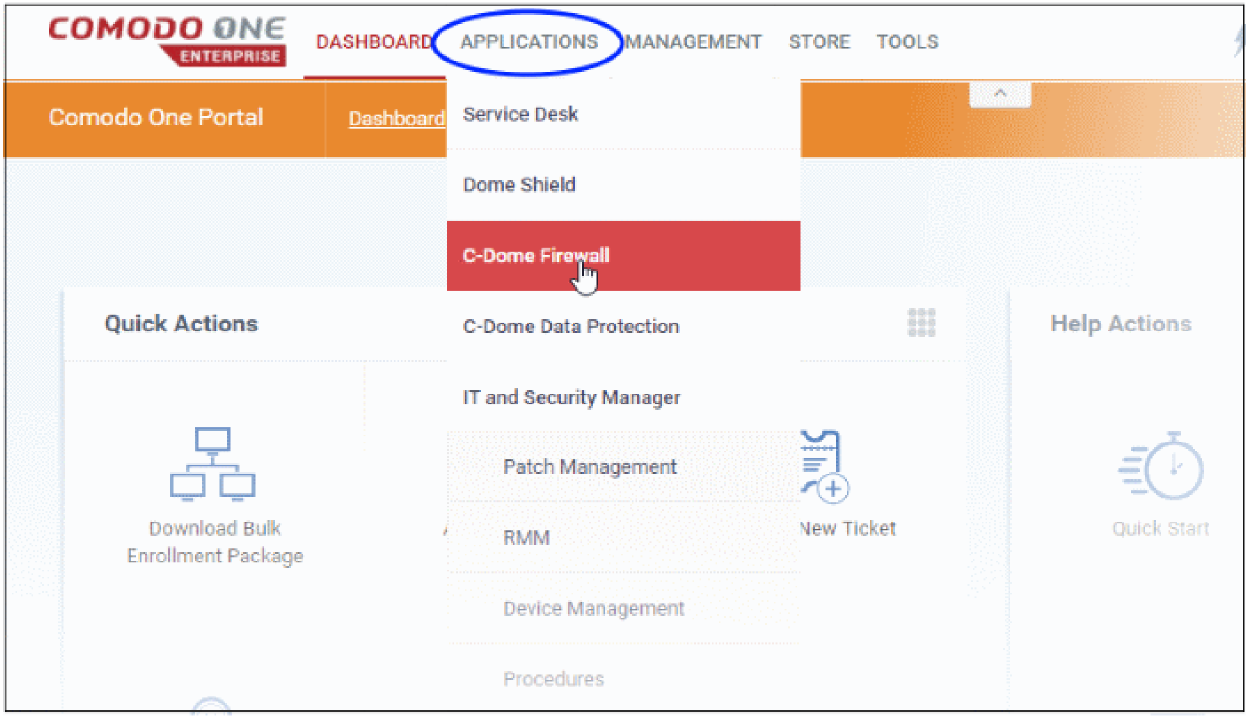

COMODO ONE
Email or Login
Password
Remember Me
Forgot password?
LOGIN
Available on the Apple Store
Android App on GOOGLE PLAY
I don't have an account > Sign Up

The C1 dashboard will be displayed.



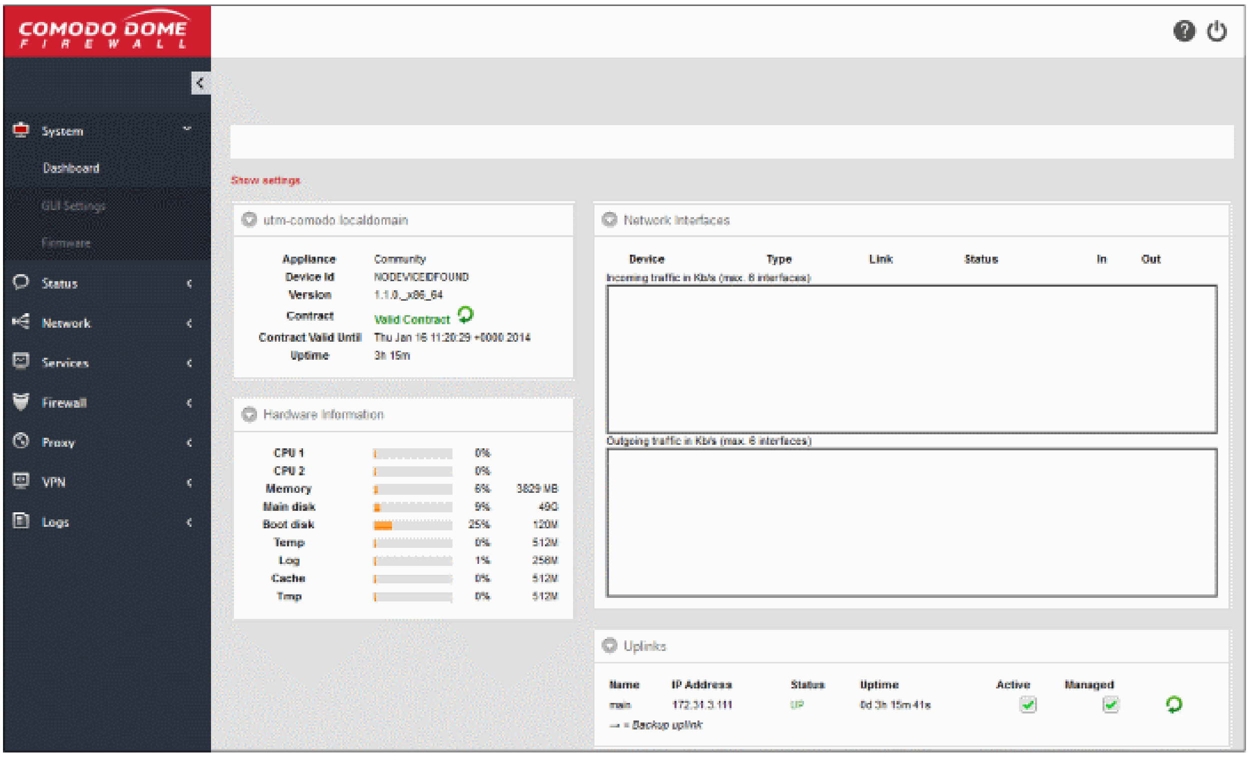
To open the Dome Cloud Firewall module

- Click 'Applications' at the top then click 'Dome Clud Firewall'
- Alternatively, click 'All Licensed Applications' under 'Applications', then click 'Open Module' in the 'Dome Clud Firewall' tile.



Note: You should have configured the Dome Cloud Firewall URL details in the **Settings** tab under 'Management' > 'Applications'. Information about this will be shown at the end of product sign up process. The service URL will be mailed to your email address when ready.

By default, the Dome Cloud Firewall 'Dashboard' screen will be displayed.



utm-comodo.localdomain

Appliance	Community
Device Id	NODEVICEIDFOUND
Version	1.1.0._x86_64
Contract	Valid Contract
Contract Valid Until	Thu Jan 16 11:20:29 +0000 2014
Uptime	3h 15m

Hardware Information

CPU 1	0%	
CPU 2	0%	
Memory	6%	3829 MB
Main disk	9%	49G
Boot disk	25%	120M
Temp	0%	512M
Log	1%	256M
Cache	0%	512M
Tmp	0%	512M

Network Interfaces

Device	Type	Link	Status	In	Out

Incoming traffic in Kb/s (max. 6 interfaces)

Outgoing traffic in Kb/s (max. 6 interfaces)

Uplinks

Name	IP Address	Status	Uptime	Active	Managed
main	172.31.3.111	UP	0d 3h 15m 41s	☑	☑

→ = Backup uplink

1.2 Getting Started

The first step is to configure your network clients to work with the Dome Cloud Firewall service. There are two ways to connect to Dome Cloud Firewall:

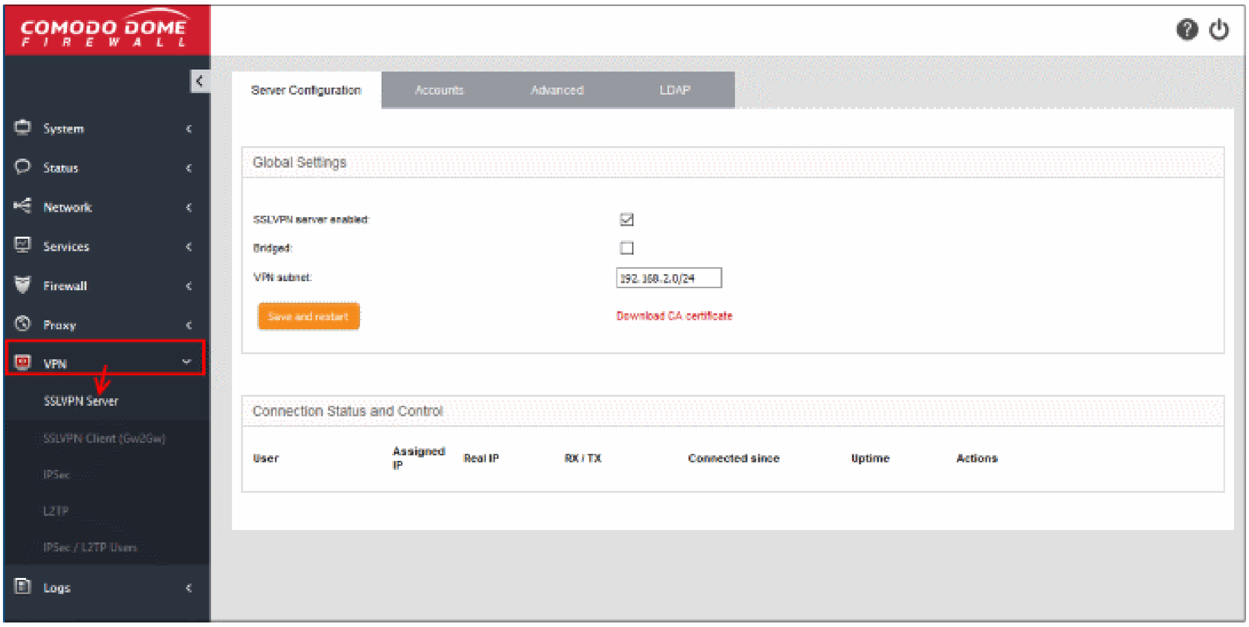
- Client to Site VPN
- Site to Site VPN

Client to Site VPN

In this method, all users/clients must be configured individually in order to route traffic via Dome Cloud Firewall. The advantage in this method is the clients will always be routed via Dome Cloud Firewall irrespective of their location.

To configure a client to connect to Dome Cloud Firewall

- Click 'VPN' on the left then 'SSLVPN Server'



SSLVPN server enabled: ☑

Bridged: □

VPN subnet: 192.168.2.0/24

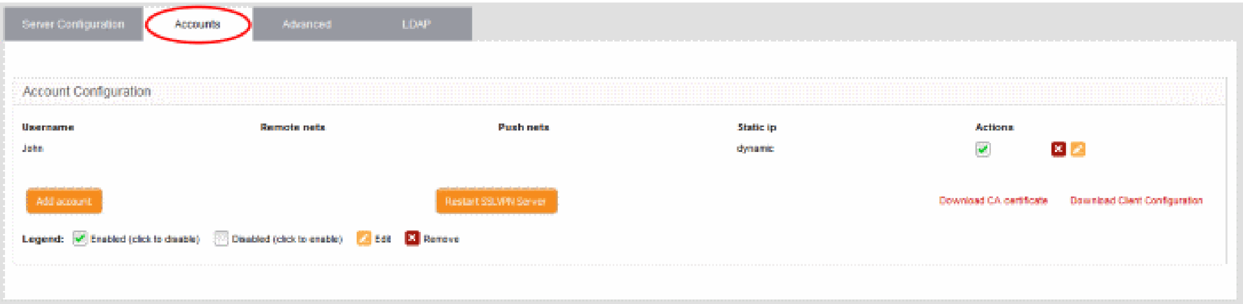
User	Assigned IP	Real IP	RX / TX	Connected since	Uptime	Actions

In the Server Configuration screen, configure the following:

- SSLVPN server enabled - Select the checkbox to enable the SSLVPN server
- Bridged - Select the checkbox if you wish to run the server in bridged mode.
- Bridge to - Choose the local network zone to which the server is to be bridged. This option will appear only if you chose to run the server in bridged mode in the previous option.
- Dynamic IP pool start address and Dynamic IP pool end address - Enter the first and last address of the IP address pool from which the IP addresses are to be dynamically assigned to the clients that are connecting to the server. All the traffic from these IP addresses will pass through the VPN firewall, if enabled.

- Click 'Save and Restart'. The SSL VPN server service will be restarted for your settings to take effect.
- To download the server certificate for deployment to the clients, click 'Download CA certificate'. The certificate can also be downloaded from the 'Accounts' interface.

Next, click the 'Accounts' tab:



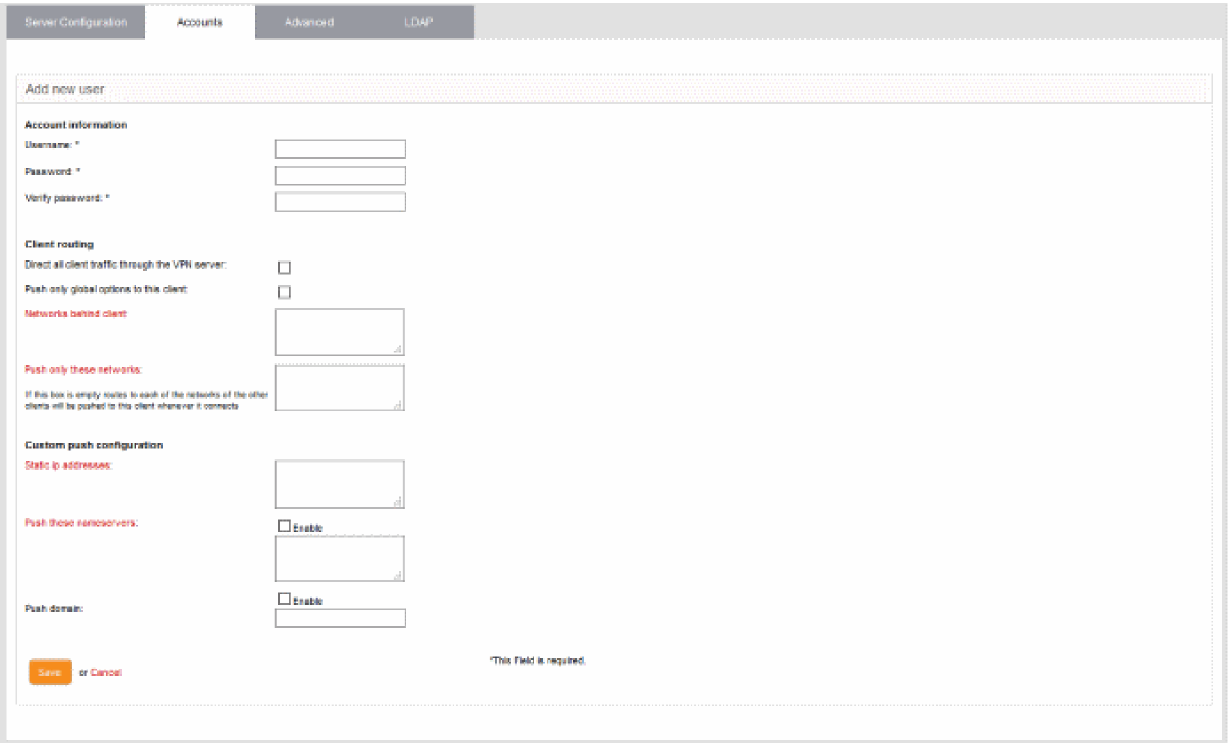
Account Configuration

Username	Remote nets	Push nets	Static ip	Actions
John			dynamic	☑ ☒ ✎

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

To add a new user account

- Click the 'Add account' button. The 'Add new user' pane for adding a new domain will open.



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: □

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 for the user account. These credentials are to be entered to the SSL VPN client for authenticating itself 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 the routing traffic for the client

- Direct all client traffic through the VPN server - Select this option for all the incoming and outgoing traffic pertaining to the client to pass through the VPN server
- Push only global options to this client - Instructs the server to push only the network routes, name servers and domains specified under the Global Push Options under the 'Advanced' settings tab.
- Networks behind client - Enter the network subnet address of the VPN gateway server for the client to connect to VPN.

  - Push only these networks - If you wish to push the routes of only selected networks to the client, then enter the network/subnet addresses of the networks. If you wish to push the routes of networks of all the other clients, leave this field blank.

Custom push configuration

  - Static ip addresses - If you wish to assign static IP addresses for the clients using this account, enter the IP addresses in CIDR format. To avoid IP address clashes, it is recommended to specify the static IP addresses outside the Dynamic IP address pool specified under the 'Server Configuration' tab.
  - 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 the clients using this account, to identify the servers and network resources in the VPN network, select the 'Enable' checkbox and enter the domain name in the text box.

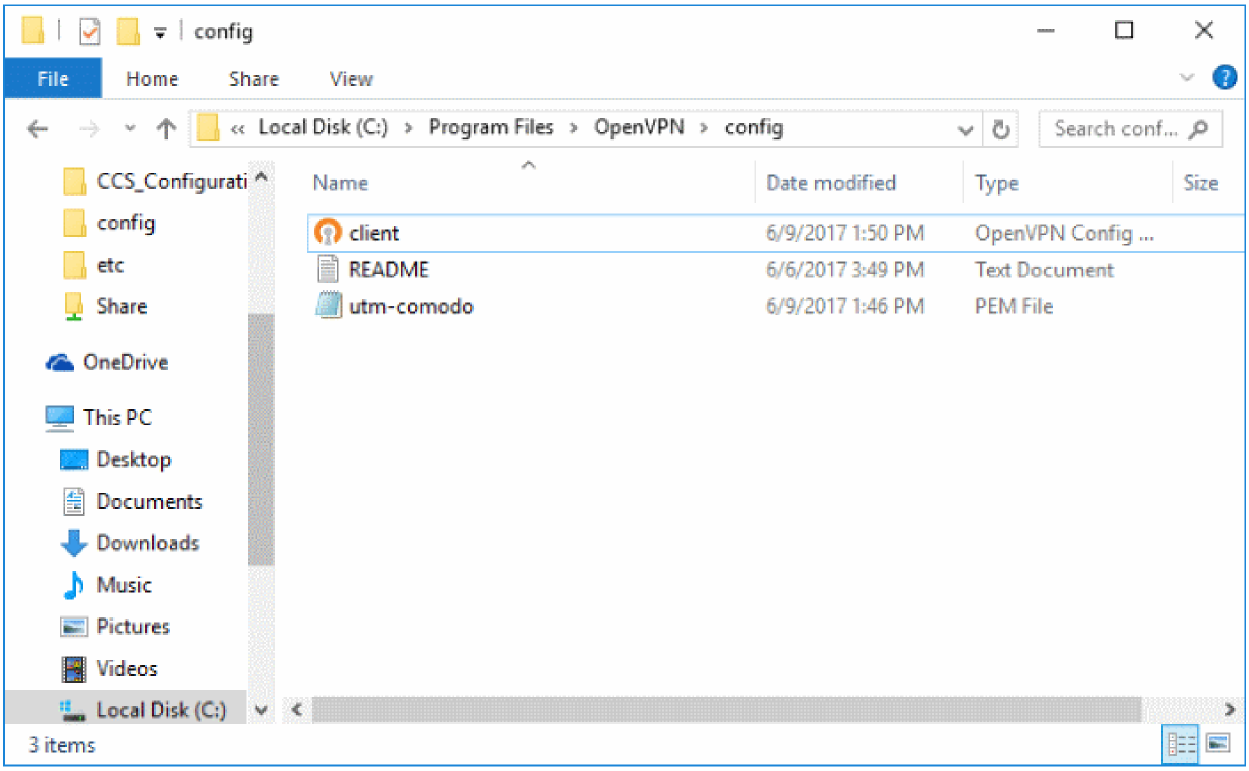
- Click 'Save'. The account will be added to the list of accounts. The account will be activated enabling the clients to connect to the server only after the next restart of the SSL VPN server.
- Click 'Restart SSL VPN server' to instantly restart the server.

Download the server certificate and the SSL VPN client configuration file from the 'Accounts' interface. The server certificate type for authentication can be configured under '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.

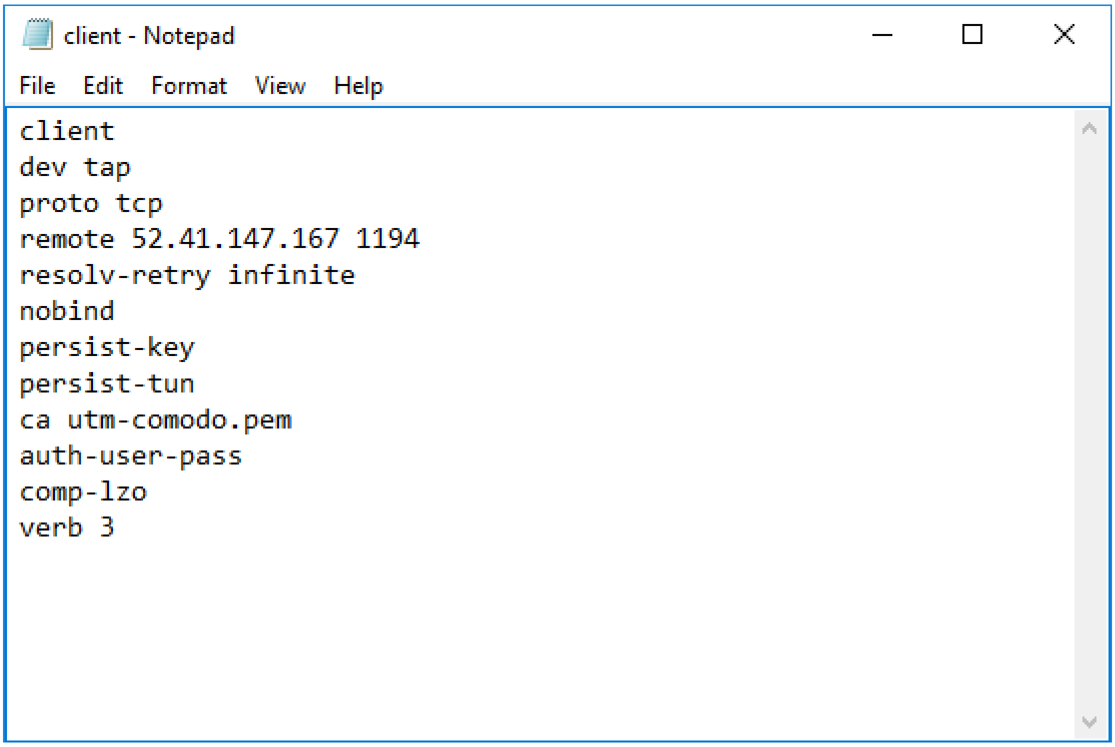
Next, transfer the certificate and the configuration file to the client. In order to connect for the client to connect to Dome Cloud Firewall, download and install openvpn client. You can download the client from **https://openvpn.net/index.php/open-source/downloads.html**

- After installing the OpenVPN GUI client, 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.



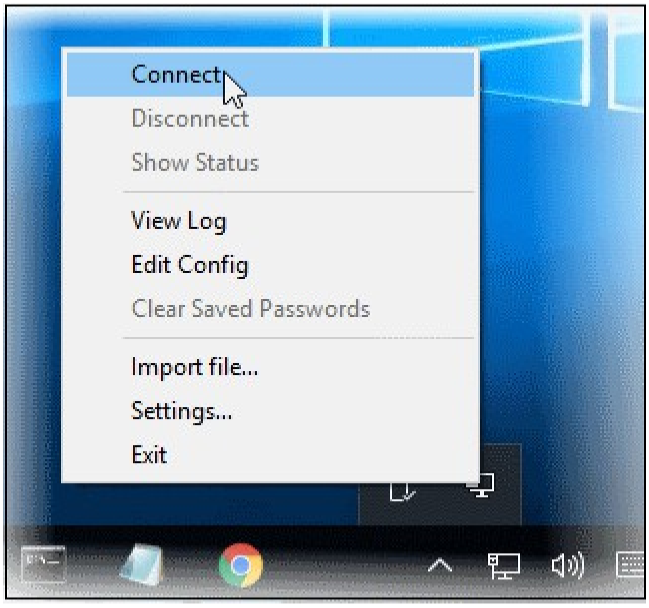
Name	Date modified	Type	Size
client	6/9/2017 1:50 PM	OpenVPN Config ...	
README	6/6/2017 3:49 PM	Text Document	
utm-comodo	6/9/2017 1:46 PM	PEM File	

- Open the configuration file and make sure the parameters are as shown below:

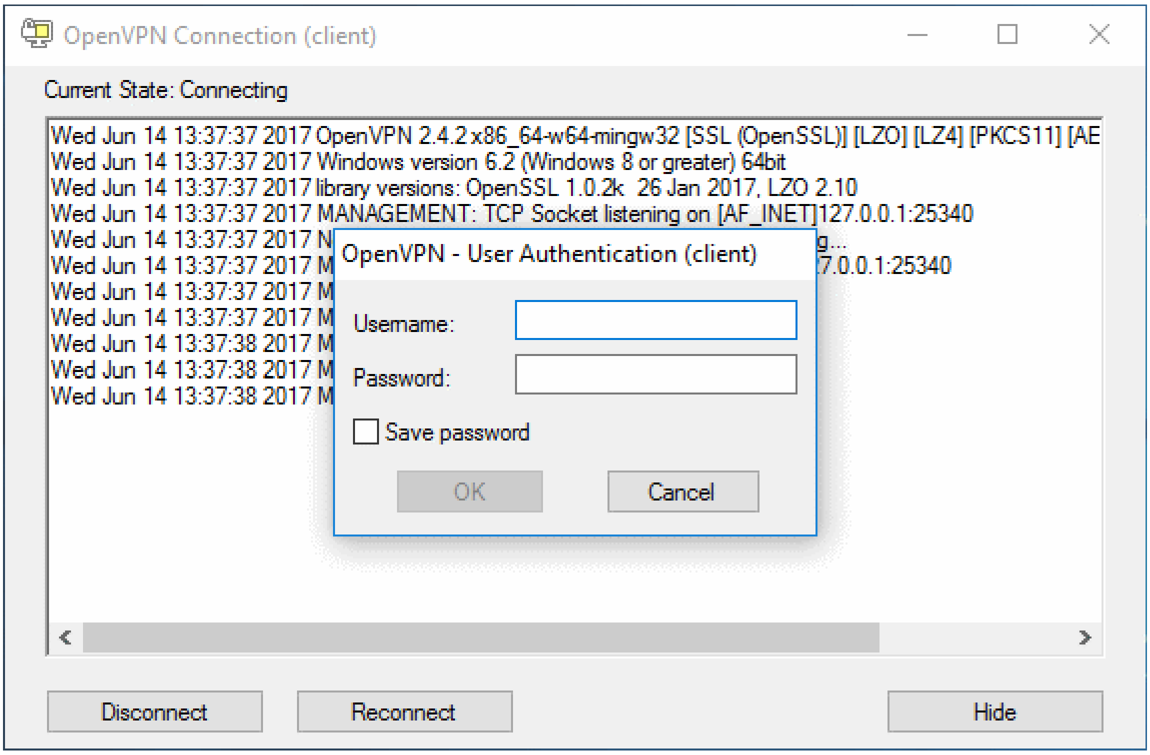


```
client
dev tap
proto tcp
remote 52.41.147.167 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca utm-comodo.pem
auth-user-pass
comp-lzo
verb 3
```

- 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 DCF 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 DCF, right-click the OpenVPN GUI icon in the task bar then 'Connect'.



The connection process will start and the user authentication should be provided.



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
```

OpenVPN - User Authentication (client)

Username:

Password:

□ Save password

- Enter the credentials in the 'Username' and 'Password' fields and click 'OK'.
- That's it, the client will be connected to Dome Cloud Firewall and can be viewed in SSLVPN Server > Server Configuration tab under 'Connection Status and Control' pane.

See '**SSL VPN Server**' and '**Configuring Clients to Connect to Dome Cloud Firewall**' for more details.

Site to Site VPN

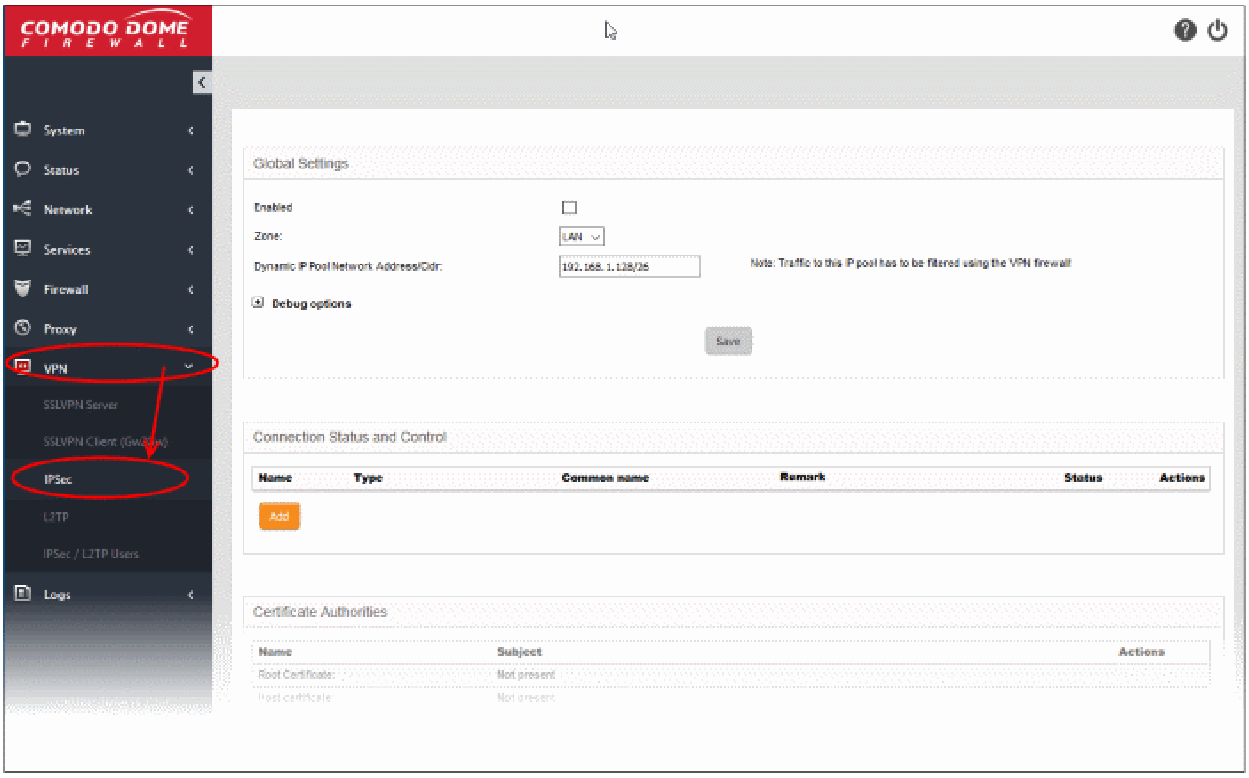
In this method, a network is configured to connect to Dome Cloud Firewall. Once done, all the clients behind the network will be routed via Dome Cloud Firewall but one disadvantage here is any client (roaming device) leaving the office network will not be routed via Dome Cloud Firewall. These roaming agents if required to connect to internet via Dome Cloud Firewall then they have to be routed via the office network.

You can use a router that supports VPN or a local firewall to create a virtual private network between that and Dome CF.

To configure a network to connect to Dome Cloud Firewall

Enable VPN tunnel at Dome Cloud Firewall

- Click 'VPN' on the left then 'IPSec'



Global Settings

Enabled □

Zone: LAN

Dynamic IP Pool Network Address/Cidr: 192.168.1.128/26

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

Certificate Authorities

Name	Subject	Actions
Root Certificate:	Not present	
Host certificate:	Not present	

In the 'Global Settings' area:

- Enabled - Select the checkbox to enable the IPsec VPN service
- Zone - Choose the network zone to allow networks to access Dome CF through the IPsec VPN
- Dynamic IP pool network address/cidr - Specify the IP addresses for dynamic assignment to the clients in CIDR notation

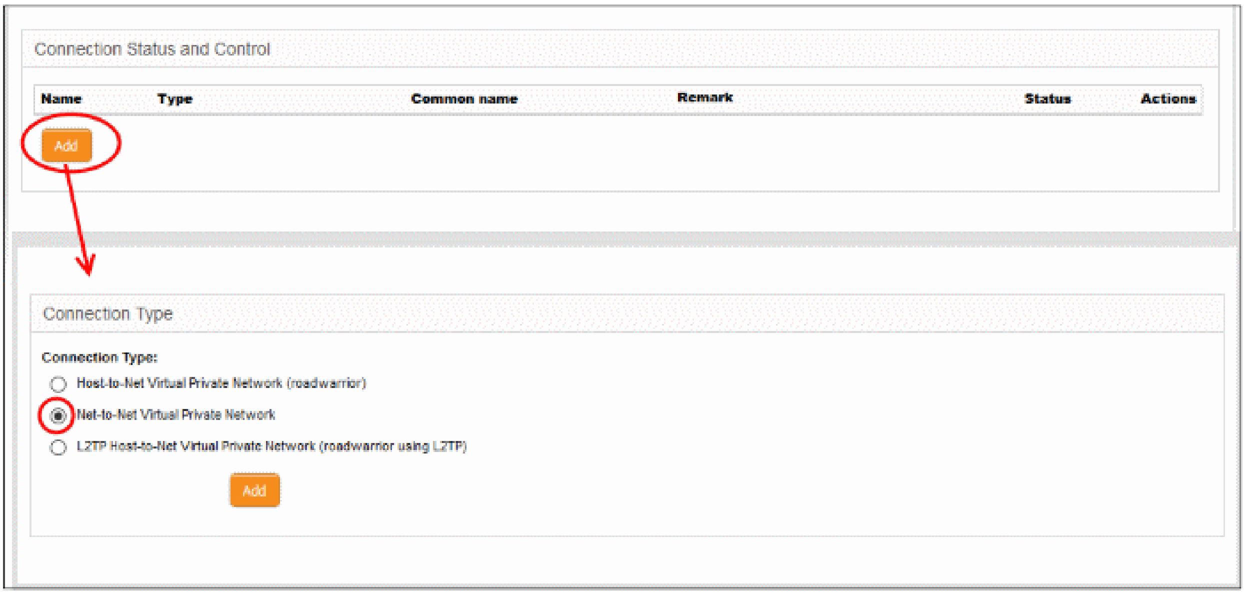
- Click 'Save' for your settings to take effect

In the 'Certificate Authorities' area:

- Click 'Generate root/host certificate' to generate a new certificate or upload an existing certificate. The certificate is used for authentication purpose between Dome CF and your router/firewall at your premises. You can also use a pre-shared key for authentication if you do not want certificate authentication option. The pre-shared key option is available in the 'Connection Configuration' screen.

In the 'Connection Status and Control' area:

- Click 'Add' to create a new tunnel
- Select 'Net-to-Net Virtual Private Network' in the next screen 'Connection Type'



Connection Status and Control

Name	Type	Common name	Remark	Status	Actions

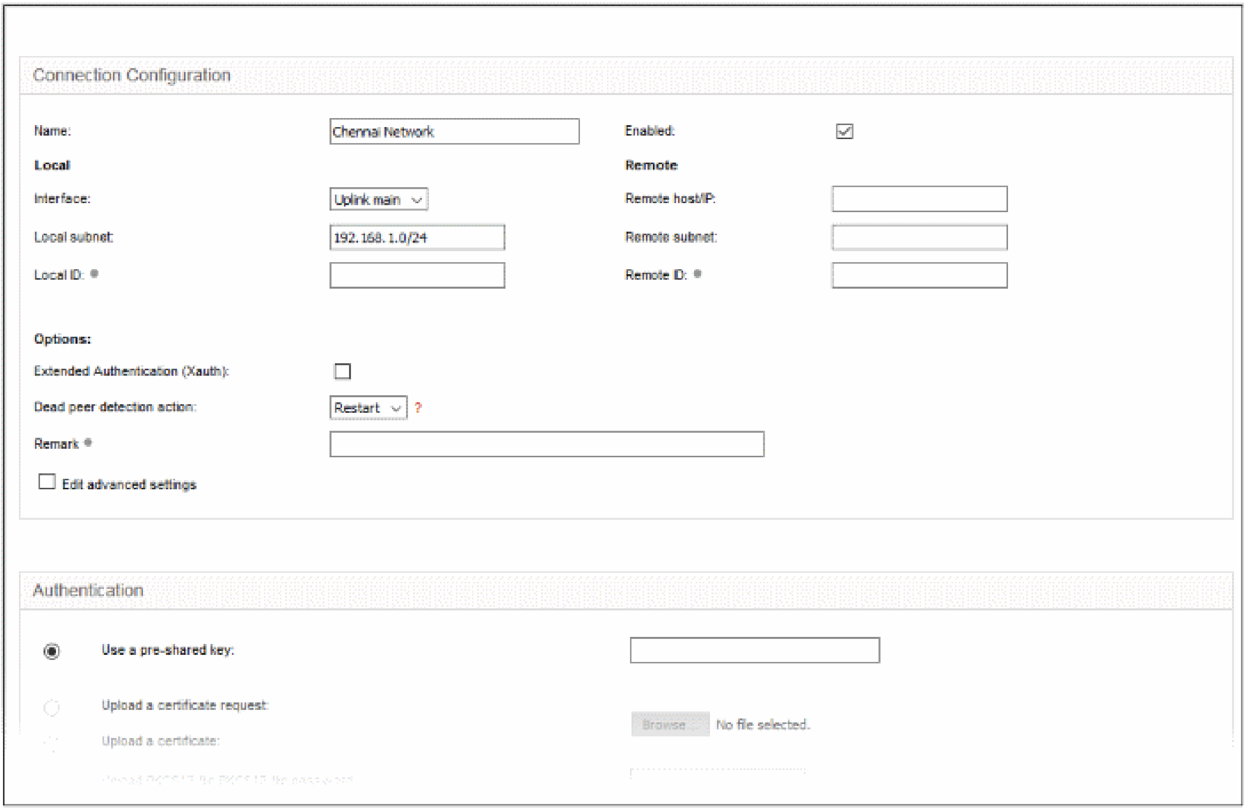
Connection Type

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)

- Click 'Add'

The 'Connection Configuration' interface will be displayed:



Connection Configuration

Name:	Chennai Network	Enabled:	☑
Local		**Remote**	
Interface:	Uplink main	Remote host/IP:	
Local subnet:	192.168.1.0/24	Remote subnet:	
Local ID: *		Remote ID: *	

Options:

Extended Authentication (Xauth): □
Dead peer detection action: Restart ?
Remark *
□ Edit advanced settings

Authentication

● Use a pre-shared key:
○ Upload a certificate request: Browse... No file selected.
○ Upload a certificate:
Upload PKCS12 file PKCS12 file password

- Name - Enter a name to identify the connection tunnel
- Enabled - Select this checkbox for the tunnel to be enabled upon creation.

Local

- Interface - Choose the internet interface for this connection.
- Local Subnet – Edit the local subnet if necessary
- 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 that is to be connected to Dome CF.
  - Remote subnet - Specify the sub network of the external network that can connect through the tunnel.
  - Remote ID - Enter an identification string for the local network.

Authentication

  - Select the authentication method. For example here we are using the pre-shared key.
- Click 'Save' to complete the tunnel setup in Dome CF.

Enable VPN tunnel at your site

In order for the connection to be established between your network and Dome CF, the same IPSec VPN configuration has to be done at the network router, firewall or gateway.

The settings in the device may vary but the main configuration should be the same at both ends. Important settings to be configured is given below:

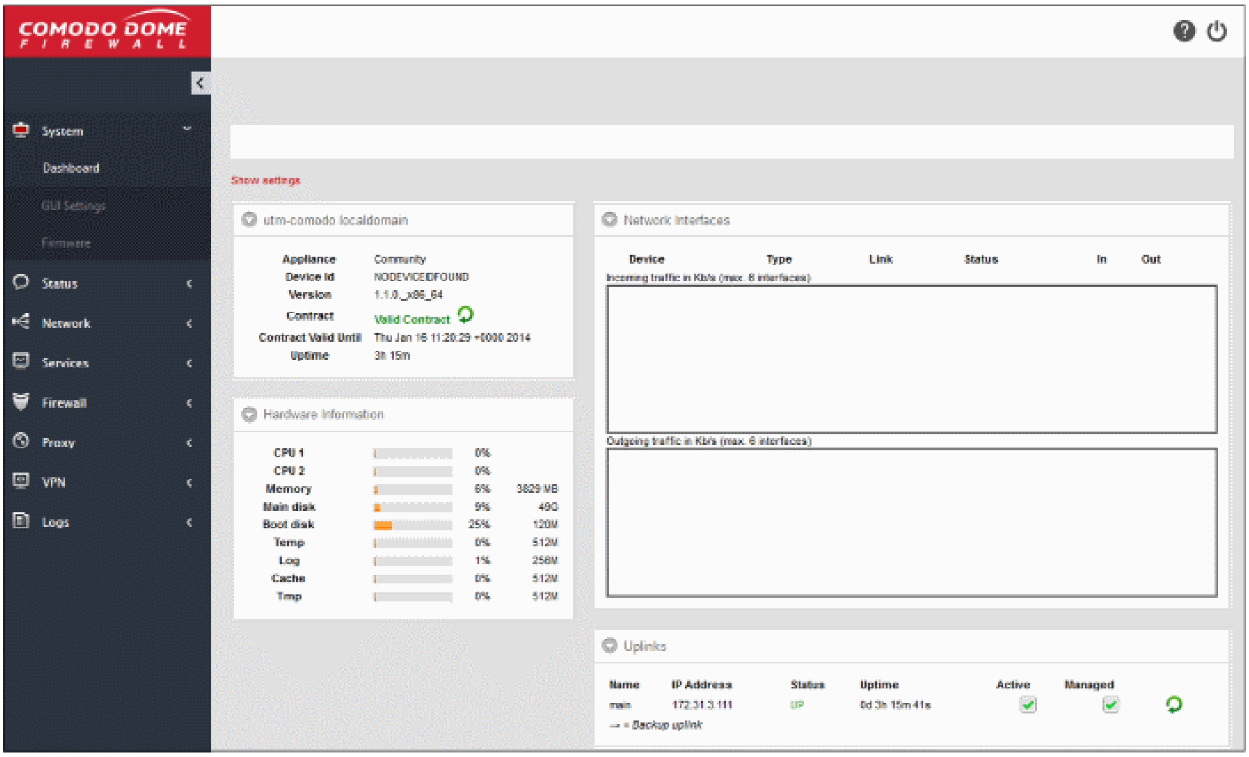
  - Select IPSec under VPN
  - Provide the public or hostname of the Dome Cloud Firewall in the 'Remote host / IP field'
  - Edit the local subnet field, if necessary
  - In the 'Remote Subnet' field, enter the parameters of 'Local Subnet' that you provided in Dome CF
  - Configure the authentication method that you selected in Dome CF. If you have chosen pre-shared key, provide the same key here.
- Click 'Save' to complete the tunnel setup in your network router, firewall or gateway.

Next, test the VPN connectivity between your network and Dome Cloud Firewall. If you need more help with this, please write to **c1-support@comodo.com**

See '**IPsec Configuration**' section for more details.

2 The Main Interface

The Dome Cloud Firewall dashboard provides 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	Community
Device Id	NODEVICEIDFOUND
Version	1.1.0._x86_64
Contract	Valid Contract
Contract Valid Until	Thu Jan 16 11:20:29 +0000 2014
Uptime	3h 15m

Hardware Information

CPU 1	0%	
CPU 2	0%	
Memory	6%	3829 MB
Main disk	9%	49G
Boot disk	25%	120M
Temp	0%	512M
Log	1%	256M
Cache	0%	512M
Tmp	0%	512M

Network Interfaces

Device	Type	Link	Status	In	Out

Incoming traffic in Kb/s (max. 6 interfaces)

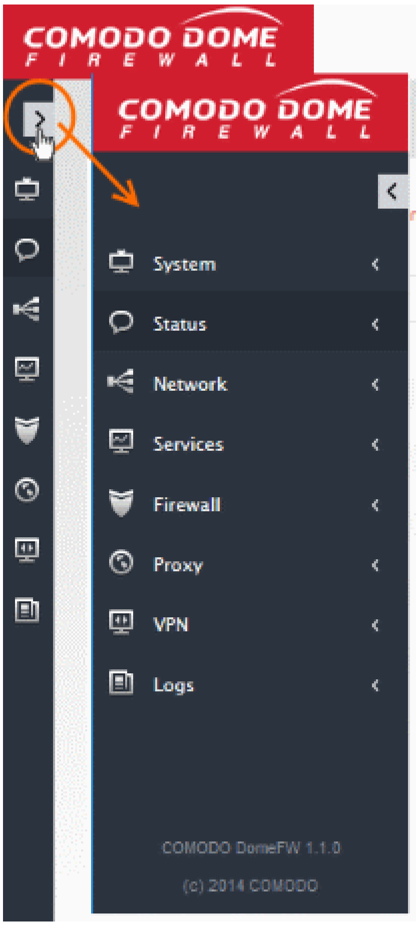
Outgoing traffic in Kb/s (max. 6 interfaces)

Uplinks

Name	IP Address	Status	Uptime	Active	Managed
main	172.31.3.111	UP	0d 3h 15m 41s	☑	☑

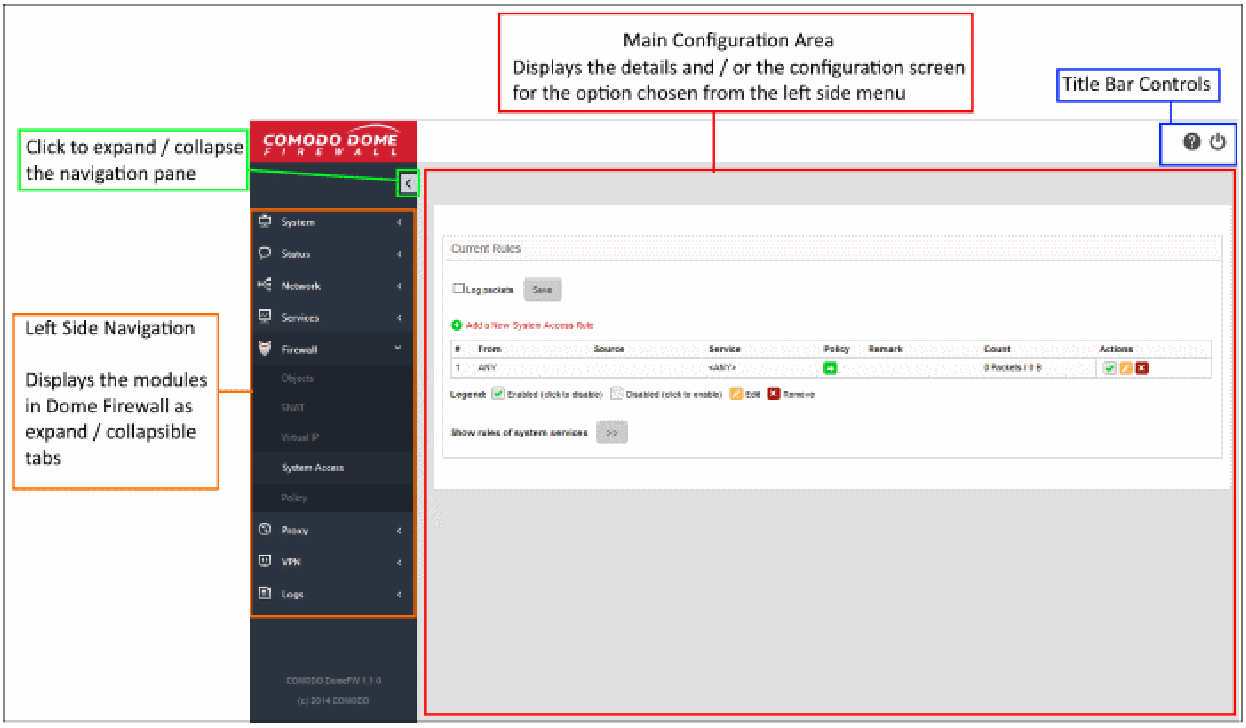
→ = Backup uplink

Dome CF application menus are on the the left of the interface. Click on a menu to expand/collapse and access its sub-menus. Click the arrow at top ‹ to expand / collapse the side menu bar. The following table is a quick overview of the modules:



- **System** - View dashboard, CF version details and configure interface language settings.
- **Status** - View Dome CF status data such as system status, network status, SSL VPN connections and more.
- **Network** – View .the number of interfaces configured for your account.
- **Services** - Configure ICAP services.
- **Firewall** - Configure firewall and apply rules for controlling inbound and outbound traffic to/from the network.
- **Proxy** - Configure proxy servers for services like HTTP/HTTPS proxy services.
- **VPN** - Configure SSLVPN server, SSLVPN client, IPsec-based VPN tunnels and L2TP connections.
- **Logs** - View logs for system events and firewall. You can also configure syslog servers for remote logging.

The user-friendly graphical interface of the administrative console provides easy access to the information and configuration screens of all Dome CF features with the LHS Navigation design.


Main Configuration Area
Displays the details and / or the configuration screen for the option chosen from the left side menu
Title Bar Controls
Click to expand / collapse the navigation pane
Left Side Navigation
Displays the modules in Dome Firewall as expand / collapsible tabs
COMODO DOME FIREWALL
System
Status
Network
Services
Firewall
Objects
SNAT
Virtual IP
System Access
Policy
Proxy
VPN
Logs
COMODO DomeFW 1.1.0
(c) 2014 COMODO

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

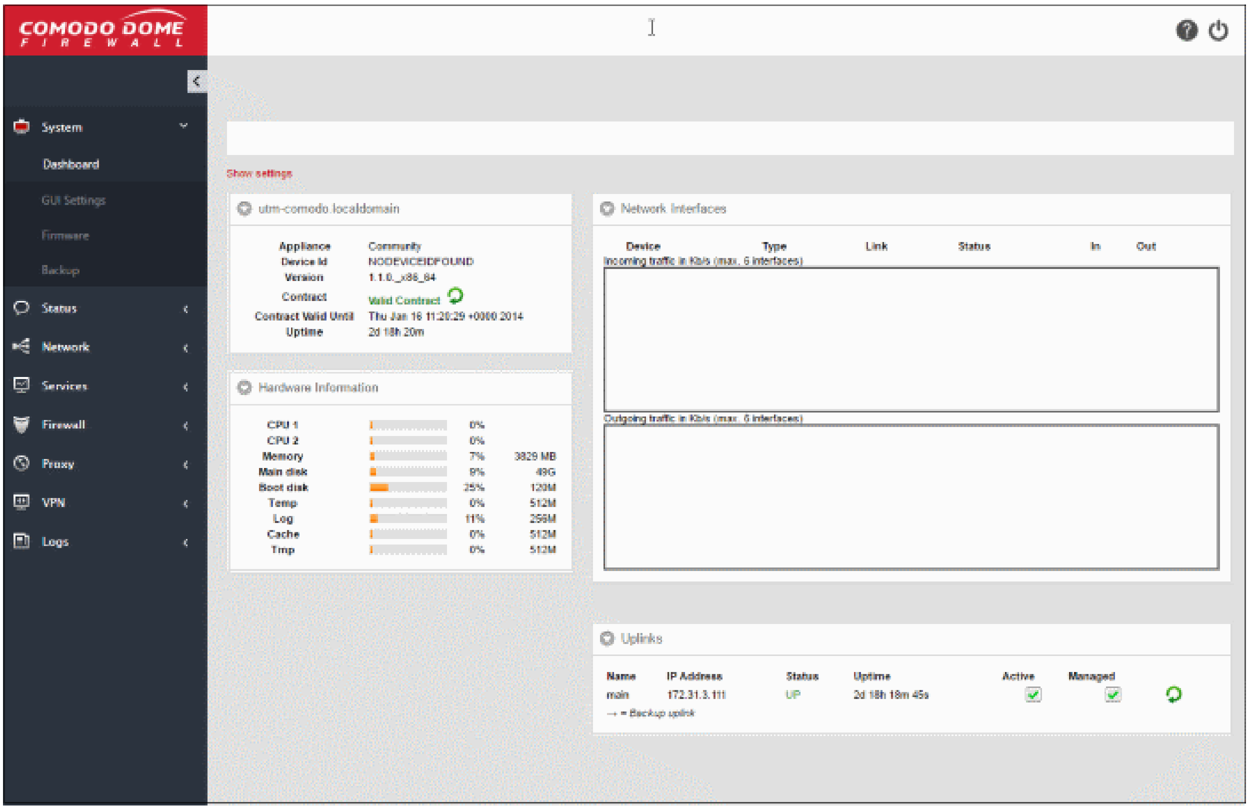
Show rules of system services >>

- **The Left Navigation Menu -** The left hand navigation displays Dome Cloud Firewall modules as tabs. Clicking on a module opens sub-tabs to open different configuration screens of the selected module.
- **The Main Configuration Area -** The main configuration area displays information pertinent to the tab selected on the left.
- **The Title Bar Controls -** The title bar contains controls for:
  - Logout - The administrator can logout of the Firewall administrator console
  - Help - Opens the online help page of Dome Cloud Firewall corresponding to the currently open configuration screen.
- **Version and Copyright Information -** Version number and copyright information of the application is displayed at the bottom left of the interface.

3 The Dashboard

The dashboard provides a at-a-glance summary of the current running status, health and usage of the CF.

The dashboard is displayed by default whenever you login to the administrative interface. To access the dashboard from a different configuration screen, select 'System' > 'Dashboard' from the left-hand navigation.



utm-comodo.localdomain

Appliance	Community
Device Id	NODEVICEIDFOUND
Version	1.1.0._x86_64
Contract	Valid Contract
Contract Valid Until	Thu Jan 16 11:20:29 +0000 2014
Uptime	2d 18h 20m

Hardware Information

CPU 1	0%	
CPU 2	0%	
Memory	7%	3829 MB
Main disk	9%	49G
Boot disk	25%	120M
Temp	0%	512M
Log	11%	256M
Cache	0%	512M
Tmp	0%	512M

Network Interfaces

Device	Type	Link	Status	In	Out

Incoming traffic in Kb/s (max. 6 interfaces)

Outgoing traffic in Kb/s (max. 6 interfaces)

Uplinks

Name	IP Address	Status	Uptime	Active	Managed
main	172.31.3.111	UP	2d 18h 18m 45s	☑	☑

→ = Backup uplink

The dashboard displays the front panel of the device model and tiles which provide details on current hardware resource use, system information, currently running services, network information and uplink status.

- The device model panel indicates the connection status of the uplink, DMZ, LAN and WiFi network zone interface devices.
- Each tile can be expanded or collapsed by clicking the down arrow at the top left of it.
- The tiles can be positioned as per the desired lay out by just dragging and dropping them to the desired position.
- The plugins which control these panes can be configured by clicking the 'Show Settings' link at the top left

of the interface. For more details on configuring the tiles, refer to the section **Configuring the Dashboard**

Hardware Information

The Hardware information tile shows the hardware resource usage statistics of Dome Cloud Firewall.

- CPU x: The usage of the CPU resources. In a multi-processor server, the load on each CPU is indicated separately, with the suffix 'x' denoting the CPU number.
- Memory - The usage of the system memory.
- Main disk - Usage of the root partition of the main disk for your account. The disk usage should not exceed 95%.
- Boot disk - Usage of the boot partition of the hard disk for your account. The disk usage should not exceed 95%.
- Temp - Usage of disk space in /tmp partition, allotted for temporary files for your account. The Temp space usage should not exceed 95%.
- Log - Usage of disk space allotted for log files for your account. 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 allotted for your account.
- Tmp - Usage of disk space by .tmp files created in Dome Cloud Firewall.

System Information

The System Information tile shows the host name and the network domain to which the Dome CF is connected in its title bar. The tile displays the general information about the appliance connected.

- Appliance - Indicates the DCF type
- Device ID - The identification number of DCF
- Version - The version number of the DCF hosted for your account.
- Contract - Indicates whether the DCF license is valid. Clicking the circled arrow refreshes the information.
- Contract Valid Until - Expiry date of the license
- Uptime - Indicates the period for which DCF is up since the last reboot

Services

The Services tile shows the On/Off status and statistics of the services like Intrusion Detection, mail filters currently loaded to the appliance.

- Clicking on the Live Log in the title bar opens the **Realtime logs** screen.
- Clicking on the service name expands the pane below it showing the detailed statistics.

The services displayed are:

- Attacks Logged - Shows the number of attacks logged by the UTM
- 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

The network interfaces tile shows statistics of the network interface devices configured for your CF account and realtime updated graphical charts of incoming and outgoing traffic through these devices.

The table in the upper half of the tile displays realtime statics of each network device.

Network Interfaces - Column Descriptions

Column Header	Description
Device	The name of the network interface device. The font color in which the name is displayed indicates the network zone to which the device belongs: Red - External network like WAN, for Internet connection Green - Local network to which workstations are connected, like LAN
Type	The connection type of the device
Link	Link status of the device
Status	Running status of the device
In/Out	Incoming/Outgoing traffic through the device

The lower half of the tile displays realtime graphical charts of the incoming and outgoing traffic through the devices selected from the list in the upper half. The administrator can select the devices to monitor the traffic through them by selecting the checkboxes beside the device names and deselect the others in the upper half. The lines are displayed in colors depending on the network zone to which the device belongs and the legend is shown at the top right of each graph.

Uplinks

The Uplinks area displays a table of uplinks configured for your account through which the CF connects to internet. The table shows the connection status and running status of each uplink and allows the administrator to enable or disable them.

Uplinks - Column Descriptions	
Column Header	Description
Name	The name of the uplinks configured by Comodo for your CF account.
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. • Connecting - The uplink is connecting to DCF, 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 DCF 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 for which the uplink is Up since the last reboot
Active	Indicates whether the uplink is active. The administrator can switch the uplink between enabled and disabled states by selecting/deselecting this checkbox
Managed	Indicates whether the uplink is managed by DCF or manually managed. The administrator can switch the management states by selecting or deselecting the

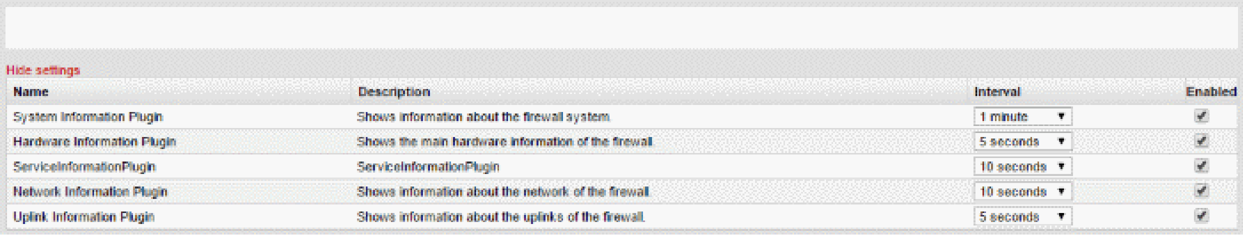
	checkbox. In Managed mode, the uplink will be continuously monitored and reconnected whenever there is a loss in connection. During testing or maintenance, the uplink can be switched to manual mode. • Clicking the circled arrow refreshes the information.

Configuring the Dashboard

Dome CF uses dashboard plug-ins to fetch the statistical information from different components of the CF 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 ▾	☑
ServiceInformationPlugin	ServiceInformationPlugin	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.

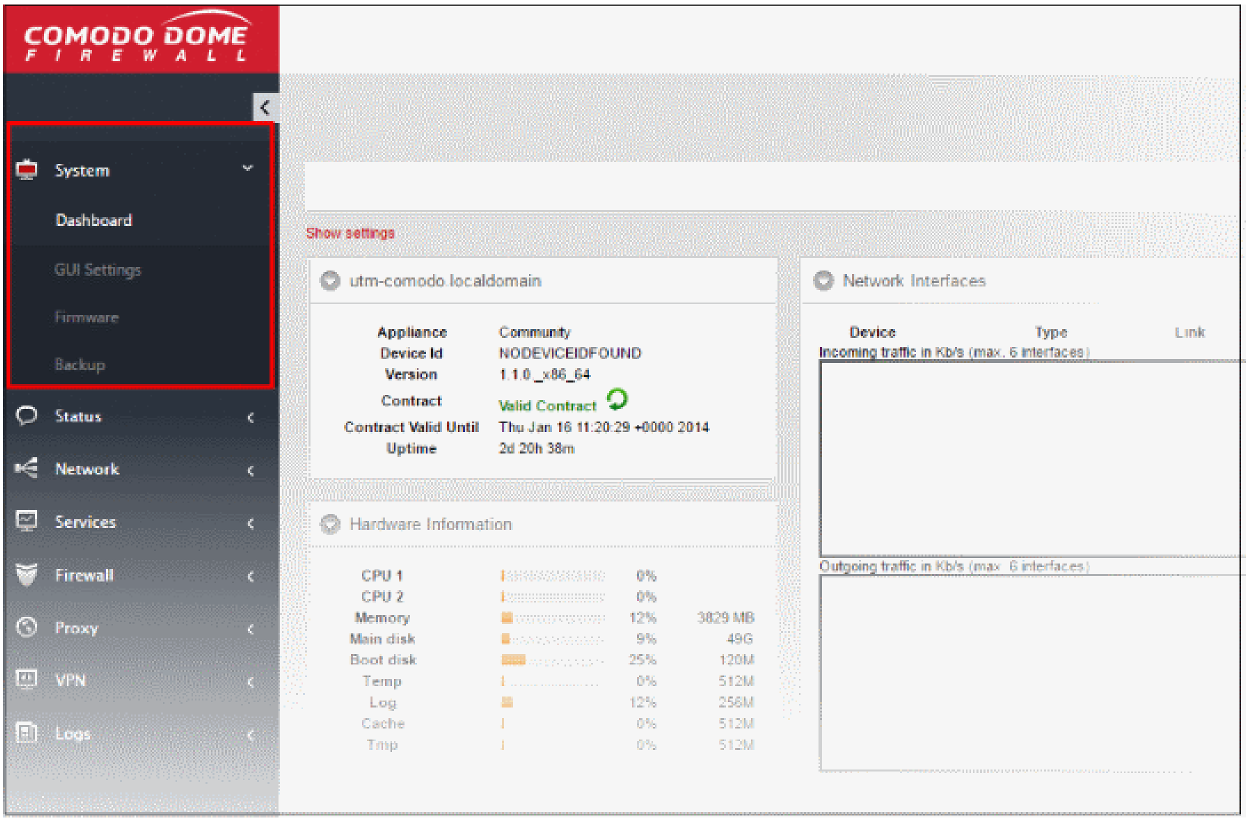
Dashboard Settings - Column Descriptions	
Column Header	**Description**
Name	The name of the plugin
Description	A short description of the plug-in. Indicates the component of DCF for which the plug-in fetches the information.
Interval	Enables the administrator to set the time interval at which the plug-in 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

From the system interface, administrators can:

- Select the interface language and modify the information which is shown in the interface
- View the current DCF version and update to a newer version if available
- Create backups of DCF state including configuration settings, logs and database dumps
- View DCF dashboard



Appliance	Community
Device Id	NODEVICEIDFOUND
Version	1.1.0_x86_64
Contract	Valid Contract
Contract Valid Until	Thu Jan 16 11:20:29 +0000 2014
Uptime	2d 20h 38m

CPU 1	0%	
CPU 2	0%	
Memory	12%	3829 MB
Main disk	9%	49G
Boot disk	25%	120M
Temp	0%	512M
Log	12%	256M
Cache	0%	512M
Tmp	0%	512M

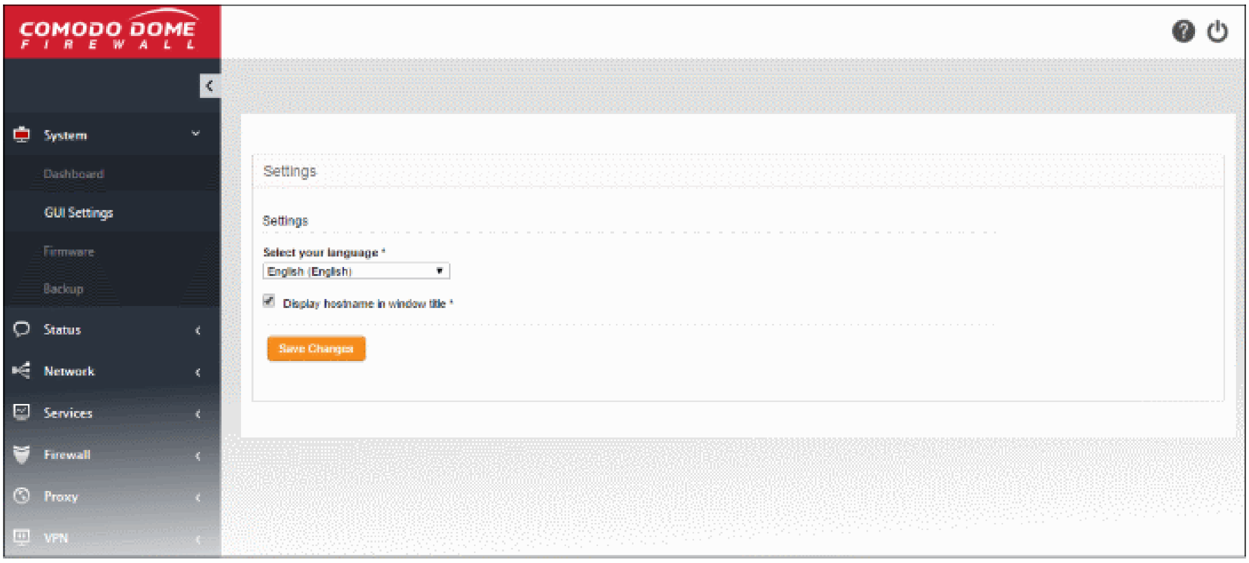
The 'System' module contains the following screens for viewing and managing the general configuration of the UTM. The screens can be accessed by clicking the following options from the sub-menu under 'System'.

- **Dashboard** - Displays an at-a-glance statistical summary of the current running status, health and usage status of DCF. See section '**The Dashboard**' for more details.
- **GUI Settings** - Enables the administrator to select the interface language to be displayed in the administrative console. See section '**Configuring the GUI settings**' for more details.
- **Firmware** - Enables the administrator to view the version number of DCF and update the firmware, if updates are available. See section '**Viewing and Updating DCF Version**' for more details.
- **Backup** - Enables the administrator to create a backup of the current state of DCF and to schedule periodical backups. In case of any abnormality or untoward incidents, the backups can be imported and applied to the device for restoring the device. See section '**Creating and Scheduling Backup of DCF State**' for more details.

4.1 Configuring GUI Settings

The 'GUI Settings' interface allows you to select the interface language and modify the information which is shown in the interface.

To open the interface, click 'System' > 'GUI settings' from the left hand side navigation.



Settings

Settings

Select your language *

English (English)

☑ Display hostname in window title *

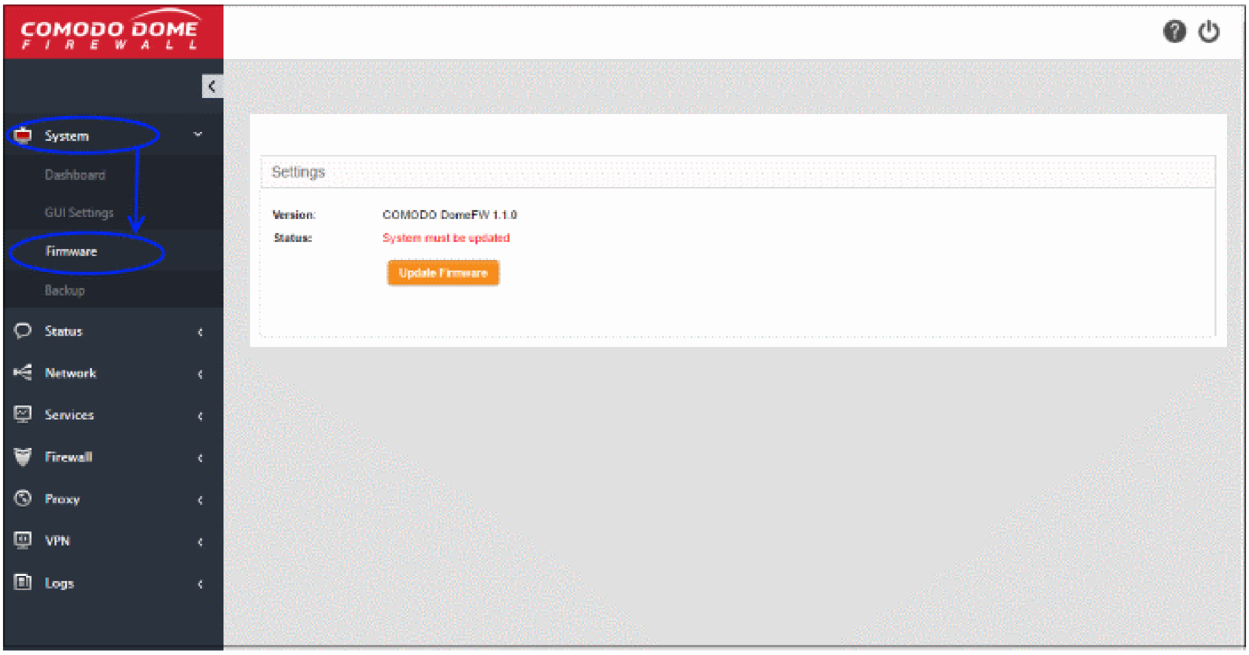
Save Changes

- Choose the language in which you wish the graphical user interface of the administrative console is to be displayed from the 'Select your language' drop-down.
- Display hostname in window title - The hostname of DCF is displayed in the title bar of the browser window in which the administrative console is opened. De-select this option if you do not want the host name to be displayed.
- Click 'Save' changes for your configuration to take effect.

4.2 Viewing and Updating DCF Version

The 'Firmware' screen displays the DCF version number and its update status. Also, if an new version is available, the administrator can initiate the update process.

To open the 'Firmware' interface, click 'System' > 'Firmware' from the left hand side navigation.



Settings

Version: COMODO DomeFW 1.1.0

Status: System must be updated

Update Firmware

- **Version** - Shows the version number of the Comodo Dome CF Firmware for your account.
- **Status** - Indicates whether your firmware is up-to-date. If it indicates 'System must be updated', you can initiate the update process by clicking the Update Firmware button. The firmware will be automatically

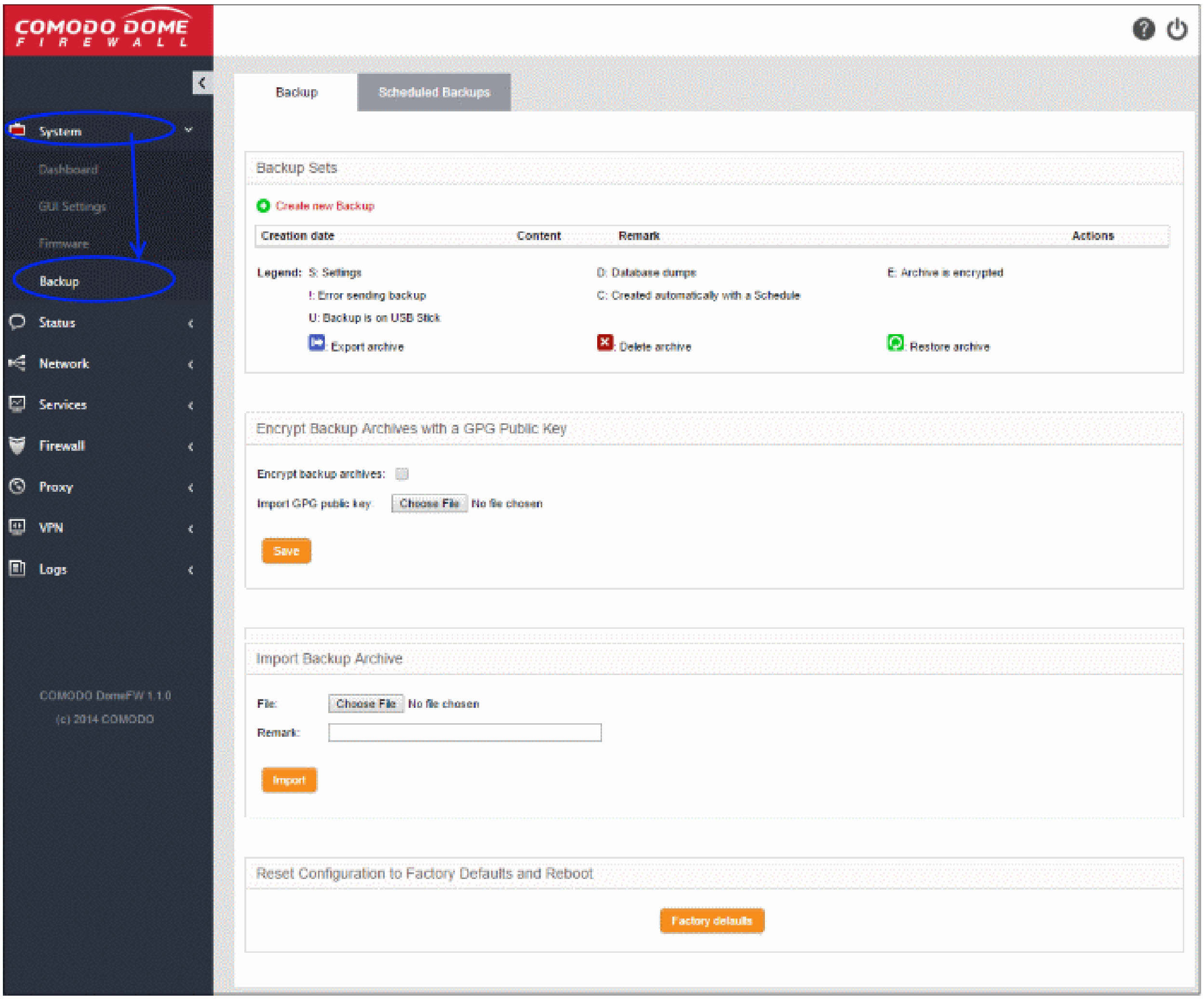
downloaded and installed.

4.3 Creating and Scheduling Backup of DCF State

Comodo Dome Cloud Firewall allows administrators to create backups of DCF state including the configuration settings, logs and database dumps at various time points. You can restore to a backup if you want to roll-back the DCF state to a previous state. You can also restore the appliance to the factory default settings should this be required.

Backups can be manually created at any time or scheduled for creation at set intervals. The backups can be encrypted, stored locally, on a USB stick or can be emailed for storage in a remote location.

To open the 'Backup' interface, click 'System' > 'Backup' from the left hand side navigation.



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

Encrypt Backup Archives with a GPG Public Key

Encrypt backup archives: □

Import GPG public key: Choose File No file chosen

Save

Import Backup Archive

File: Choose File No file chosen

Remark:

Import

Reset Configuration to Factory Defaults and Reboot

Factory defaults

The 'Backup' interface displays a list of backups created so far under 'Backup sets' and allows the administrator to export the backups to desired location for archiving, remove backups and restore a selected backup to rollback the DCF to the respective time point.

Backup Sets - Column Descriptions	
Column Header	**Description**
Creation date	Date and time at which the backup was created
Content	Displays the components of the DCF state, contained in the backup, its history and

<table>
<tr><td></td><td>errors, if any, occurred during backup creation. The legend is given below:
<table>
<tr><td>Charact er</td><td>Expansion</td><td>Description</td></tr>
<tr><td>A</td><td>Archive</td><td>Contains archived log files</td></tr>
<tr><td>C</td><td>Chronologic al</td><td>The backup was created automatically by the schedule</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 was encrypted</td></tr>
<tr><td>L</td><td>Log files</td><td>Contains log files</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 in the 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 so that the backup can be saved in the local storage of the computer from which the administrative console is accessed
 - Deletes the backup
 -Restores the backup and rollbacks DCF state to the respective time point.</td></tr>
</table>

The following sections explain in detail on backup tasks:

- **Manually creating a backup**
- **Scheduling backup operations**
- **Encrypting backup archives**
- **Exporting a backup**
- **Importing a backup from an archive**
- **Rolling back DCF to a previous time point**
- **Resetting DCF to factory defaults**

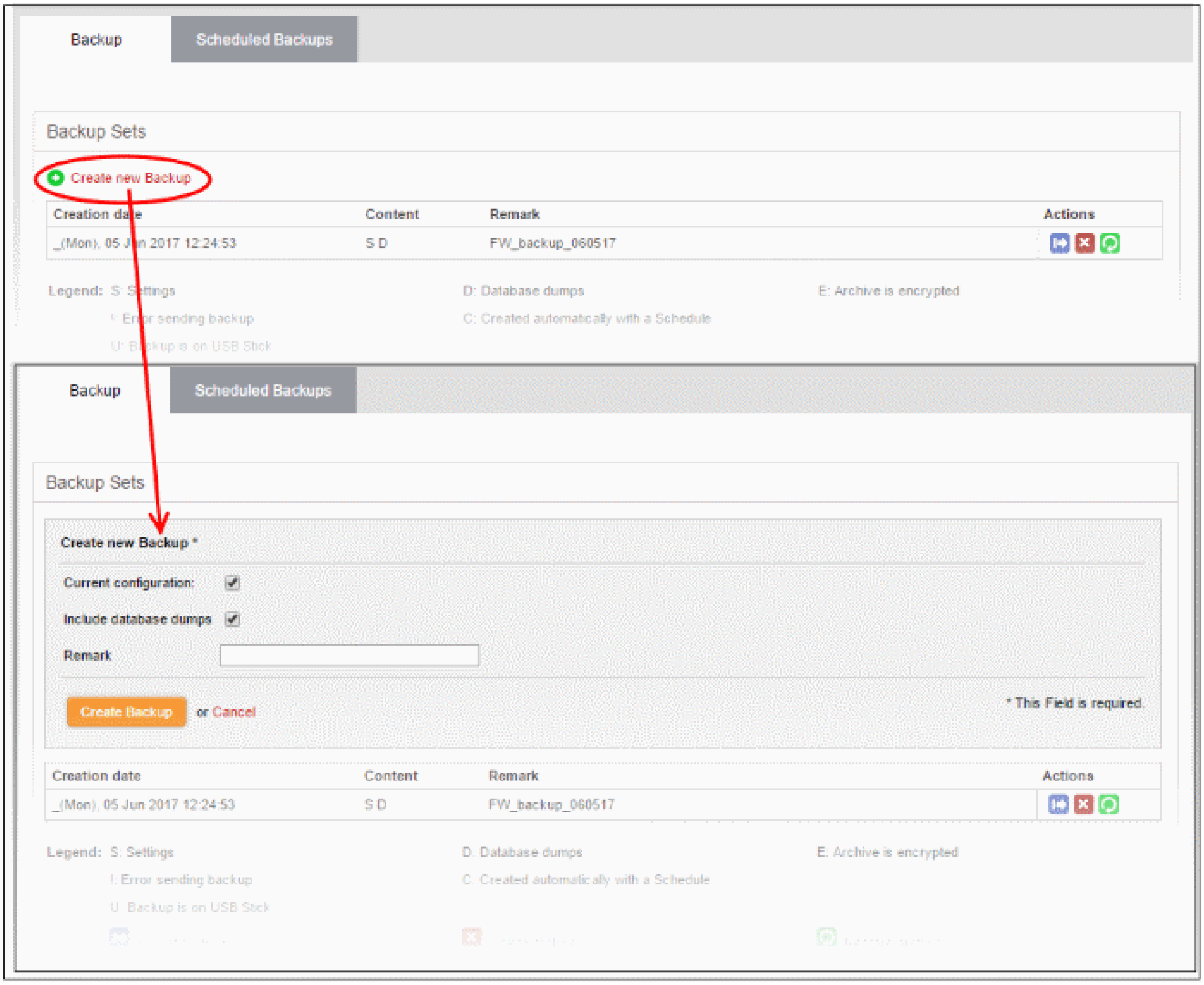
4.3.1 Manually Creating a Backup

An administrator can create backup of DCF at any desired time, for example, before making a critical configuration change to roll back DCF state, just in case the new configuration creates any glitches. The backup can be configured for inclusion of the components and can be stored either locally in DCF or in a USB drive.

To create a backup

- Open the 'Backup' interface by clicking 'System' > 'Backup' from the left hand side navigation
- In the 'Backup' section, click the 'Create new backup' link above the list of backups

The 'Create new Backup' pane will open.



Creation date	Content	Remark	Actions
_(Mon), 05 Jun 2017 12:24:53	S D	FW_backup_060517	

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

Create new Backup *

Current configuration: ☑

Include database dumps ☑

Remark

* This Field is required.

Creation date	Content	Remark	Actions
_(Mon), 05 Jun 2017 12:24:53	S D	FW_backup_060517	

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

- Choose the components to be included in the backup:
  - Current configuration - Includes the current configuration of DCF in the backup. Deselect the checkbox if you do not want the current configuration to be backed up.
  - Include database dumps - Adds the CF 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.

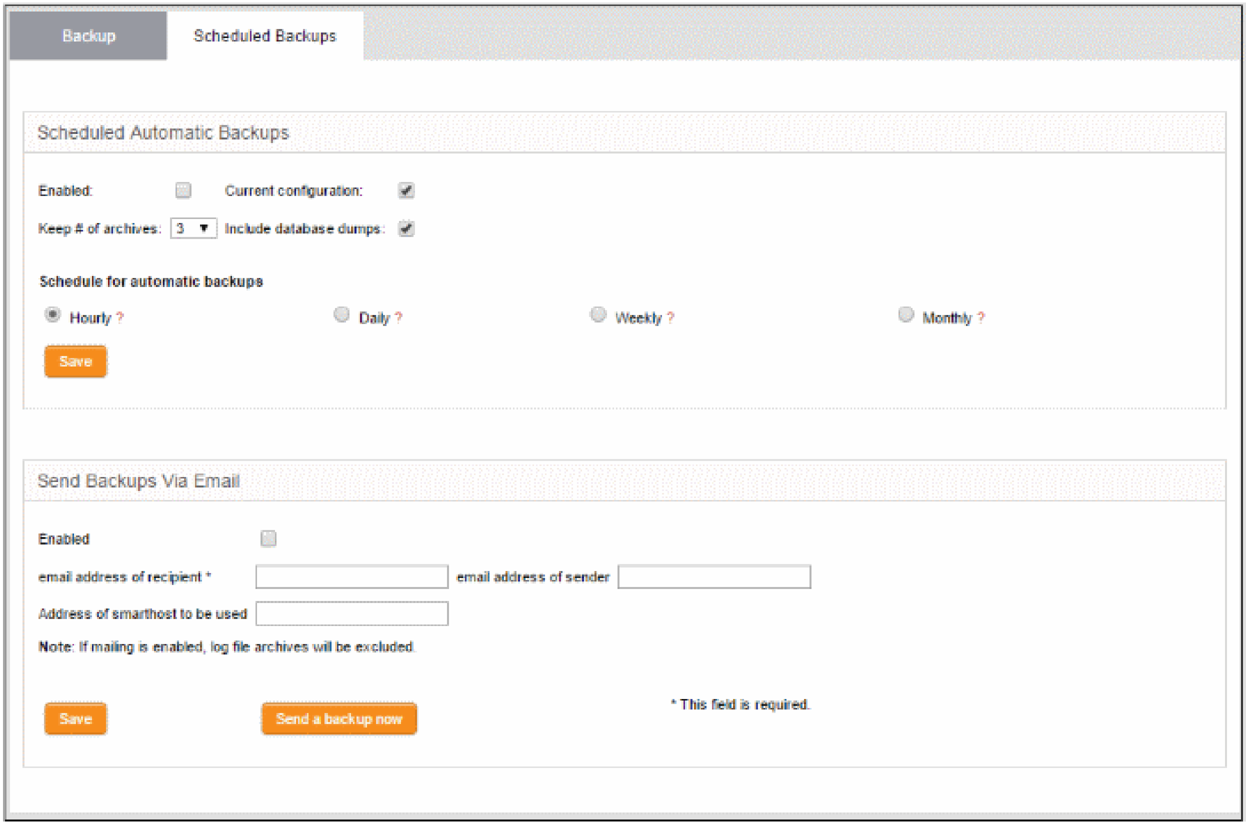
The backup will be created and added to the list of backups. If encryption is enabled, the backup file will be encrypted and saved. See section '**Encrypting Backup Archives**' for more details.

4.3.2 Scheduling Backup Operations

An 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



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' section
    - 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 CF 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 CF 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 DCF state will be created and sent to the specified email address.

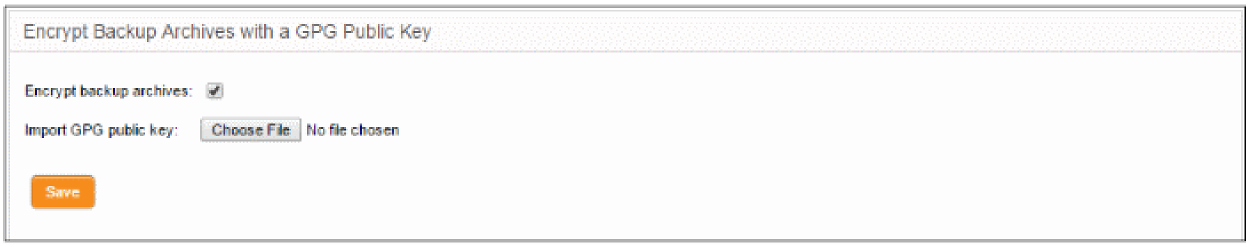
4.3.3 Encrypting Backup Archives

Comodo Dome CF can encrypt and store the backup archives created on both manual backup operation and scheduled backups using a GNU Privacy Guard (GPG) public key. An administrator can choose to 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 for encrypting backups

- Open the Backup interface by clicking 'System' > 'Backup' from the left hand side navigation.
- In the 'Backup' section, configure the encryption 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

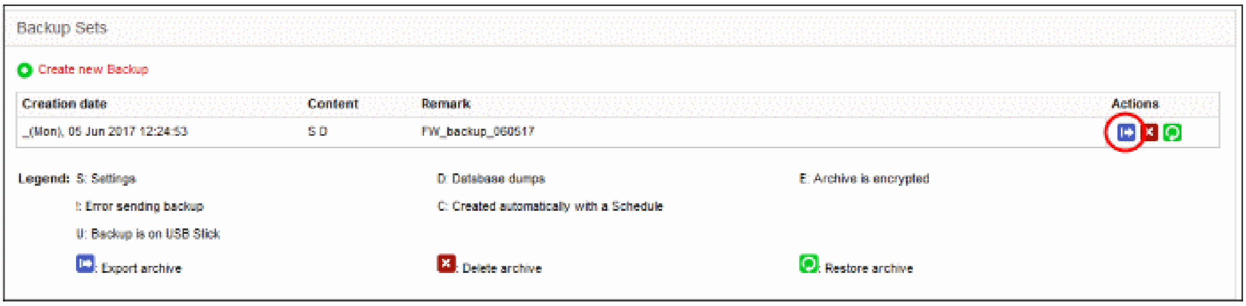
  - Encrypt backup archives - Select this option to encrypt the backup archives
  - Import GPG public key - Click 'Browse' and navigate to the location where the public key is stored in the local computer and clock 'Open' in the 'Choose file to upload' dialog.
- Click 'Save' to upload the public key and save the configuration.

4.3.4 Exporting a Backup

Backup archives stored on DCF or connected drives can be exported as required. See '**Importing a Backup**' and. '**Rolling Back DCF State to a Previous Time Point**' for details about importing and restoring to backups.

To export a backup archive

- Click 'System' > 'Backup' on the left hand menu.
- A list of available archives will be displayed. Any backups stored on connected USB drives will also be shown.



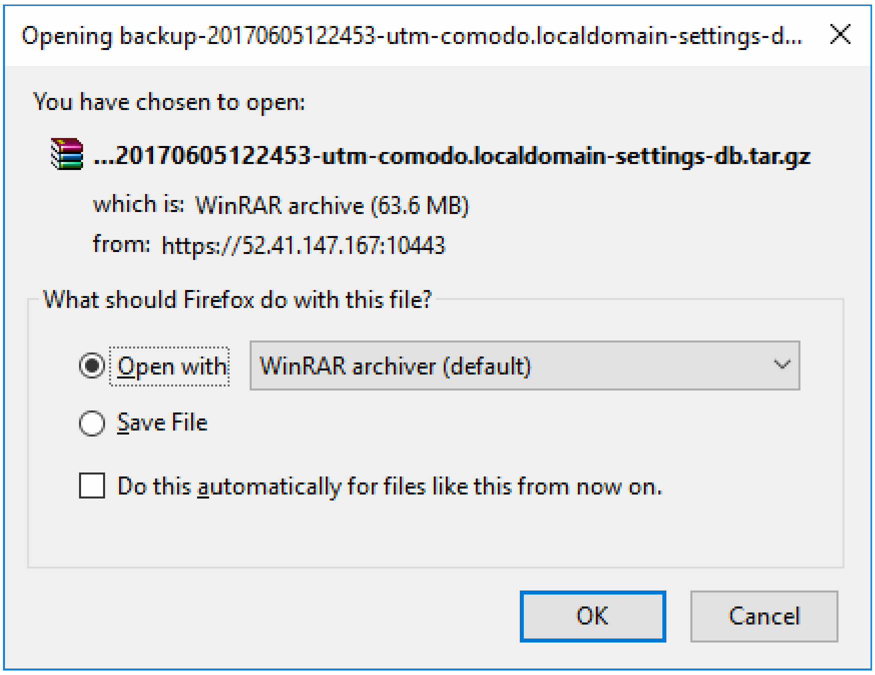
Backup Sets

Creation date	Content	Remark	Actions
_(Mon), 05 Jun 2017 12:24:53	S D	FW_backup_060517	

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

- Select the backup file you wish to export.

- Click the Export button ➡.
- The file will be downloaded to the default download location or a 'File Download' dialog will be displayed depending on the browser and/or settings for downloading files.



Opening backup-20170605122453-utm-comodo.localdomain-settings-d...

You have chosen to open:

...20170605122453-utm-comodo.localdomain-settings-db.tar.gz

which is: WinRAR archive (63.6 MB)

from: https://52.41.147.167:10443

What should Firefox do with this file?

● Open with WinRAR archiver (default)

○ Save File

□ Do this automatically for files like this from now on.

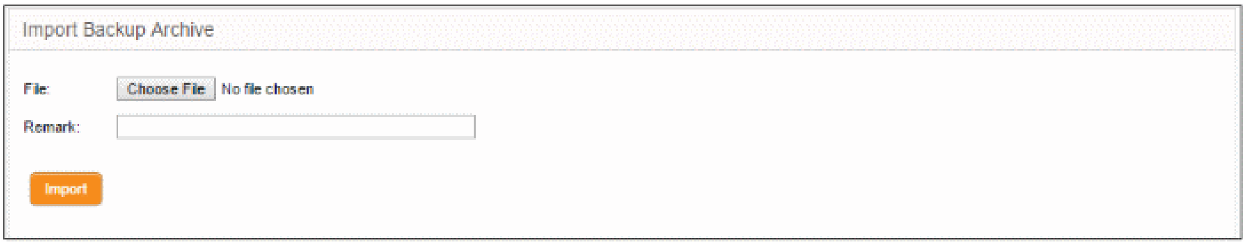
- Click 'Save File'. The file will be saved to default download location.
- The backup archive will be saved as a time-stamped archive in .tar.gz format.
- The default file name will use the format: 'backup-<time stamp>-utm-<hostname of the appliance>-<component1 in backup>-<component 2 in backup>.tar.gz'.

4.3.5 Importing a Backup Archive from a Local Computer

Exported backup archives can be imported to the console to roll back the DCF state to a previous time point. Refer to **Exporting a backup** for help to export a backup.

To import a backup archive

- Login to the Comodo Dome CF administrative interface from the computer on which the backup is stored
- Click 'System' > 'Backup' on the left hand menu
- In the 'Backup' screen scroll down to the 'Import Backup Archive' section.



Import Backup Archive

File: Choose File No file chosen

Remark:

- Click 'Choose File' then browse to and open the required archive. Backup archives are stored in tar.gz format
- 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 on DCF.

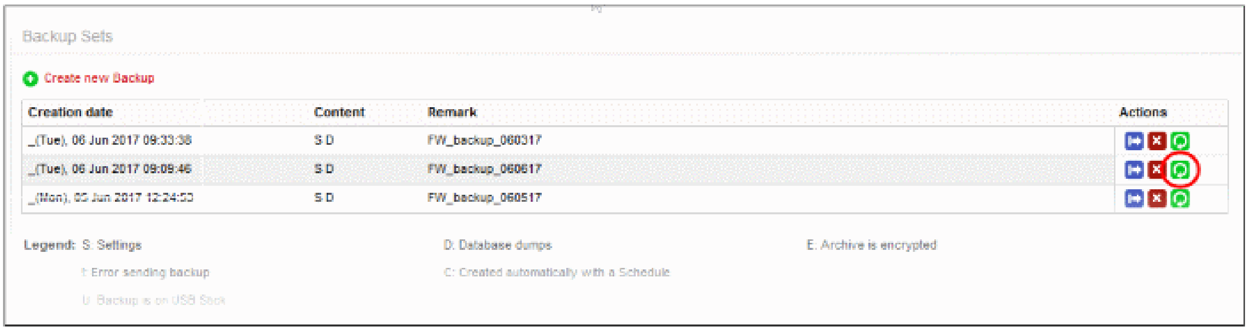
After importing, the archive will be added to the 'Backup Sets' list. Admins can use the file to restore the firewall to a previous state. Refer to '**Rolling Back DCF State to a Previous Time Point**' for more details on this.

4.3.6 Rolling Back DCF Sate to a Previous Time Point

Backup archives allow administrators to roll-back the DCF state to a previous point in time. DCF will restart after the restore operation is complete.

To restore a from a backup

- Click 'System' > 'Backup' from the left hand menu
- A list of available archives will be displayed.
- Select the archive from which you wish to restore then click the 'Restore' button:



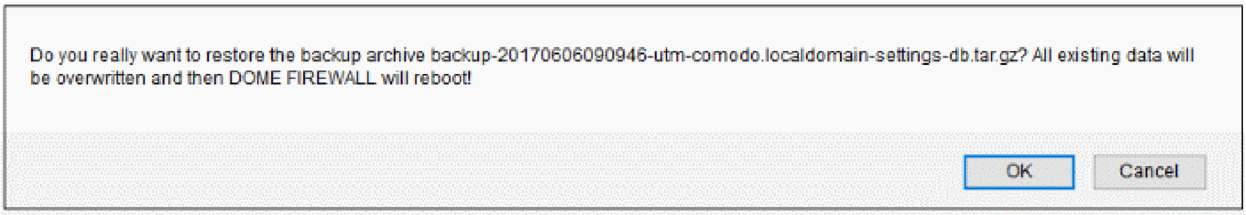
Backup Sets

Create new Backup

Creation date	Content	Remark	Actions
_(Tue), 06 Jun 2017 09:33:38	S D	FW_backup_060317	
_(Tue), 06 Jun 2017 09:09:46	S D	FW_backup_060617	
_(Mon), 05 Jun 2017 12:24:53	S D	FW_backup_060517	

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

- Click 'OK' at the confirmation dialog:



Do you really want to restore the backup archive backup-20170606090946-utm-comodo.localdomain-settings-db.tar.gz? All existing data will be overwritten and then DOME FIREWALL will reboot!

The firewall will restart to apply the backup configuration. The firewall's existing configuration, log files and database dumps will be overwritten with those of the backup.

4.3.7 Resetting DCF State to Factory Defaults

Resetting the DCF state to its initial state will clear all existing configurations, passwords, database dumps and logs.

Administrators will need to reconfigure login credentials, network connections and so on.

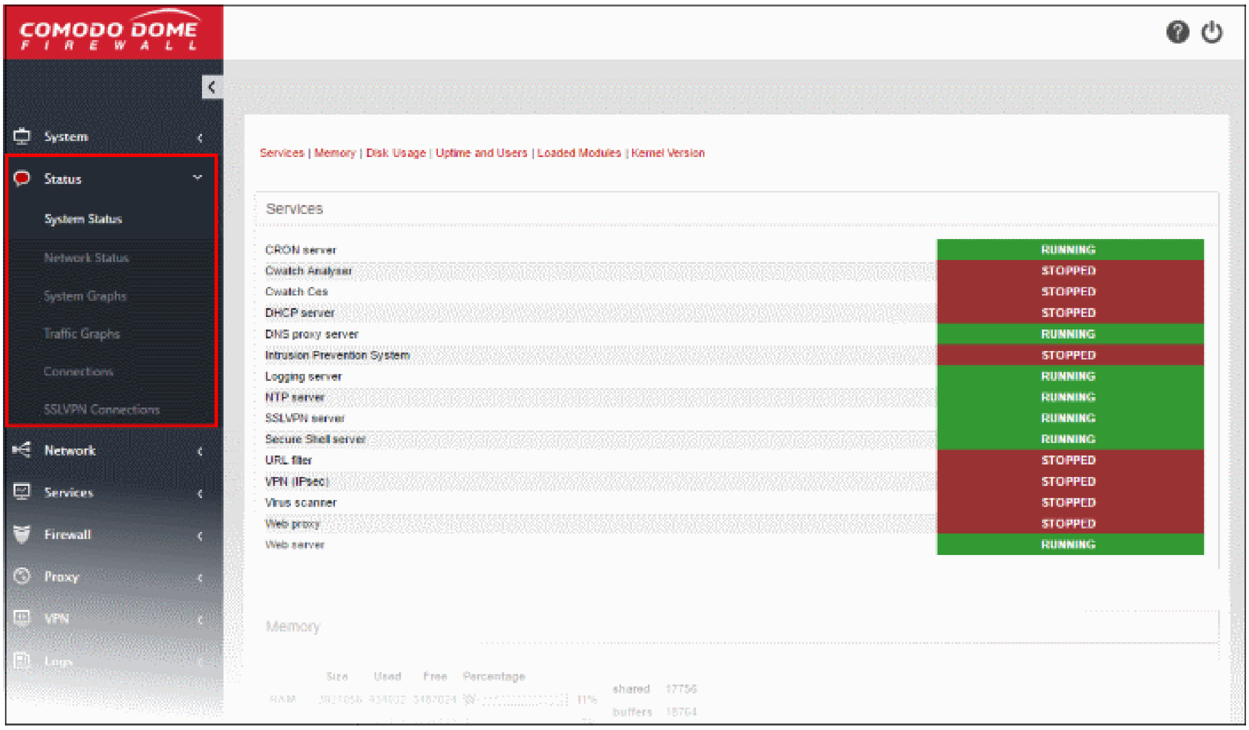
Note: As a fail-safe measure, Dome CF creates a backup of the current state before resetting to factory defaults.

To reset Dome CF

- Click 'System' > 'Backup' from the left hand side navigation.
- In the 'Backup' section, click the 'Factory defaults' button under 'Reset configuration to factory defaults and reboot'. A confirmation dialog will appear.
- Click 'OK' in the dialog. Dome CF will be reset and restarted with the default factory settings.

5 Viewing Dome Cloud Firewall Status

The 'Status' module displays statistics about various Dome Cloud Firewall components, including system status, network status, network connections, realtime network traffic and SSL VPN connections.



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

Services

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

Memory

Size Used Free Percentage

shared 17756
buffers 18764

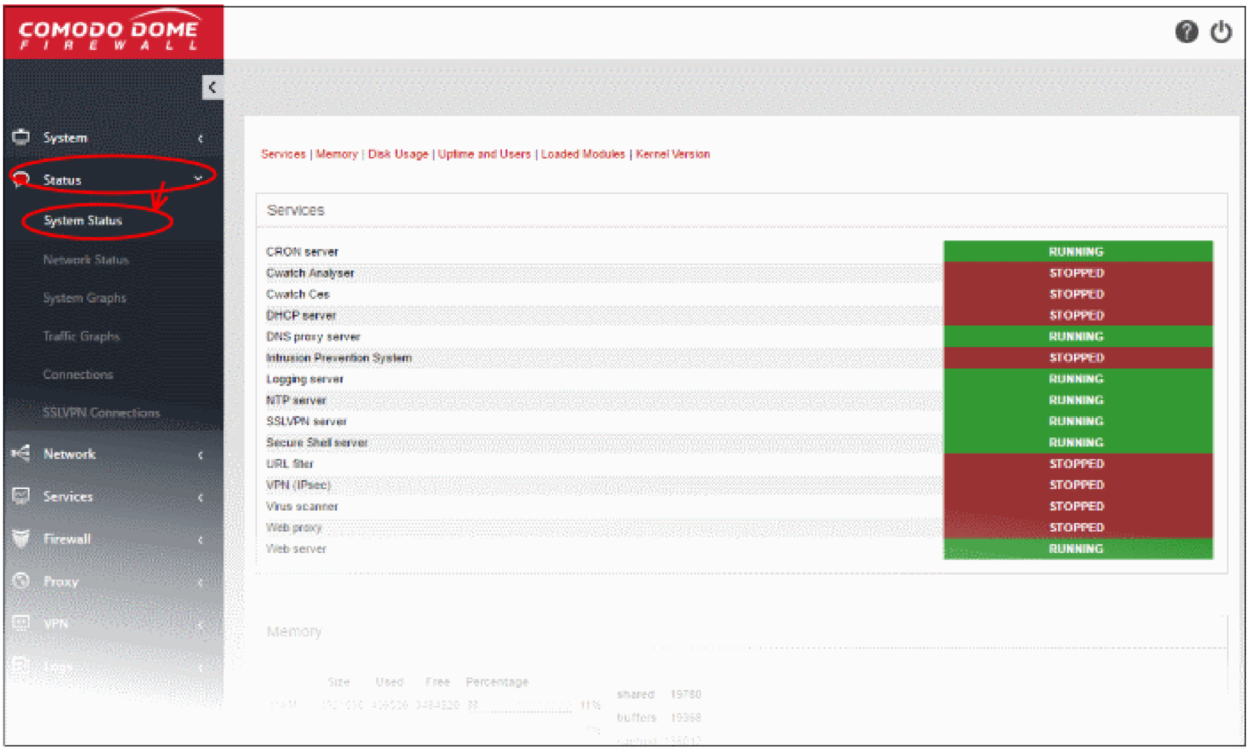
The 'Status' module contains the following items:

- **System Status** - Statistics about the current running state of the firewall, including services loaded, memory usage, disk usage and so on. See '**System Status**' for more details.
- **Network Status** - Statistics about active 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** - Shows real-time traffic data over different network zones (LAN, internet etc). See '**Network Traffic**' for more details.
- **Connections** - Shows connections to, from and through Dome CF. Includes connection source, destination, protocol and status. See '**Network Connections**' for more details.
- **SSL VPN Connections** - Shows users that have connected through SSL VPN and currently running VPN services. See '**SSL VPN Connections**' for more details.

5.1 System Status

The 'System Status' screen shows information about running services.

To open the 'System Status' interface, click 'Status' on the left then 'System Status':



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

Services

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

Memory

Size Used Free Percentage

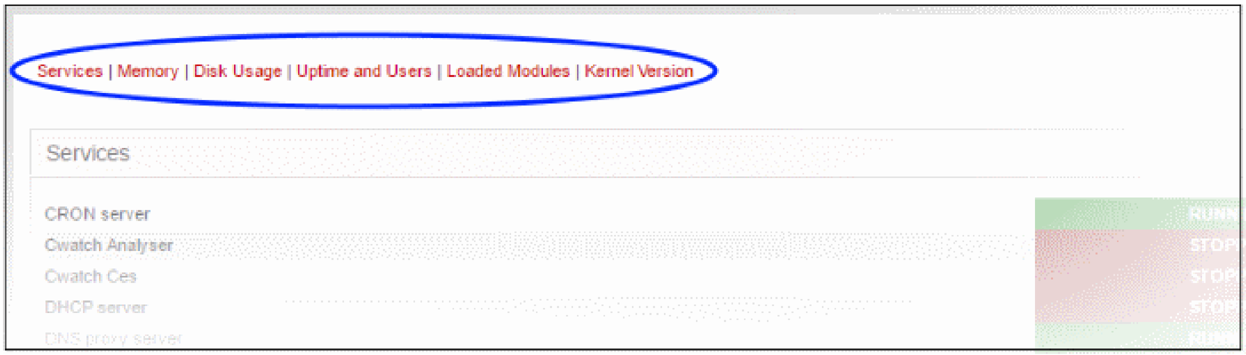
11%

shared 19780

buffers 19368

- **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 CF 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

Administrators 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

Cwatch Analyser

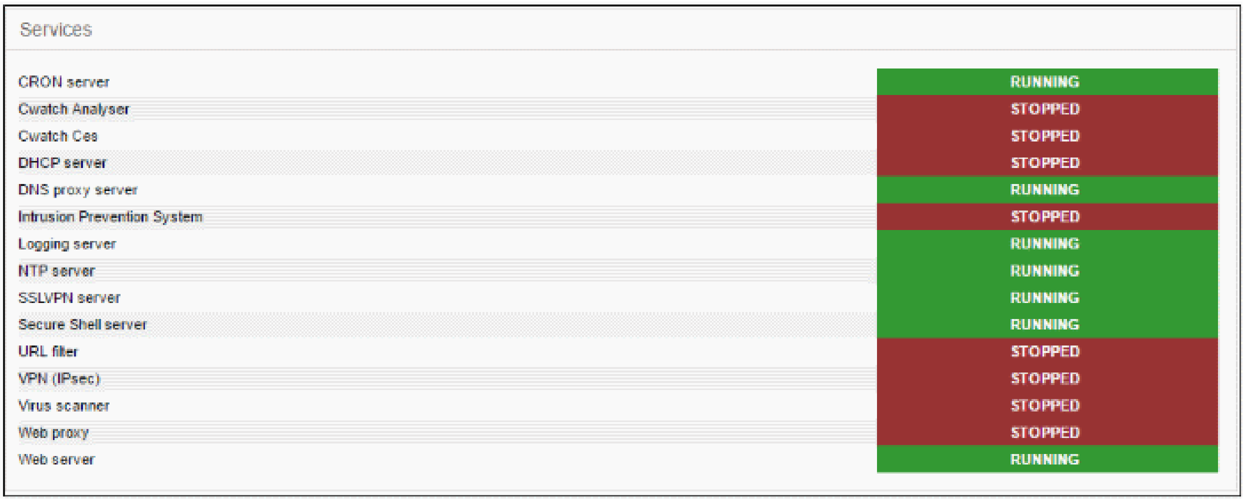
Cwatch Ces

DHCP server

DNS proxy server

Services

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

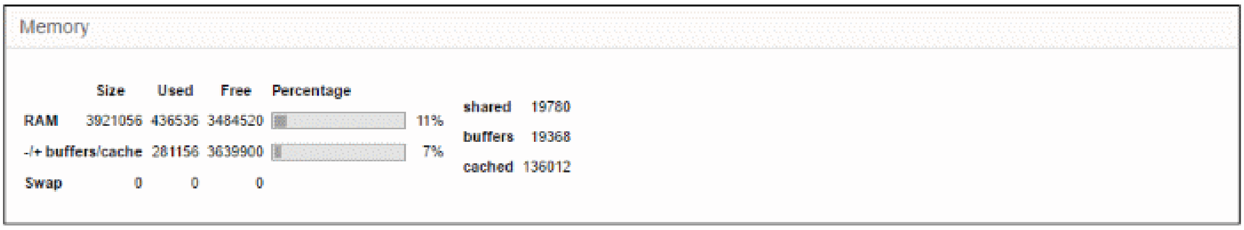


Services

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

Memory

The memory pane shows the usage status of the physical memory in DCF server.



Memory

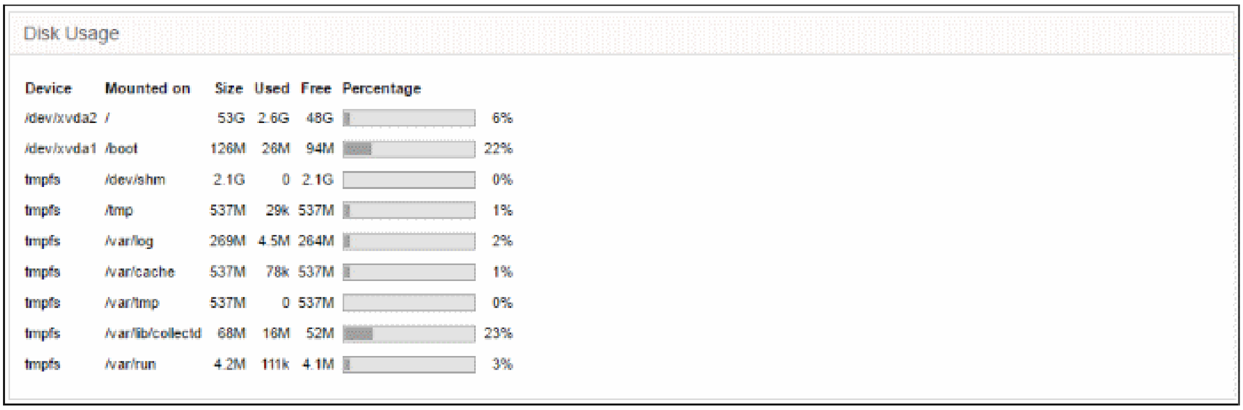
	Size	Used	Free	Percentage	
RAM	3921056	436536	3484520	11%	
-/+ buffers/cache		281156	3639900	7%	
Swap	0	0	0		

shared	19780
buffers	19368
cached	136012

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 Dome CF 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 Dome Cloud Firewall, their mount point and the space of each disk partition similar to the output of Linux Disk Free (df) command.



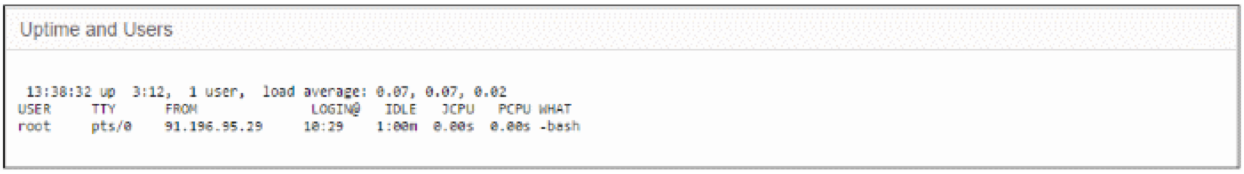
Disk Usage

Device	Mounted on	Size	Used	Free	Percentage
/dev/xvda2	/	53G	2.6G	48G	6%
/dev/xvda1	/boot	126M	26M	94M	22%
tmpfs	/dev/shm	2.1G	0	2.1G	0%
tmpfs	/tmp	537M	29k	537M	1%
tmpfs	/var/log	269M	4.5M	264M	2%
tmpfs	/var/cache	537M	78k	537M	1%
tmpfs	/var/tmp	537M	0	537M	0%
tmpfs	/var/lib/collectd	68M	16M	52M	23%
tmpfs	/var/run	4.2M	111k	4.1M	3%

Disk Usage - Column Descriptions	
Column	**Description**
Device	The disk device or partition for various Dome CF 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 DCF is continuously running from the last boot time and the list of users that are currently logged-in.



Uptime and Users

```
 13:38:32 up  3:12,  1 user,  load average: 0.07, 0.07, 0.02
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    91.196.95.29     10:29    1:00m  0.00s  0.00s -bash
```

The first line displays the following items in order:

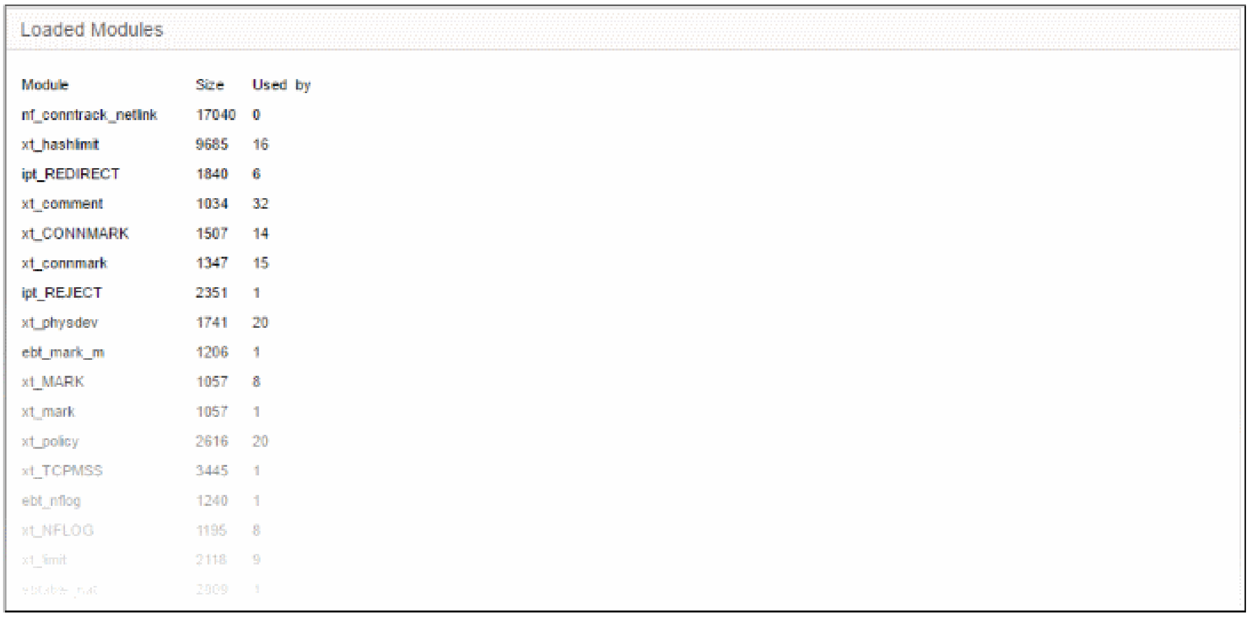
- Current time
- The period for which the Dome CF is up and running from the last boot time
- The number of users currently logged into the system
- The average load on the system for the past 1, 5 and 15 minutes.

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.



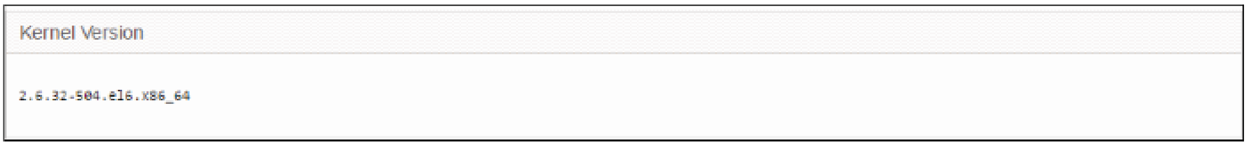
Loaded Modules

```
Module               Size    Used by
nf_conntrack_netlink 17040   0
xt_hashlimit         9685    16
ipt_REDIRECT         1840    6
xt_comment           1034    32
xt_CONNMARK          1507    14
xt_connmark          1347    15
ipt_REJECT           2351    1
xt_physdev           1741    20
ebt_mark_m           1206    1
xt_MARK              1057    8
xt_mark              1057    1
xt_policy            2616    20
xt_TCPMSS            3445    1
ebt_nflog            1240    1
xt_NFLOG             1195    8
xt_limit             2118    9
ebtable_nat          2009    1
```

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.



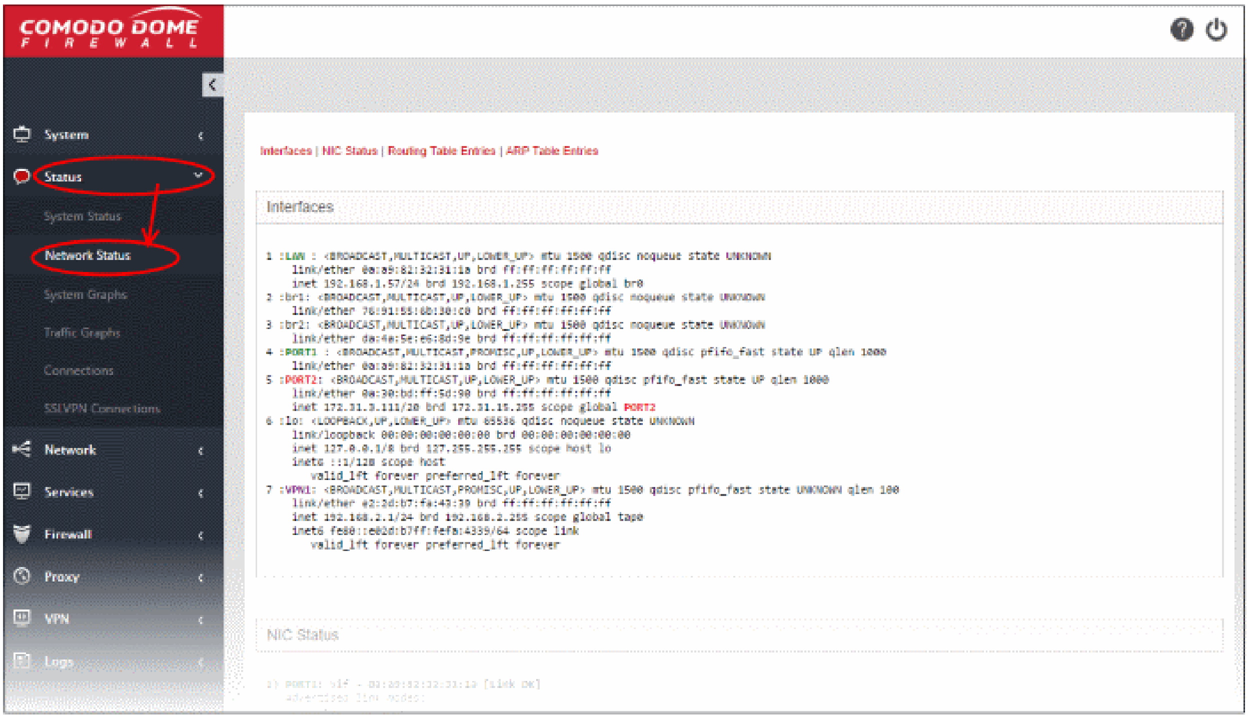
Kernel Version

```
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).

To open the 'Network Status' interface, click 'Status' on the left then 'Network Status':



Interfaces

```
1 :LAN : <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 0a:a9:82:32:31:1a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.57/24 brd 192.168.1.255 scope global br0
2 :br1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 76:91:55:6b:30:c0 brd ff:ff:ff:ff:ff:ff
3 :br2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether da:4e:5e:e6:8d:9e brd ff:ff:ff:ff:ff:ff
4 :PORT1 : <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 0a:a9:82:32:31:1a brd ff:ff:ff:ff:ff:ff
5 :PORT2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 0a:30:bd:ff:5d:90 brd ff:ff:ff:ff:ff:ff
    inet 172.31.3.111/20 brd 172.31.15.255 scope global PORT2
6 :lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 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
7 :VPN1: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 100
    link/ether e2:2d:b7:fa:43:39 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.1/24 brd 192.168.2.255 scope global tape
    inet6 fe80::e02d:b7ff:fefa:4339/64 scope link
       valid_lft forever preferred_lft forever
```

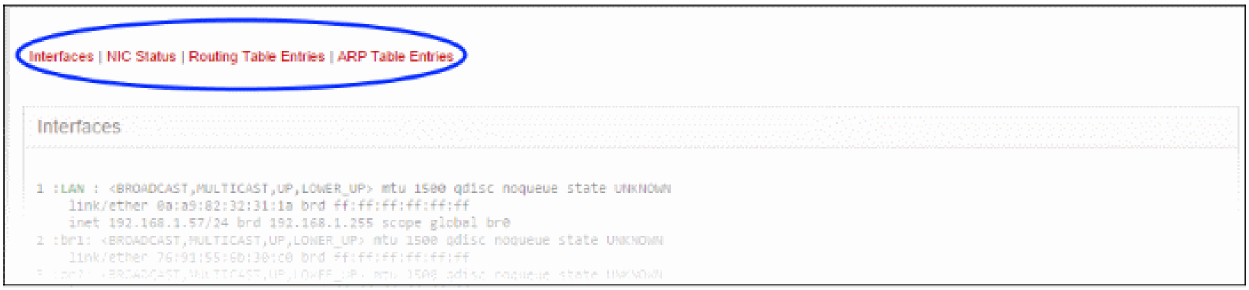
NIC Status

```
1) PORT1: sif - 0a:a9:82:32:31:1a [link OK]
    advertised link modes:
```

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

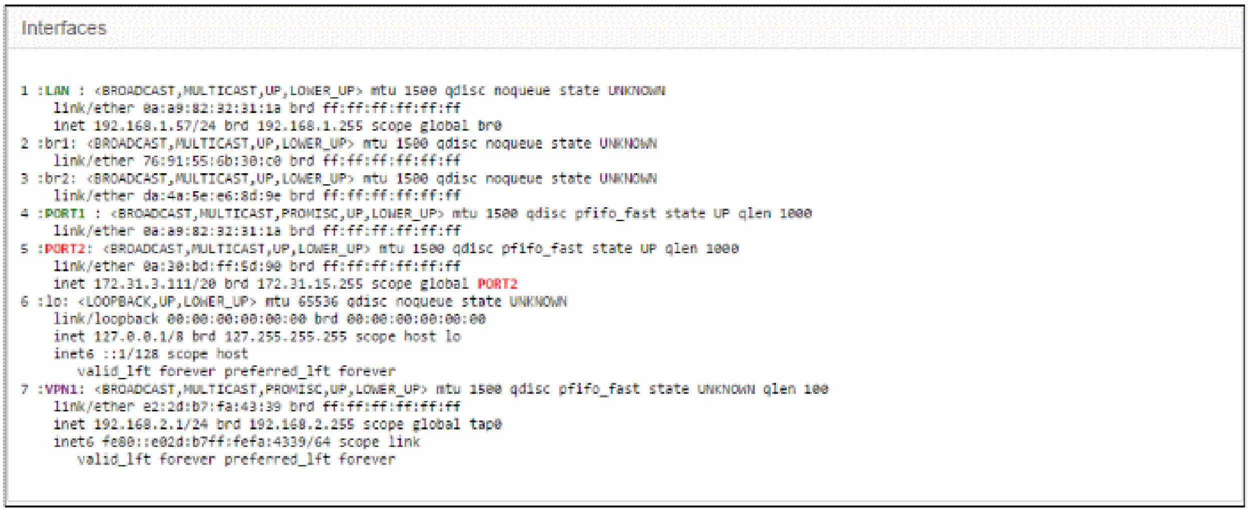
Interfaces

```
1 :LAN : <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 0a:a9:82:32:31:1a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.57/24 brd 192.168.1.255 scope global br0
2 :br1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 76:91:55:6b:30:c0 brd ff:ff:ff:ff:ff:ff
3 :br2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
```

Interfaces

The 'Interfaces' pane displays a list of all network interfaces connected to Dome CF 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 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

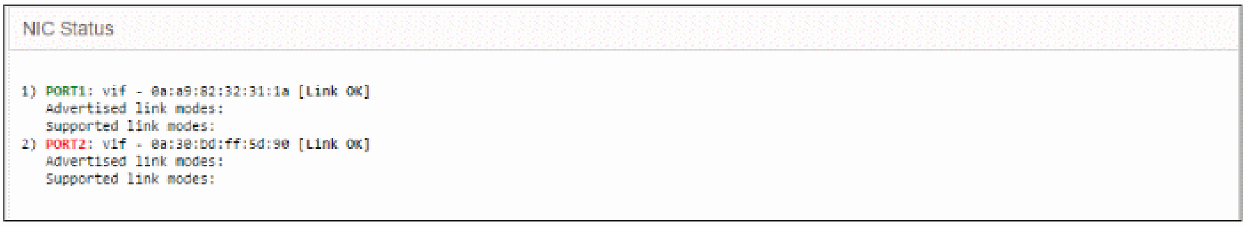


Interfaces

```
1 :LAN : <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 0a:a9:82:32:31:1a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.57/24 brd 192.168.1.255 scope global br0
2 :br1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 76:91:55:6b:30:c0 brd ff:ff:ff:ff:ff:ff
3 :br2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether da:4a:5e:e6:8d:9e brd ff:ff:ff:ff:ff:ff
4 :PORT1 : <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 0a:a9:82:32:31:1a brd ff:ff:ff:ff:ff:ff
5 :PORT2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 0a:30:bd:ff:5d:90 brd ff:ff:ff:ff:ff:ff
    inet 172.31.3.111/20 brd 172.31.15.255 scope global PORT2
6 :lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 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
7 :VPN1: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 100
    link/ether e2:2d:b7:fa:43:39 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.1/24 brd 192.168.2.255 scope global tap0
    inet6 fe80::e02d:b7ff:fefa:4339/64 scope link
       valid_lft forever preferred_lft forever
```

NIC Status

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

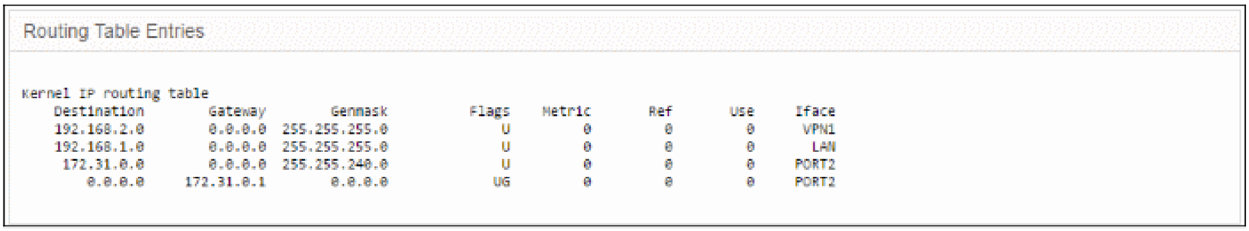


NIC Status

```
1) PORT1: vif - 0a:a9:82:32:31:1a [Link OK]
   Advertised link modes:
   Supported link modes:
2) PORT2: vif - 0a:30:bd:ff:5d:90 [Link OK]
   Advertised link modes:
   Supported link modes:
```

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.



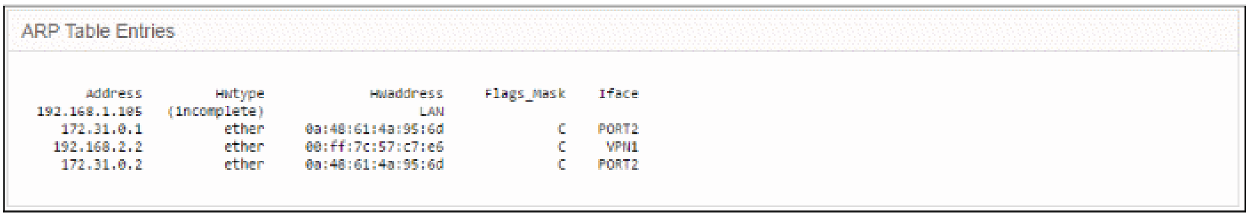
Routing Table Entries

```
Kernel IP routing table
    Destination         Gateway         Genmask          Flags    Metric       Ref       Use     Iface
    192.168.2.0         0.0.0.0   255.255.255.0              U         0         0         0      VPN1
    192.168.1.0         0.0.0.0   255.255.255.0              U         0         0         0       LAN
     172.31.0.0         0.0.0.0   255.255.240.0              U         0         0         0     PORT2
        0.0.0.0      172.31.0.1         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 - Th 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

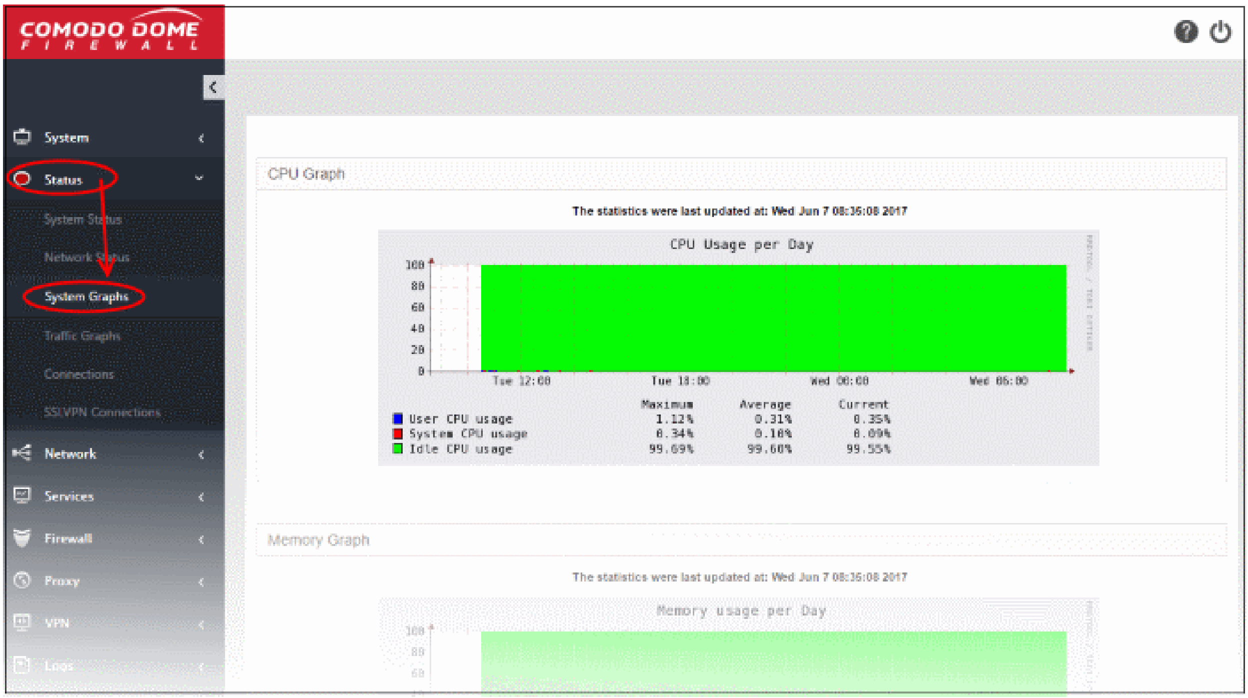
```
      Address         HWtype           HWaddress     Flags_Mask     Iface
  192.168.1.105   (incomplete)               LAN
     172.31.0.1          ether  0a:48:61:4a:95:6d             C     PORT2
    192.168.2.2          ether  00:ff:7c:57:c7:e6             C      VPN1
     172.31.0.2          ether  0a:48:61:4a:95:6d             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 shows resource usage for the past 24 hours. This includes CPU, system memory, swap memory and disk drive use.

To open the interface, click 'Status' on the left then 'System Graphs':



CPU Graph

The statistics were last updated at: Wed Jun 7 08:36:08 2017

```
                     Maximum    Average    Current
🟦 User CPU usage      1.12%      0.31%      0.35%
🟥 System CPU usage    0.34%      0.10%      0.09%
🟩 Idle CPU usage     99.69%     99.60%     99.55%
```

Memory Graph

The statistics were last updated at: Wed Jun 7 08:36:08 2017

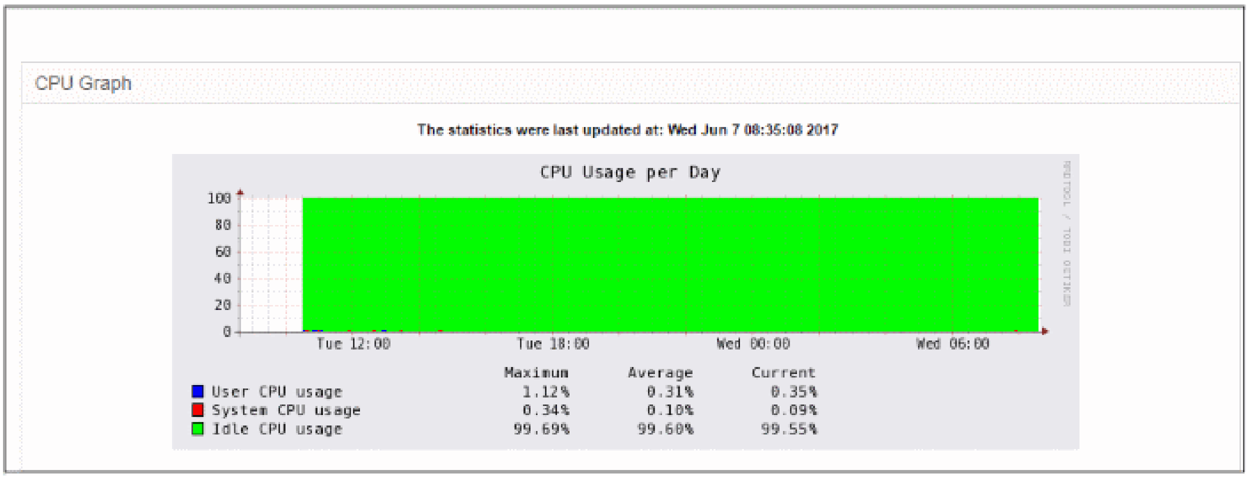
Clicking any graph will show more information about that component. Click the following links for details on each:

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

CPU Graph

The 'CPU Graph' displays the load on the DFS server 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 Jun 7 08:35:08 2017

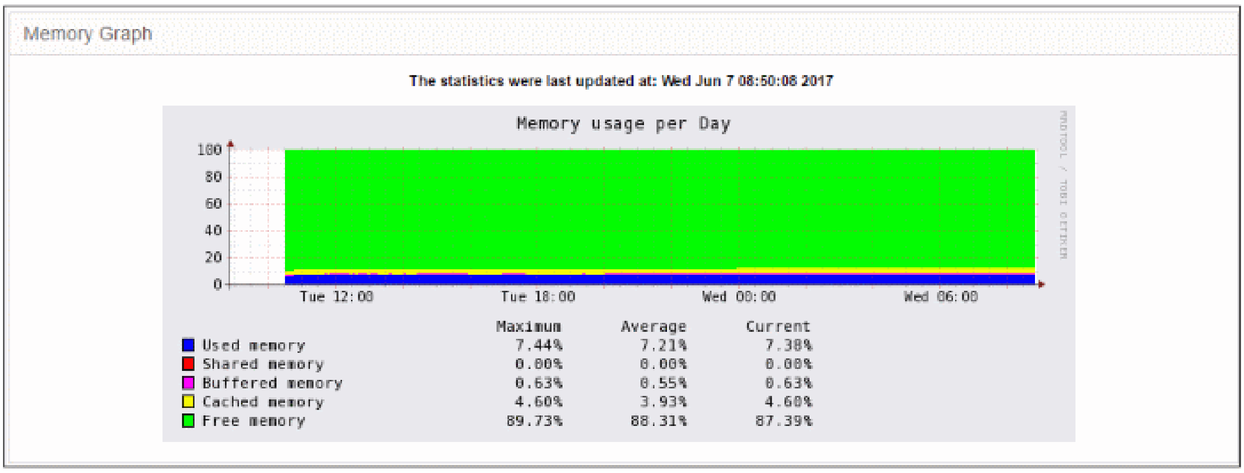
	Maximum	Average	Current
🟦 User CPU usage	1.12%	0.31%	0.35%
🟥 System CPU usage	0.34%	0.10%	0.09%
🟩 Idle CPU usage	99.69%	99.60%	99.55%

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 Jun 7 08:50:08 2017

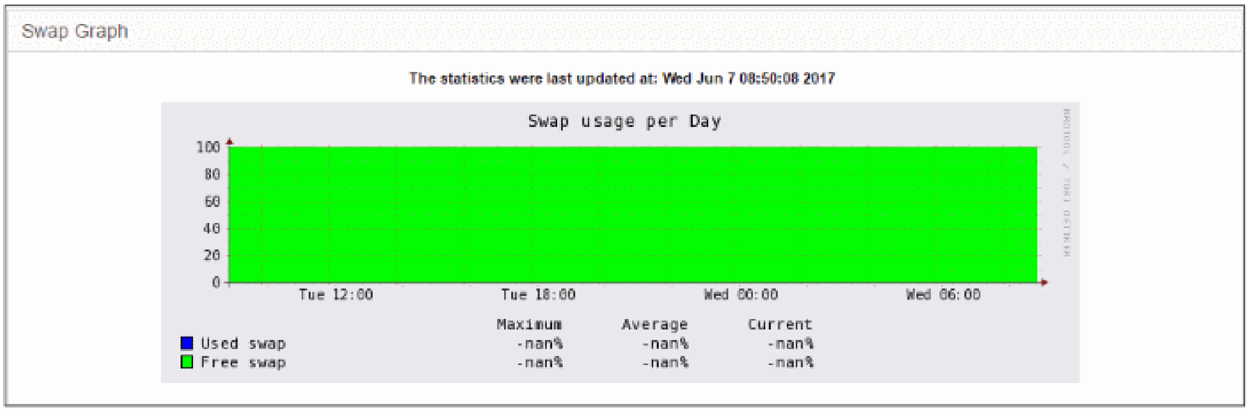
	Maximum	Average	Current
🟦 Used memory	7.44%	7.21%	7.38%
🟥 Shared memory	0.00%	0.00%	0.00%
🟪 Buffered memory	0.63%	0.55%	0.63%
🟨 Cached memory	4.60%	3.93%	4.60%
🟩 Free memory	89.73%	88.31%	87.39%

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

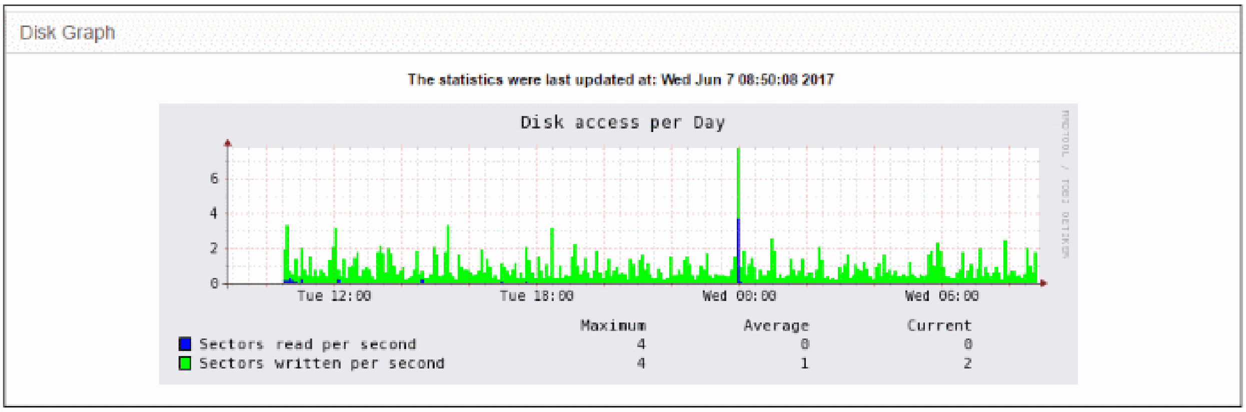
The statistics were last updated at: Wed Jun 7 08:50:08 2017

	Maximum	Average	Current
🟦 Used swap	-nan%	-nan%	-nan%
🟩 Free swap	-nan%	-nan%	-nan%

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 Jun 7 08:50:08 2017

	Maximum	Average	Current
🟦 Sectors read per second	4	0	0
🟩 Sectors written per second	4	1	2

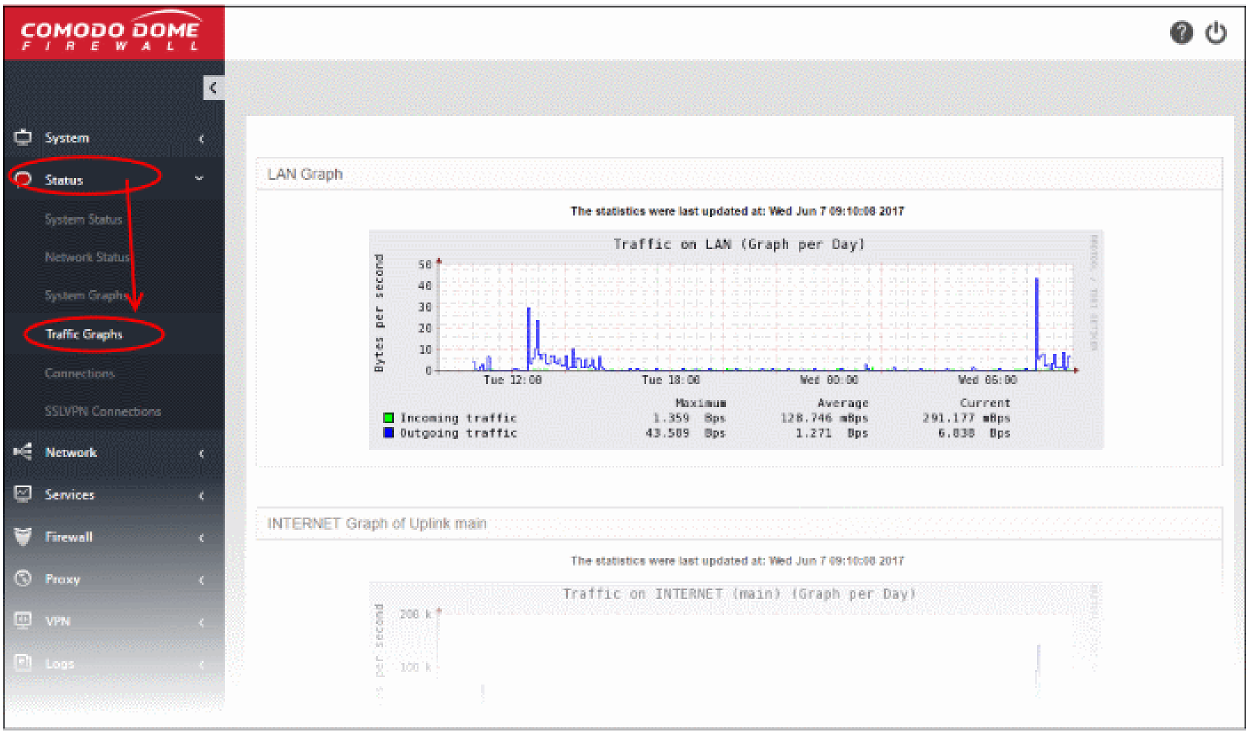
- Green - Percentage of sectors accessed for writing into the disk
- Blue - Percentage of sectors accessed for reading from the disk

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 and internet zone). The number of graphs shown on this page depends on the number of network zones configured in Dome CF.

To open the 'Traffic Graphs' interface, click 'Status' on the left then 'Traffic Graphs':



LAN Graph

The statistics were last updated at: Wed Jun 7 09:10:08 2017

```
                    Maximum       Average       Current
Incoming traffic    1.359  Bps    128.746 mBps  291.177 mBps
Outgoing traffic    43.589 Bps    1.271  Bps    6.838  Bps
```

INTERNET Graph of Uplink main

The statistics were last updated at: Wed Jun 7 09:10:08 2017

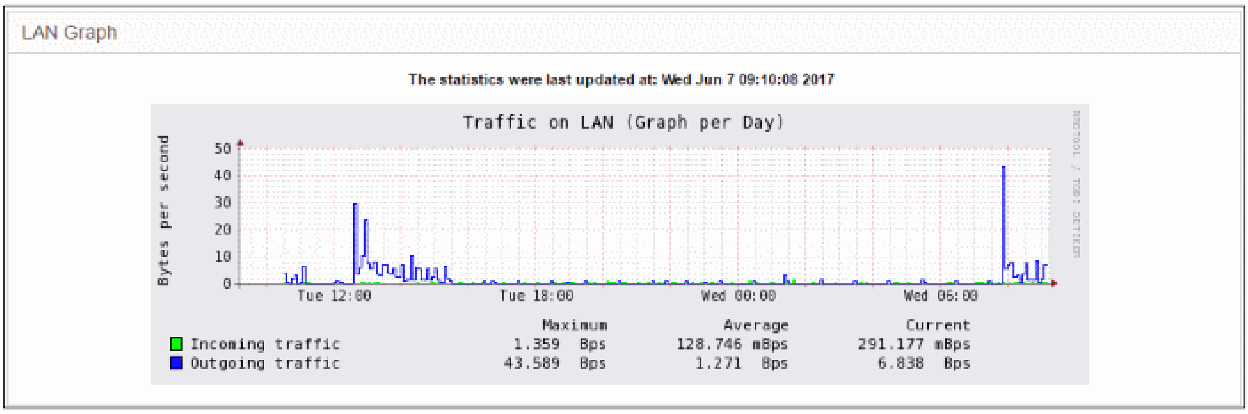
Click any graph to view traffic for the previous day, week, month and year. See the following links for more details:

- LAN Graph
- Uplink Graphs

LAN Graph

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

- Green - Incoming traffic
- Blue - Outgoing traffic



LAN Graph

The statistics were last updated at: Wed Jun 7 09:10:08 2017

```
                      Maximum        Average         Current
🟩 Incoming traffic    1.359  Bps    128.746 mBps    291.177 mBps
🟦 Outgoing traffic   43.589  Bps      1.271  Bps      6.838  Bps
```

The table below the graph shows maximum, average and current data traffic through the local network for the past day. Click the graph to view detailed traffic statistics for the past day, week, month and year.

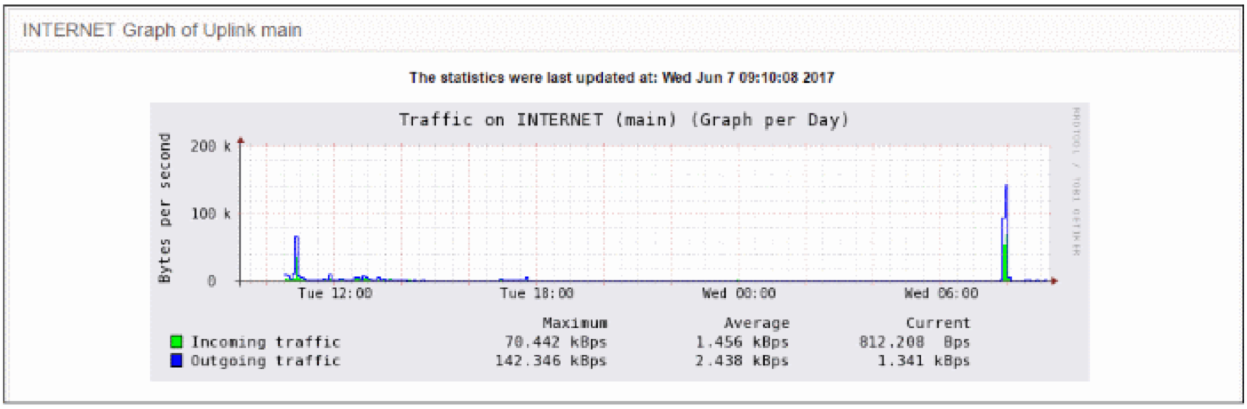
Uplink Graphs

The 'Uplink Graph' shows traffic through external network zones, like WANs, which are connected to the internet.

Note: Separate graphs will be shown for each uplink configured for your account.

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 Jun 7 09:10:08 2017

	Maximum	Average	Current
🟩 Incoming traffic	70.442 kBps	1.456 kBps	812.208 Bps
🟦 Outgoing traffic	142.346 kBps	2.438 kBps	1.341 kBps

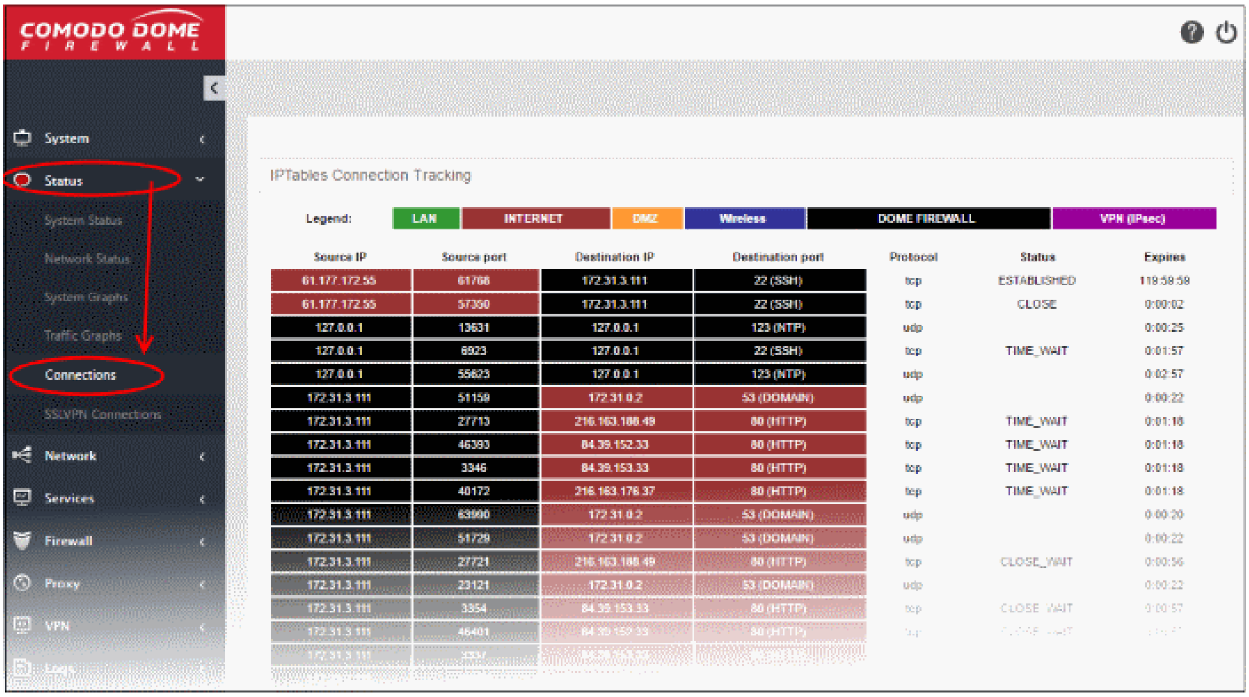
The table below the graph shows maximum, average and current traffic through the zone for the past day. Click the graph to view detailed traffic for the past day, week, month and year.

5.5 Network Connections

The 'Connections' interface displays current network connections to, from and through Dome CF. Each connection is shown with its source, destination, protocol and status. The cell colors in the table indicate the type of connection:

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

To open the 'IP Tables Connection Tracking' interface, click 'Status' on the left then 'Connections':



IPTables Connection Tracking

Legend: 🟩 LAN 🟥 INTERNET 🟧 DMZ 🟦 Wireless ⬛ DOME FIREWALL 🟪 VPN (IPsec)

Source IP	Source port	Destination IP	Destination port	Protocol	Status	Expires
61.177.172.55	61768	172.31.3.111	22 (SSH)	tcp	ESTABLISHED	119:59:58
61.177.172.55	57350	172.31.3.111	22 (SSH)	tcp	CLOSE	0:00:02
127.0.0.1	13631	127.0.0.1	123 (NTP)	udp		0:00:25
127.0.0.1	6923	127.0.0.1	22 (SSH)	tcp	TIME_WAIT	0:01:57
127.0.0.1	55623	127.0.0.1	123 (NTP)	udp		0:02:57
172.31.3.111	51159	172.31.0.2	53 (DOMAIN)	udp		0:00:22
172.31.3.111	27713	216.163.188.48	80 (HTTP)	tcp	TIME_WAIT	0:01:18
172.31.3.111	46393	84.39.152.33	80 (HTTP)	tcp	TIME_WAIT	0:01:18
172.31.3.111	3346	84.39.153.33	80 (HTTP)	tcp	TIME_WAIT	0:01:18
172.31.3.111	40172	216.163.176.37	80 (HTTP)	tcp	TIME_WAIT	0:01:18
172.31.3.111	63990	172.31.0.2	53 (DOMAIN)	udp		0:00:20
172.31.3.111	51729	172.31.0.2	53 (DOMAIN)	udp		0:00:22
172.31.3.111	27721	216.163.188.49	80 (HTTP)	tcp	CLOSE_WAIT	0:00:56
172.31.3.111	23121	172.31.0.2	53 (DOMAIN)	udp		0:00:22
172.31.3.111	3354	84.39.153.33	80 (HTTP)	tcp	CLOSE_WAIT	0:00:57
172.31.3.111	46401	84.39.152.33	80 (HTTP)	tcp	CLOSE_WAIT	[illegible]
172.31.3.111	3357	[illegible]	[illegible]			

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, Close, Time_Wait, Close_Wait and Syn_Recv.
Expires	Indicates the time the connection remained in the same status.

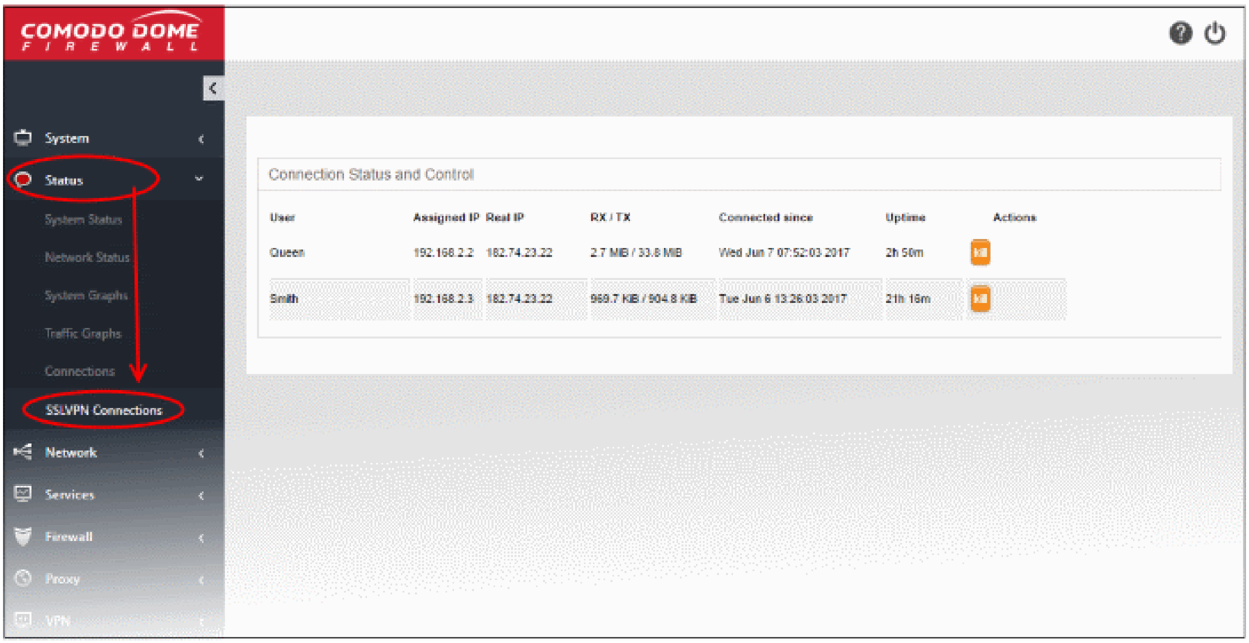
- Clicking an IP address will provide 'WHOIS' data
- Clicking a port number will lead to 'Internet Storm Center' webpage providing details of the port activity such as which services used that port including any exploits and the number of attacks received.

5.6 SSLVPN Connections

The 'SSLVPN Connections' interface lists SSL VPN users that are connected to Dome CF. See '**Configuring Virtual Private Network Settings**' for more details.

Administrators view connection details and can terminate user connections from this interface.

To open the interface, click 'Status' on the left then 'SSL VPN Connections':



Connection Status and Control

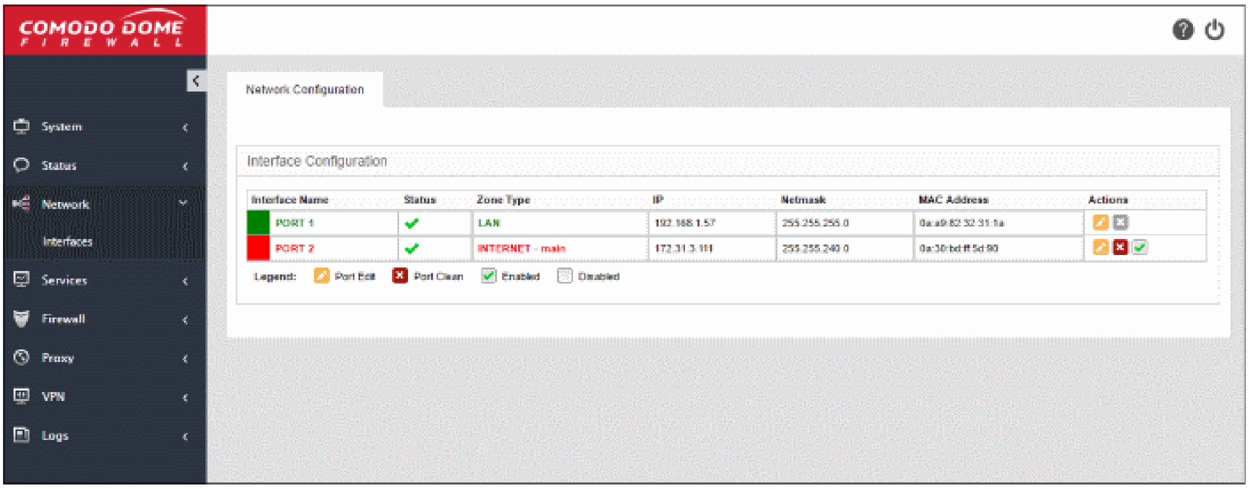
User	Assigned IP	Real IP	RX / TX	Connected since	Uptime	Actions
Queen	192.168.2.2	182.74.23.22	2.7 MiB / 33.8 MiB	Wed Jun 7 07:52:03 2017	2h 50m	kill
Smith	192.168.2.3	182.74.23.22	969.7 KiB / 904.8 KiB	Tue Jun 6 13:26:03 2017	21h 16m	kill

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 CF.
Real IP	The original externally facing IP address of the client.
RX / TX	Displays data transmitted and received by Dome CF 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 - Terminates the connection.

6 Network Configuration

The 'Network Configuration' screen shows settings configured by Comodo to connect your networks/clients to LAN and/or internet zones.

To open the 'Interface Configuration' screen, click 'Network' on the left then 'Interfaces':



Interface Configuration

Interface Name	Status	Zone Type	IP	Netmask	MAC Address	Actions
🟩 PORT 1	✓	LAN	192.168.1.57	255.255.255.0	0a:a9:82:32:31:1a	✎ ☒
🟥 PORT 2	✓	INTERNET - main	172.31.3.111	255.255.240.0	0a:30:bd:ff:5d:90	✎ ☒ ☑

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

The 'Interface Configuration' table shows interface devices configured by Comodo with their status and other details.

Interface Configuration Table - Column Descriptions	
Column Header	**Description**
Interface Name	Name of the CF port. The font color indicates the type of network zone to which the port is connected. Red - External networks, like WAN, for internet connection Green - Local Area Network to which workstations are connected
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
IP	LAN - The network IP address range. Internet – The IP address configured by Comodo to connect to external network .
Netmask	The netmask of the IP
MAC Address	The Media Access Control (MAC) address details.
Actions	Displays control buttons for editing and deleting the port entries. ✎ - Opens connection settings and allows you to edit the parameters of the interface. See '**Updating Network Interfaces**' for more details. ☒ - 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.

Updating Network Interfaces

The interfaces configured by Comodo can be updated for both LAN and Internet interfaces such as IP address / Netmask, primary DNS and secondary DNS. The following sections provide detailed explanations on updating the network zone interfaces:

- Updating WAN network zone to connect to the internet
- Updating LAN network zone

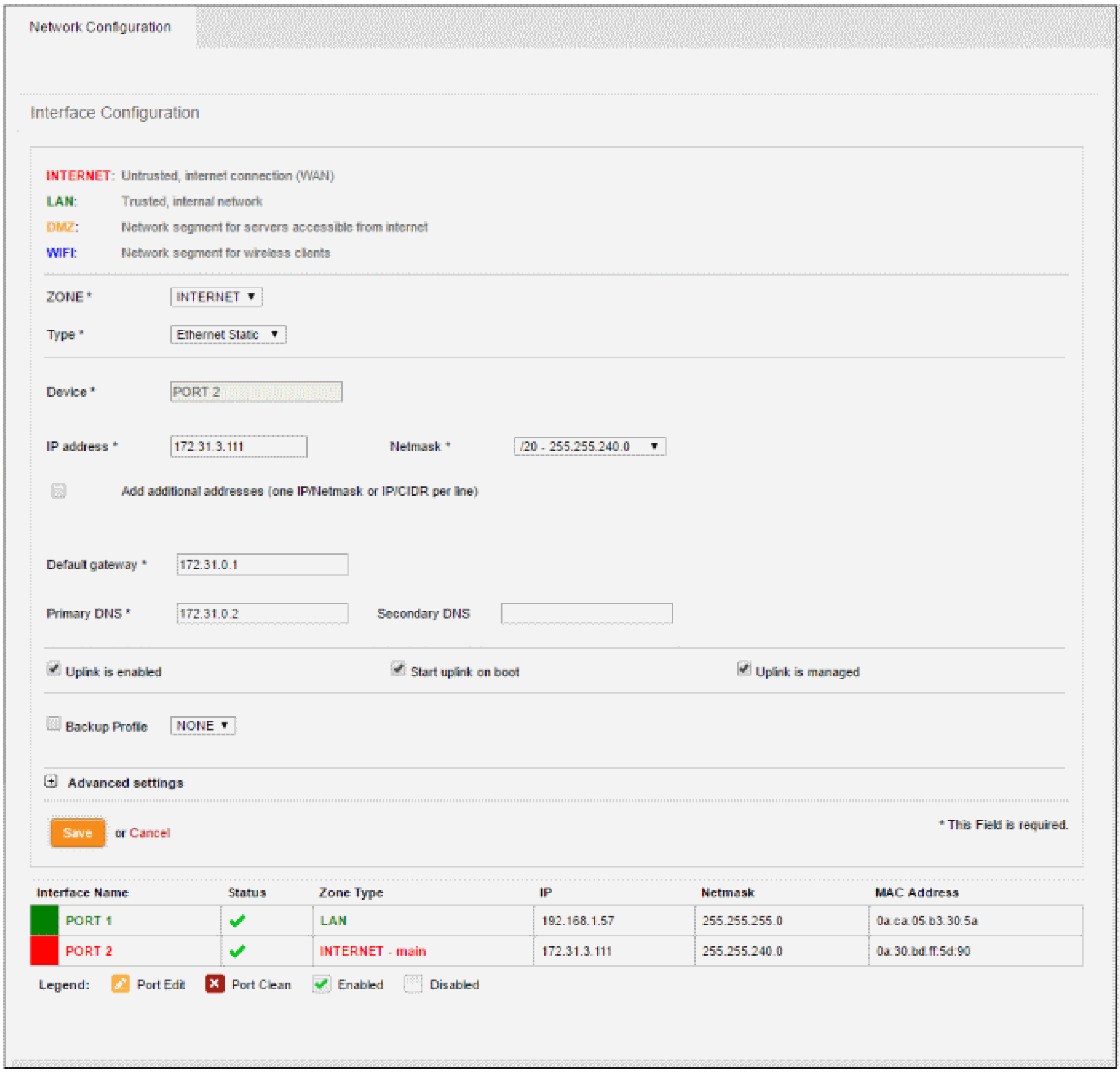
Updating WAN network zone to connect to the internet

The external network interface is configured by Comodo and you can update the DNS and advanced settings only.

To update 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.

The pane for configuring the network interface device will open.



Network Configuration

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 2

IP address * 172.31.3.111 Netmask * /20 - 255.255.240.0 ▼

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

Default gateway * 172.31.0.1

Primary DNS * 172.31.0.2 Secondary DNS

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

□ Backup Profile NONE ▼

⊞ Advanced settings

* This Field is required.

Interface Name	Status	Zone Type	IP	Netmask	MAC Address
🟩 PORT 1	✓	LAN	192.168.1.57	255.255.255.0	0a.ca.05.b3.30.5a
🟥 PORT 2	✓	INTERNET - main	172.31.3.111	255.255.240.0	0a.30.bd.ff.5d:90

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

- Zone - This is pre-configured as 'INTERNET' and cannot be changed.
- Type - This is pre-configured as 'Ethernet Static' and cannot be changed.

Device Settings

- Device - The port to which the interface device is connected. The port is pre-selected and cannot be edited.
- IP Address – This is configured by Comodo and cannot be edited.
- Netmask - This is configured by Comodo and cannot be edited.
- Add additional addresses – Not applicable.
- Default gateway - This is configured by Comodo and cannot be edited.
- 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 by default. Deselect this checkbox if you don't want to enable the uplink device at this time. You can enable the uplink at a later time in two ways:
  - Select the checkbox in the 'Actions' column of the 'Interface Configuration' interface.
  - Select the 'Active' checkbox beside the uplink in the Uplinks box from the Dashboard.
- Start uplink on boot - The uplink will start automatically on every restart of DCF. Deselect this checkbox if you want to manually start the uplink only when required.
- Uplink is managed - The uplink will be managed by DCF 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.
- 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 DCF 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.

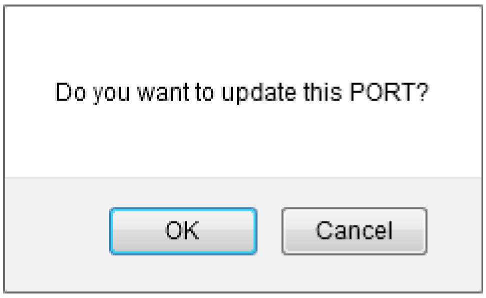
Advanced Settings:

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 - DCF 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.

DCF 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.

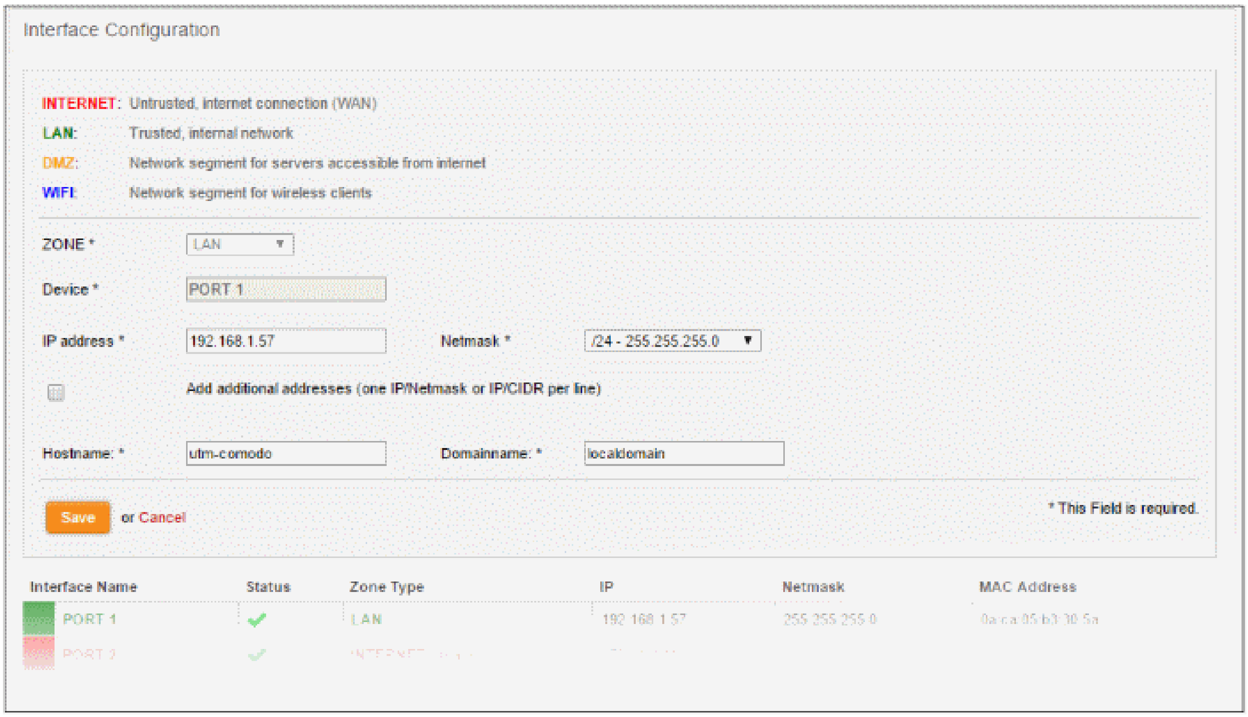
Tip: You can edit the network configuration e.g. for changing selected parameters like hostname or the network range of a zone, at any time depending on changes in your network. Click Network > Interface, click the 'Edit icon' in the 'Internet' row of the table, make the changes and save the changes.

Updating LAN network zone

The setup for internal networks involves configuring network parameters and preferences for the LAN zone.

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 1
IP address *: 192.168.1.57 Netmask *: /24 - 255.255.255.0
□ Add additional addresses (one IP/Netmask or IP/CIDR per line)
Hostname: *: utm-comodo Domainname: *: localdomain

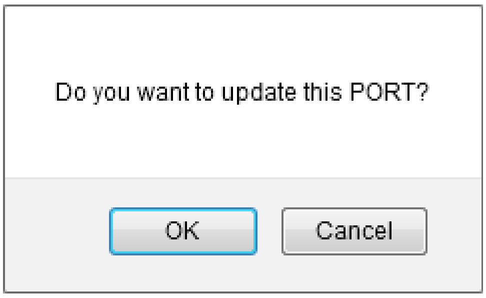
* This Field is required.

Interface Name	Status	Zone Type	IP	Netmask	MAC Address
🟩 PORT 1	✓	LAN	192.168.1.57	255.255.255.0	0a:ca:05:b3:30:5a
🟥 PORT 2	✓	INTERNET	[illegible]		

- Zone - Displays 'LAN' by default. This cannot be edited.
- Device - The port to which the interface device is connected. The port is pre-selected and cannot be edited.
- IP Address - Enter your network IP address range

  - Netmask – The netmask of the IP
  - 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.

DCF will restart for your settings to take effect.

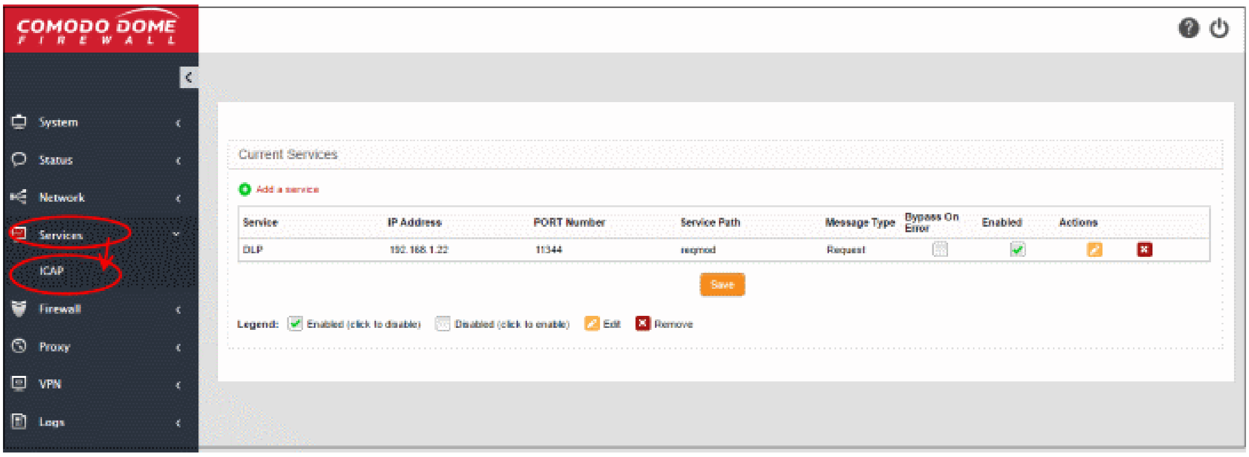
  - Network configuration activities like date, time, type of event, subject id, component name and the event outcome are logged.

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.

7 Configuring ICAP Services

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 MyDLP data loss prevention software.

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

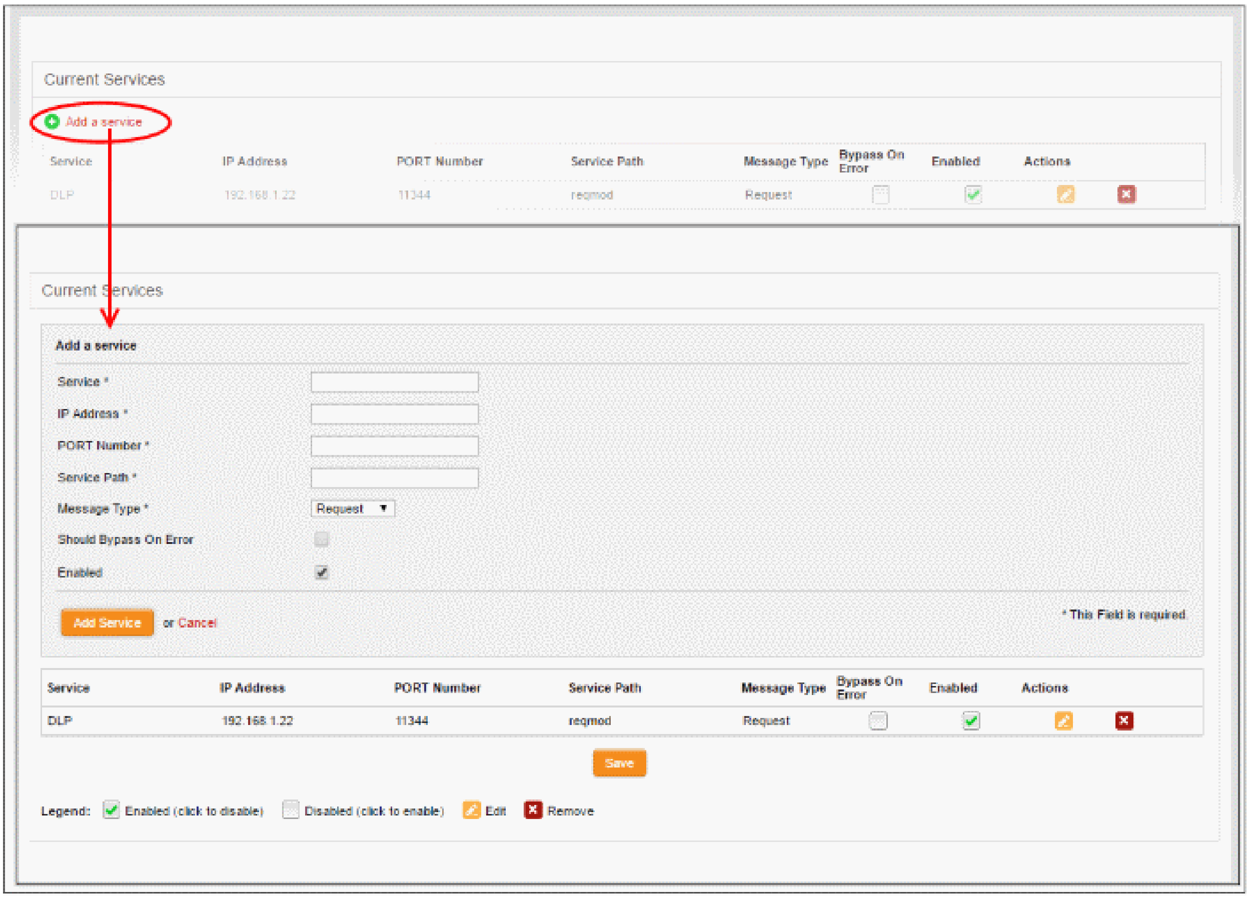


Service	IP Address	PORT Number	Service Path	Message Type	Bypass On Error	Enabled	Actions	
DLP	192.168.1.22	11344	reqmod	Request	□	☑	✎	☒

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

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
DLP	192.168.1.22	11344	reqmod	Request	☐	☑	✎ ☒

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
DLP	192.168.1.22	11344	reqmod	Request	☐	☑	✎ ☒

Save

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

- Service - Enter the service name, for example : 'MyDLP'
- 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.

8 Managing Firewall Configuration

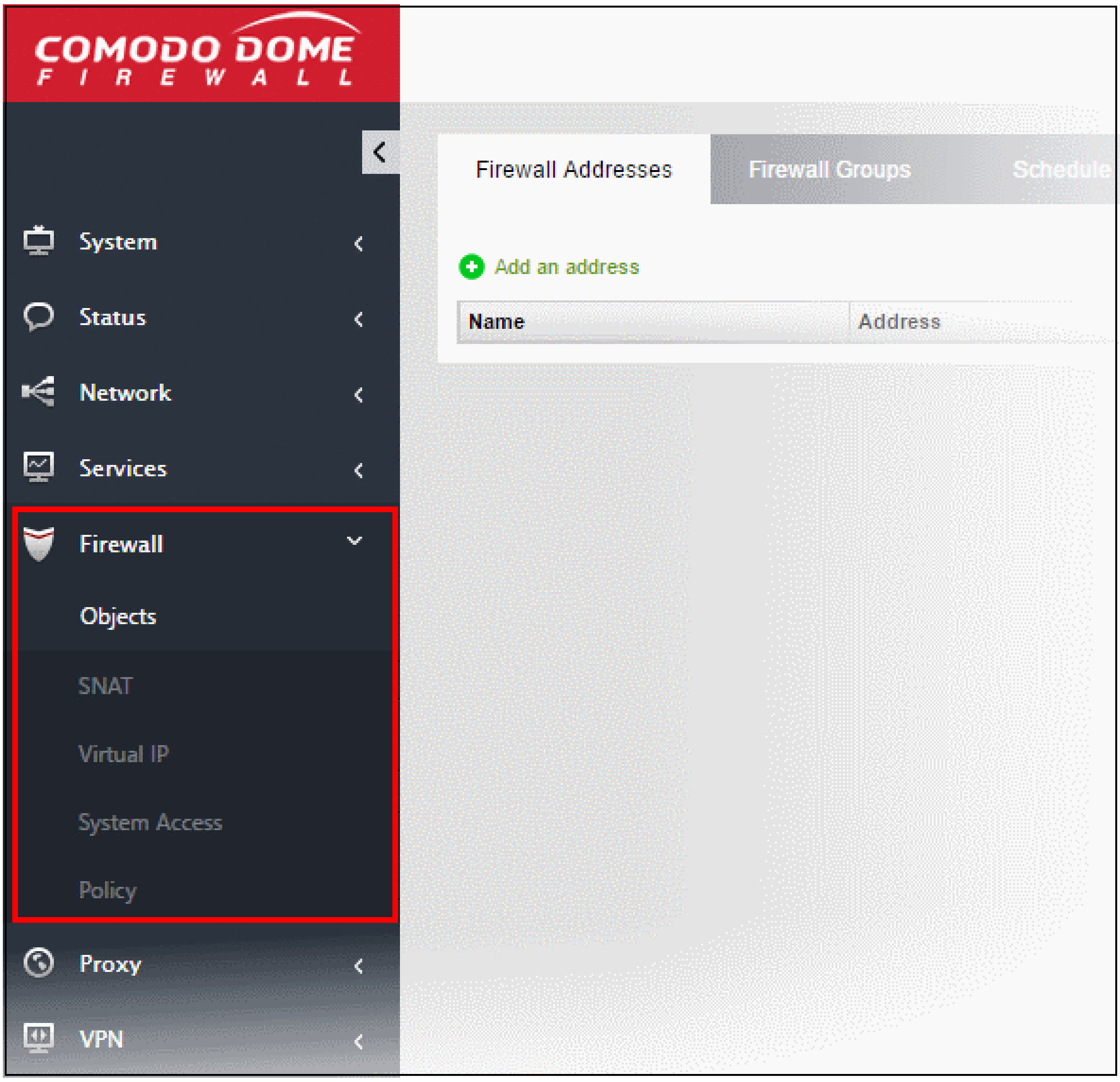
Dome Cloud Firewall provides enterprises with a highly configurable packet filtering firewall which offers the highest levels of security against inbound and outbound threats.

Dome CF allows you to create rules for managing the following types of traffic:

- NAT - (Network address translation) Traffic from external sources directed to a host in the network (Virtual IP) with port forwarding
- Incoming traffic - Traffic from external network zones to specified 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 Dome CF
- VPN traffic - Traffic generated by VPN users
- System Access - Access to Dome CF

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

Clicking the 'Firewall' tab on the left opens a sub-menu which allows you to create and manage rules.



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**

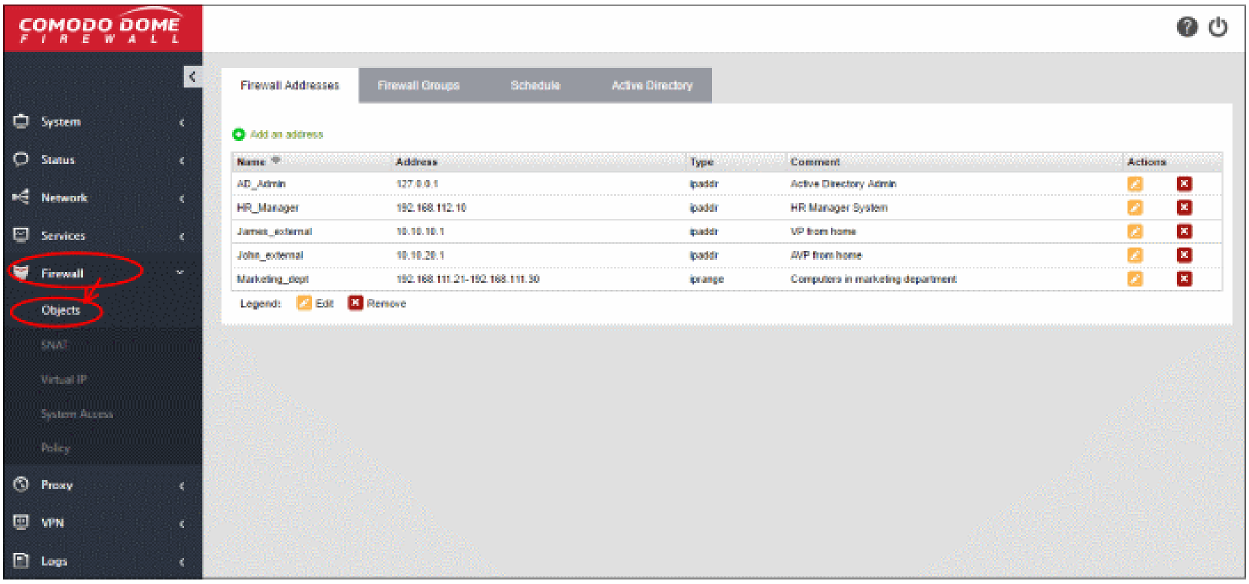
8.1 Firewall Objects

A firewall address object can be defined as a network IP address, a range of IP addresses, a sub-net of a host or a set of hosts and can be used to quickly reference these defined addresses/host in any firewall rules you create. Once defined, the object can be edited at any time to change the referenced host(s) and the change will be propagated to all firewall rules which include that object. This relieves administrators of the burden of editing each individual firewall rule.

A firewall object group can be defined with a group of firewall address objects, that enables the administrator to configure firewall rules for several objects at once, by just referencing the firewall group while configuring the rule.

The 'Firewall Objects' interface enables the administrator to create and manage firewall address objects and firewall object groups for use in configuring the firewall rules in Comodo Dome Cloud Firewall. Also the administrator can create a time schedule for the periods at which the Firewall needs to be active and configure integration with AD server for importing the users from the Active Directory.

To open the 'Firewall Objects' interface, click 'Firewall' on the left then 'Objects'



Name	Address	Type	Comment	Actions
AD_Admin	127.0.0.1	ipaddr	Active Directory Admin	✎ ☒
HR_Manager	192.168.112.10	ipaddr	HR Manager System	✎ ☒
James_external	10.10.10.1	ipaddr	VP from home	✎ ☒
John_external	10.10.20.1	ipaddr	AVP from home	✎ ☒
Marketing_dept	192.168.111.21-192.168.111.30	iprange	Computers in marketing department	✎ ☒

Legend: ✎ Edit ☒ Remove

The interface contains four tabs:

- **Firewall Addresses** - Allows the administrator to create and manage 'Firewall Address Objects'. See section '**Managing Firewall Address Objects**' for more details.
- **Firewall Groups** - Allows the administrator to create and manage 'Firewall Object Groups'. See section '**Managing Firewall Object Groups**' for more details.
- **Schedule** - Allows the administrator to create schedule objects that cover set the time periods for which the firewall should be active. See section '**Managing Firewall Schedules**' for more details.
- **Active Directory** - Allows the administrator to integrate company's Active Directory (AD) server for importing users, adding them to firewall objects and using them in firewall rules created for the users. See section '**Active Directory Integration**' for more details.

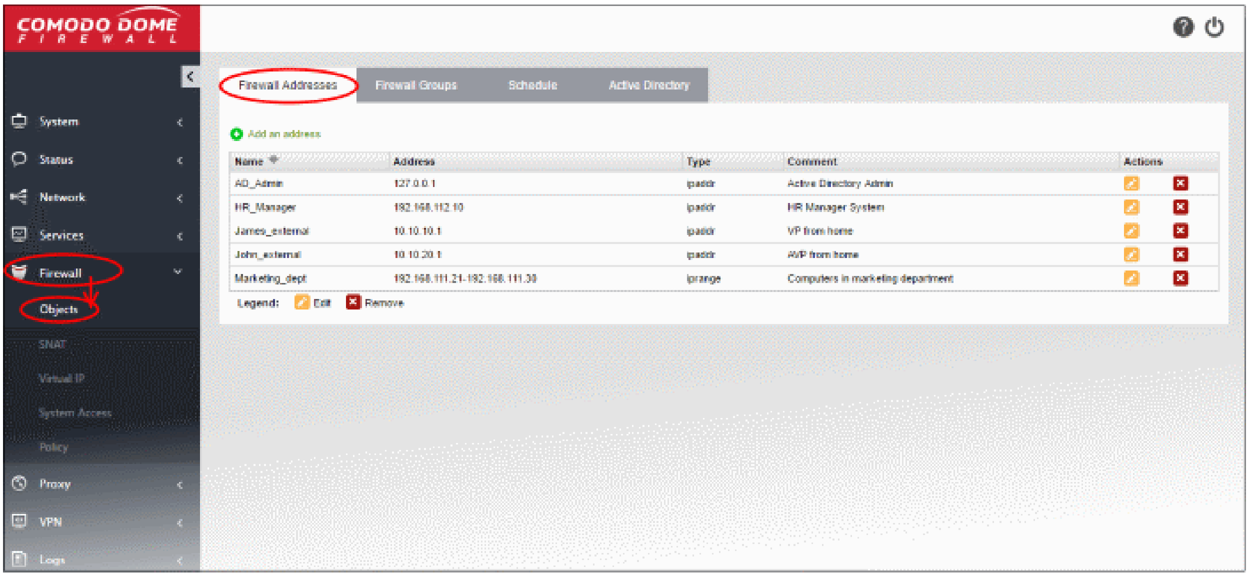
8.1.1 Managing Firewall Address Objects

'Firewall Address Objects' can be created to reference a specific host or a group of hosts in the internal network infrastructure. Instead of continually entering the IP address/IP address range/Subnet while creating firewall rules for a host computer or group, the administrator can just refer to the object name. If firewall rules are to be configured for a collection of objects, objects groups can be formed and can be referred to in the rule.

Firewall address objects can be edited at anytime. Any changes will be effected in all rules which include the object.

To create / manage firewall address objects

- Click 'Firewall' on the left hand side navigation then 'Objects'
- Open the 'Firewall Addresses' interface by clicking the 'Firewall Addresses' tab.



Name	Address	Type	Comment	Actions
AD_Admin	127.0.0.1	ipaddr	Active Directory Admin	
HR_Manager	192.168.112.10	ipaddr	HR Manager System	
James_external	10.10.10.1	ipaddr	VP from home	
John_external	10.10.20.1	ipaddr	AVP from home	
Marketing_dept	192.168.111.21-192.168.111.30	iprange	Computers in marketing department	

The 'Firewall Addresses' interface displays a list of firewall address objects added to DCF and allows the administrator to create new objects.

Firewall Address Objects Table - Column Descriptions	
Column	Description

Name	The name of the firewall address object.
Address	The IP address(s) of the host computer(s) contained in the object.
Type	The reference type of the hosts in the object. It can be IP address, IP address range or Subnet.
Comment	A short description of the object.
Actions	Displays control buttons for managing the object. ✎ - Opens the 'Edit' interface and enables to edit the parameters of the object. The Edit interface is similar to 'Add Object' interface. See section '**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.

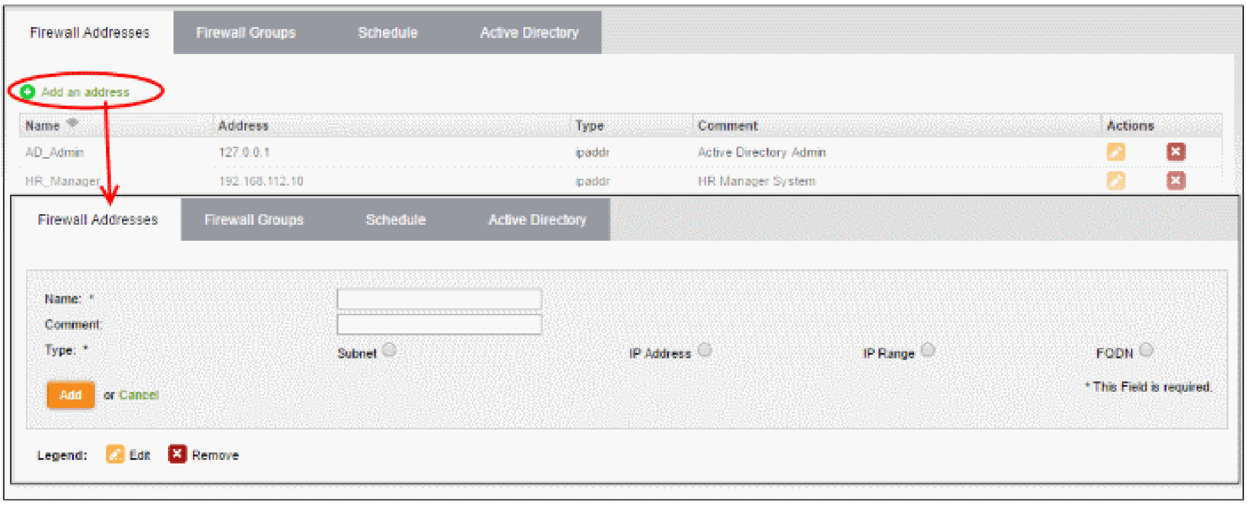
Creating a Firewall Address Object

The firewall address object can be created in two ways:

- From the 'Add an Address' pane by defining a name for the object and the, IP address, IP range or subnet of the host(s) to be included in the object. Refer to the **section below** for more details.
- Importing users from Active Directory. See section '**Adding User to Firewall Objects**' under the section '**Active Directory Integration**'.

To create a new object

- Click 'Firewall' > 'Objects' from the left hand side navigation and click the 'Firewall Addresses' tab.
- Click 'Add an address' at the top left



Name	Address	Type	Comment	Actions
AD_Admin	127.0.0.1	ipaddr	Active Directory Admin	✎ ✖
HR_Manager	192.168.112.10	ipaddr	HR Manager System	✎ ✖

Name: *

Comment:

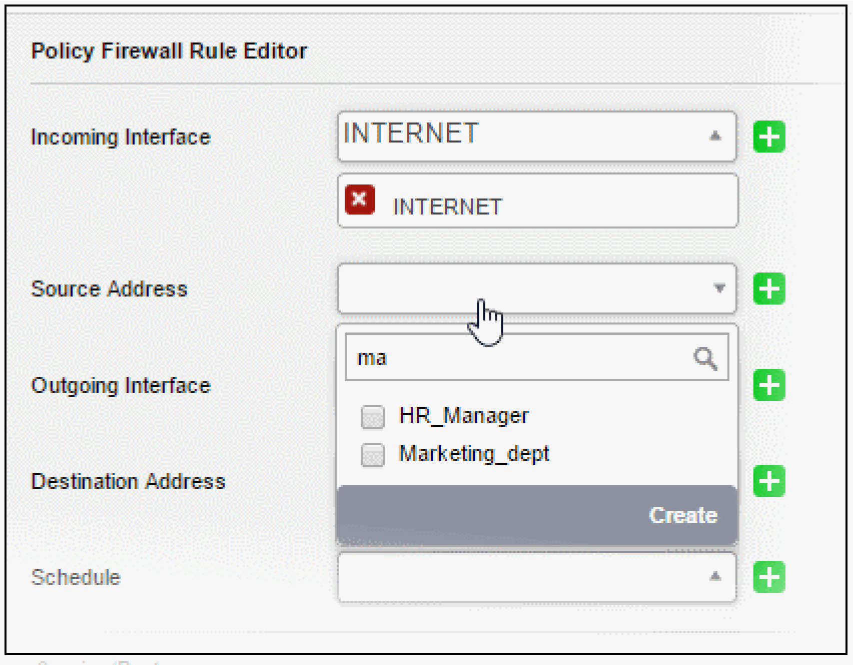
Type: * Subnet ○ IP Address ○ IP Range ○ FQDN ○

* This Field is required.

- Enter the parameters for the new object as shown below:
  - **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 a fully qualified domain name is to be covered by the object and enter the same.
- Click 'Add'. The new object will be added to the list.

The object will be available for selection for specifying source or destination while creating a firewall rule, by starting to type the first few letters of the object name.



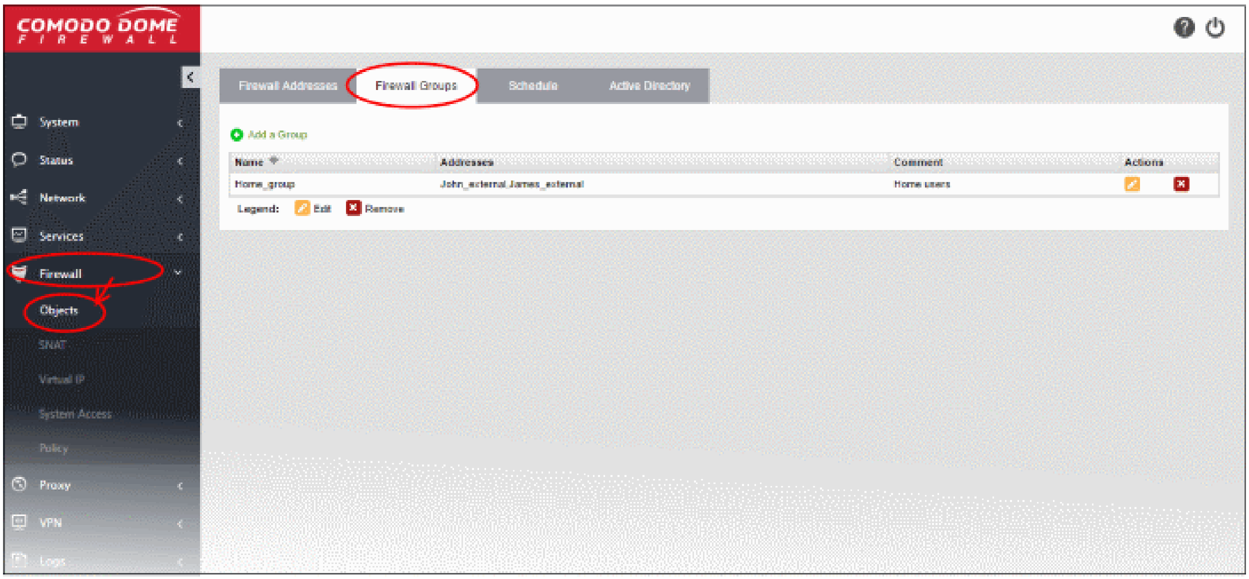
8.1.2 Managing Firewall Object Groups

Firewall object group can be created with a collection of firewall address objects, if the collection is required to be referenced as source and/or destination in the firewall rules configured in DCF.

The object groups can be edited at anytime to change the member objects included in it, and the change will be effected in all the firewall rules involving the object group, allowing collective management of different firewall rules at once.

To create / manage firewall address object groups

- Click 'Firewall' on the left hand side navigation then 'Objects'
- Open the 'Firewall Groups' interface by clicking the 'Firewall Groups' tab.



Name	Addresses	Comment	Actions
Home_group	John_external,James_external	Home users	

The 'Firewall Groups' interface displays a list of firewall address object groups added to DCF and allows the administrator to create and manage object groups.

Firewall Groups Table - Column Descriptions	
Column	**Description**
Name	The name of the firewall address object group.
Address	The member objects of the group.
Comment	A short description of the object group.
Actions	Displays control buttons for managing the object group. ✎ - Opens the 'Edit' interface and enables to edit the parameters of the object group. The Edit interface is similar to 'Add Group' interface. See '**Creating a Firewall Address Object Group**' for more details. ☒ - Removes the object group. **Note**: The object group which is currently referenced in a firewall rule cannot be removed. To remove a group, the group is to be first removed from the firewall rules in which it is included as source/destination.

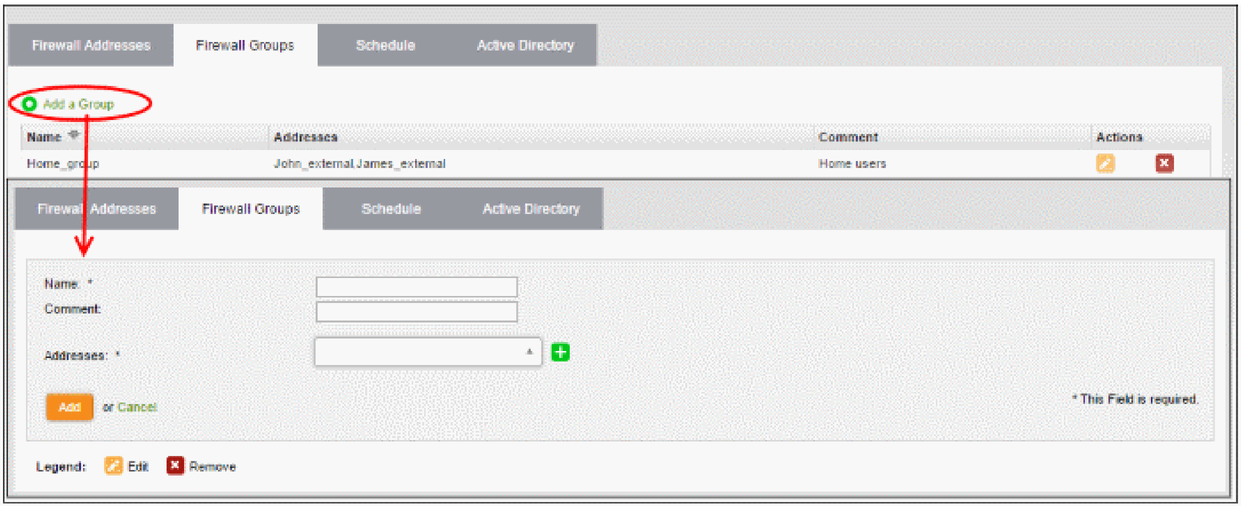
Creating a Firewall Address Object Group

The firewall object group can be created in two ways:

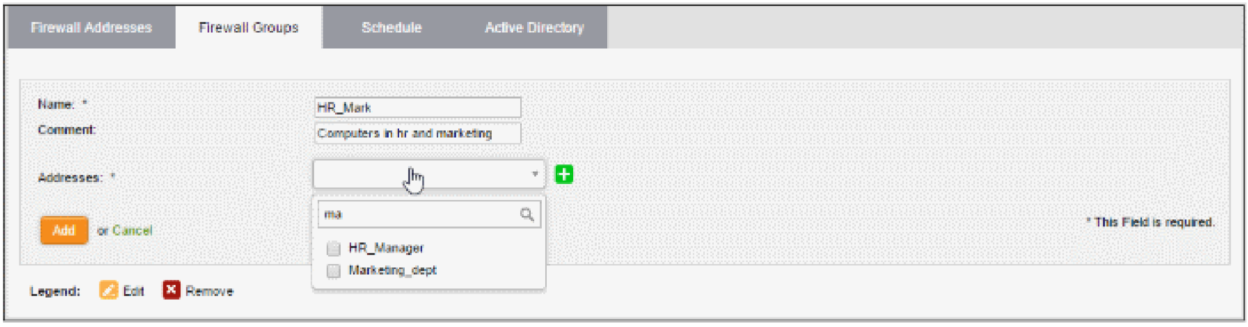
- From the 'Add a Group' pane by defining a name for the group and the member objects to be included in the group. Refer to the **section below** for more details.
- Importing users from Active Directory. See section '**Adding User Groups as Firewall Object Groups**' under the section '**Active Directory Integration**'.

To create a new object group

- Open the 'Firewall Groups' interface by clicking the 'Firewall Groups' tab under 'Firewall' > 'Objects'
- Click the 'Add a group' at the top left



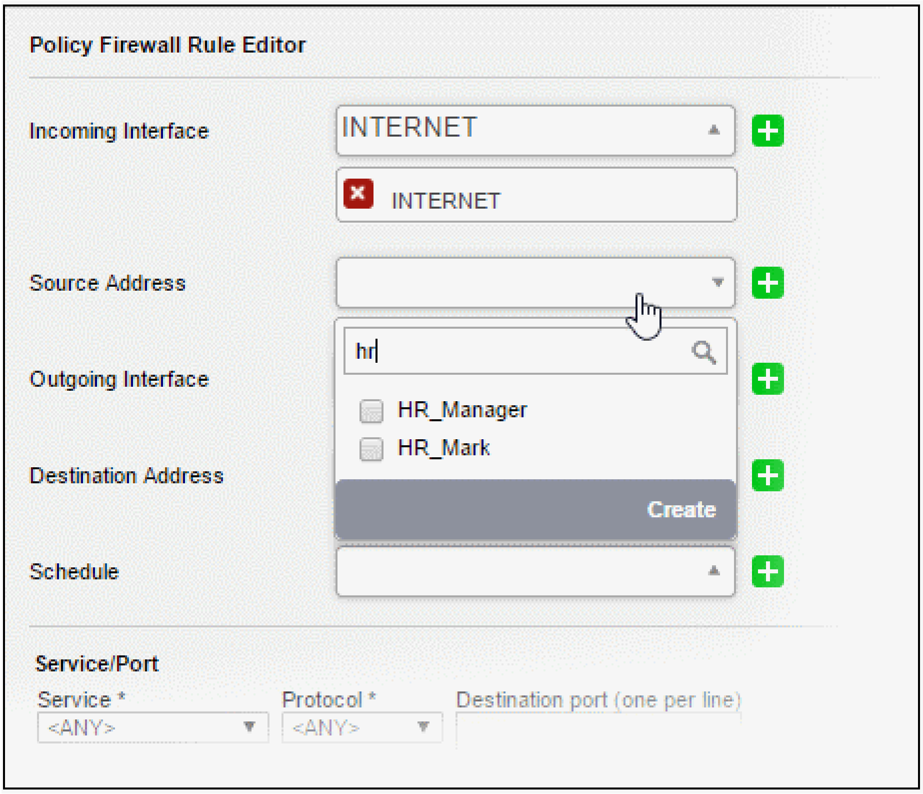
- Enter the parameters for the new group as shown below:
  - **Name -** Specify a name for the group (15 characters max).
  - **Comment -** Enter a short description of the group.
  - **Addresses -** Enter the names of the objects separated by comma, for inclusion in the group. Typing the first few letters of the name of an object will show the matching objects as a drop-down to select from.



Name: * HR_Mark
Comment: Computers in hr and marketing
Addresses: * ma

- Click 'Add'. The new object will be added to the list.

The group will be available for selection for specifying source or destination while creating a firewall rule, by starting to type the first few letters of the group name.



8.1.3 Managing Firewall Schedules

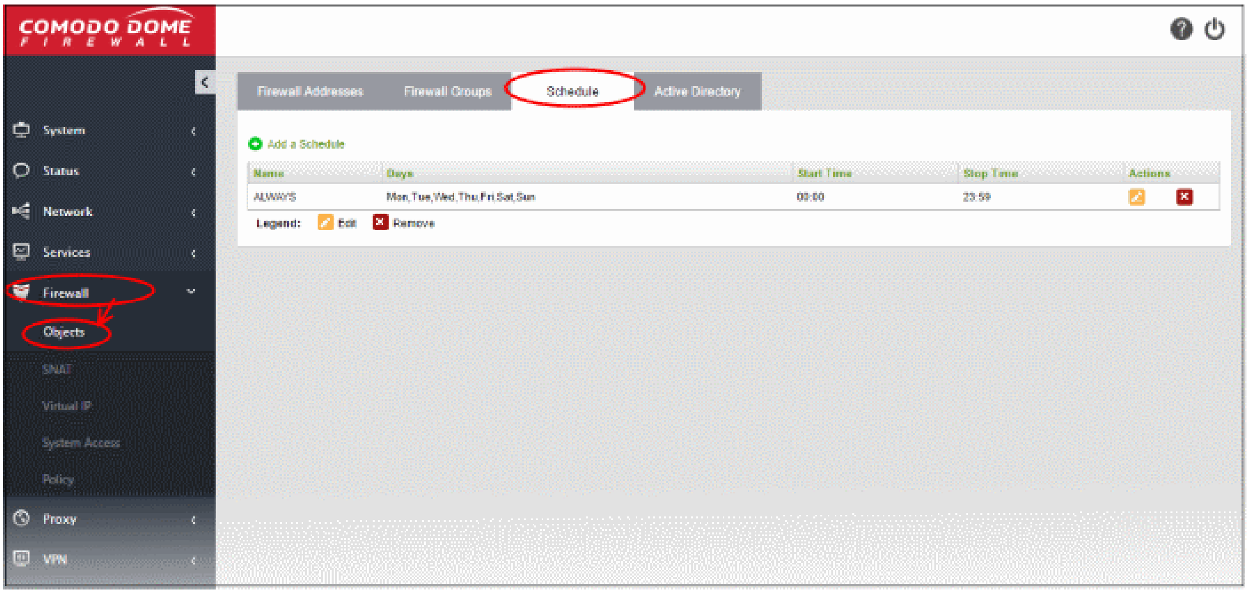
The 'Schedule' tab in 'Firewall' > 'Objects' allows you to specify the days and times when a firewall rule should be active. For example, it could be that a more restrictive firewall rule is applied on weekends and non-working hours than the one during working hours (when greater flexibility may be required).

Once a schedule object has been created in this interface, it can be applied it to a particular rule when creating or editing a rule in the 'Firewall' section. If the schedule of a rule needs to be changed, it is sufficient to edit the schedule object in this interface. The change will be propagated to all the rules to which the schedule object is applied.

DCF ships with a default and recommended schedule of 'Always' to keep the firewall activated at all times. Administrators may edit and create new schedules using the controls in the 'Actions' column.

To access the Schedule interface

- Click 'Firewall' > 'Objects' from the left hand side navigation
- Click the 'Schedule' tab



Name	Days	Start Time	Stop Time	Actions
ALWAYS	Mon,Tue,Wed,Thu,Fri,Sat,Sun	00:00	23:59	✎ ☒

Legend: ✎ Edit ☒ Remove

The 'Schedule' interface displays a list of existing schedule objects. Each schedule displays the days and times when the firewall will be active.

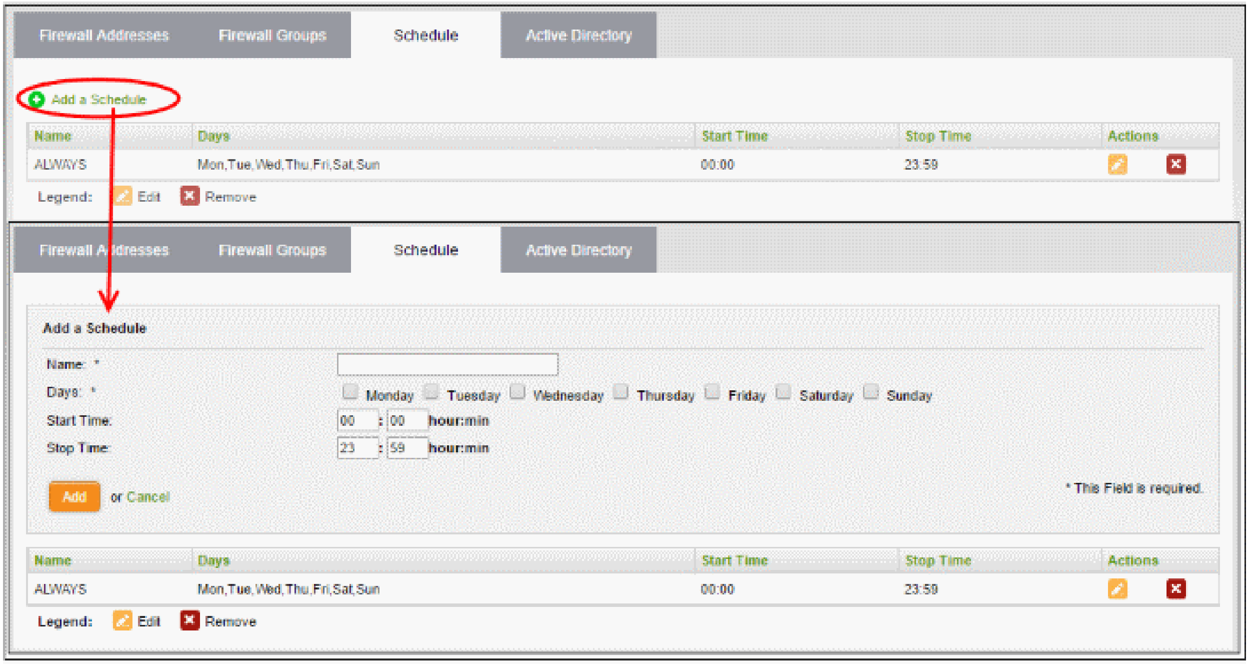
Schedules Table - Column Descriptions	
Column	**Description**
Name	Name of the schedule.
Days	The days of the week at which the rule is activated.
Start Time	The time at which the rule is started on the days listed in the 'Days' column.
Stop Time	The time at which the rule is disabled on the days listed in the 'Days' column.
Actions	Displays controls for managing the schedule. ✎ - Opens the 'Edit' interface and enables to edit the days and start and stop times of the rule. The Edit interface is similar to 'Add a Schedule' interface. See '**Creating a new Schedule**' for more details. ☒ - Removes the schedule.

Creating a new schedule

A new firewall schedule can be created from the 'Add a Schedule' pane by specifying the days and start/stop times for the rule.

To create a new schedule

- Open the 'Schedule' interface by clicking the 'Schedule' tab under 'Firewall' > 'Objects'
- Click 'Add a Schedule' at top left



Name	Days	Start Time	Stop Time	Actions
ALWAYS	Mon,Tue,Wed,Thu,Fri,Sat,Sun	00:00	23:59	✎ ✖

Legend: ✎ Edit ✖ Remove

Add a Schedule

Name: *

Days: * □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

Start Time: 00 : 00 hour:min

Stop Time: 23 : 59 hour:min

Add or Cancel

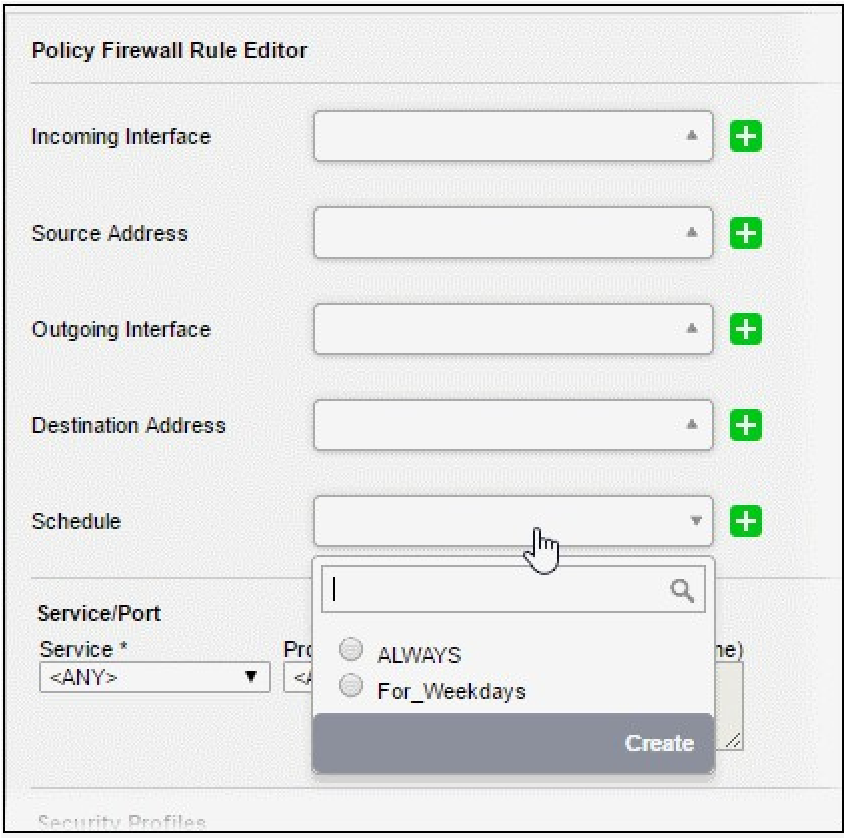
* This Field is required.

Name	Days	Start Time	Stop Time	Actions
ALWAYS	Mon,Tue,Wed,Thu,Fri,Sat,Sun	00:00	23:59	✎ ✖

Legend: ✎ Edit ✖ Remove

- Enter the parameters for the new schedule as shown below:
  - **Name -** Specify a name for the schedule.
  - **Days -** Select the days of the week at which the firewall should be active.
  - **Start Time and Stop Time -** Enter a time at which the firewall should be started and stopped at the selected days in 24 Hrs time format.
- Click 'Add' for the new schedule to be created.

The schedule will be available for selection while creating and editing individual firewall rules from the 'Policy Firewall' interface.



8.1.4 Active Directory Integration

Integrating Dome Cloud Firewall with your Active Directory (AD) server allows you to implement identity-based security on your network. Once a directory has been imported, DCF will map usernames to IP addresses, allowing you to apply firewall policies to individuals or groups.

DCF uses LDAP (Lightweight Directory Access Protocol) to import network users from the AD server, track login activity and regulate user traffic to and from the IP addresses.

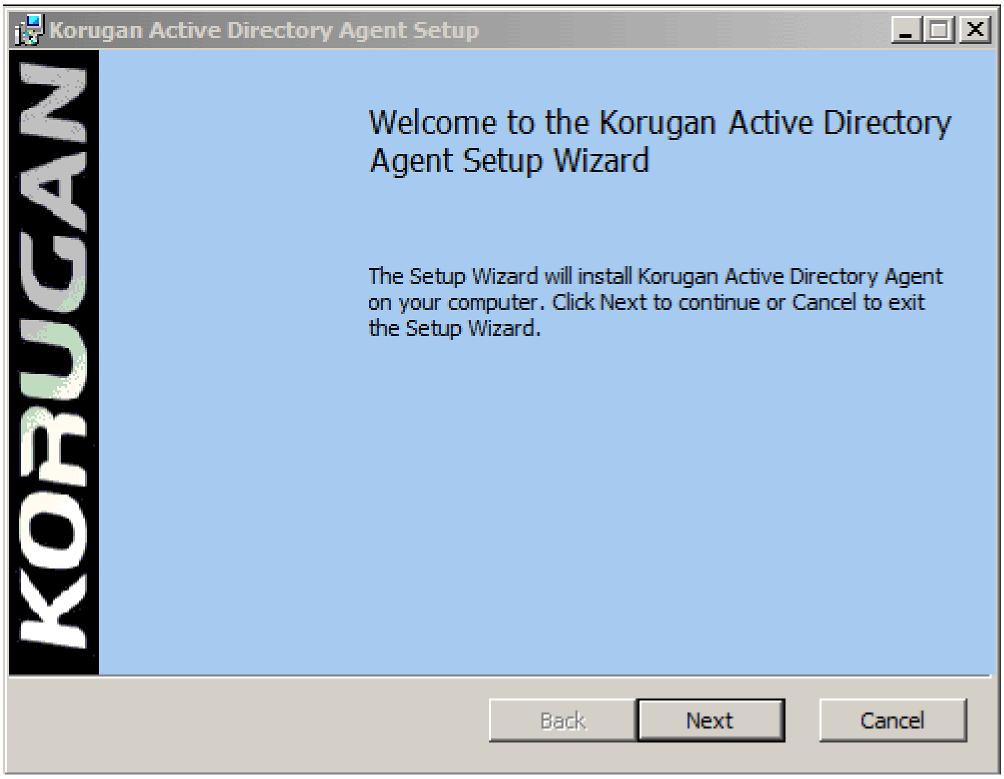
AD server integration involves four steps:

- Step 1- Install the Dome Cloud 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 Dome Cloud Firewall

Step 1- Install the Dome Cloud Firewall AD Agent onto the 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 DCF 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
2. Double-click the setup file to start the installation wizard.

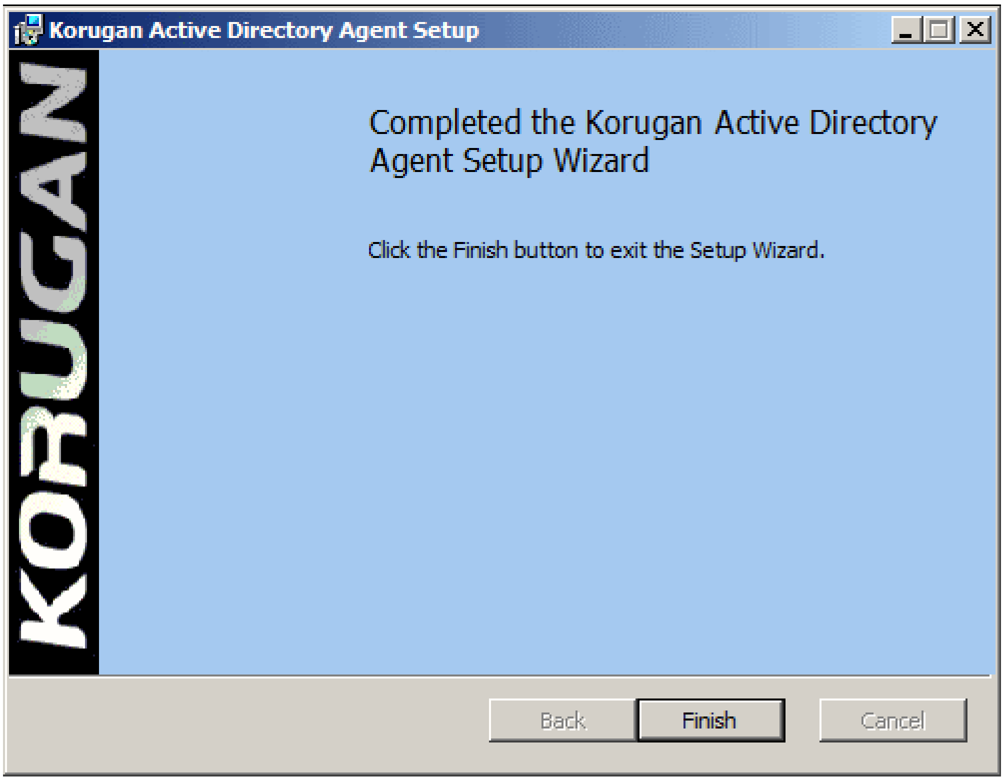


Korugan Active Directory Agent Setup

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 at C:\Program Files (32 bit system) or C:\Program Files (x86) (64-bit system).



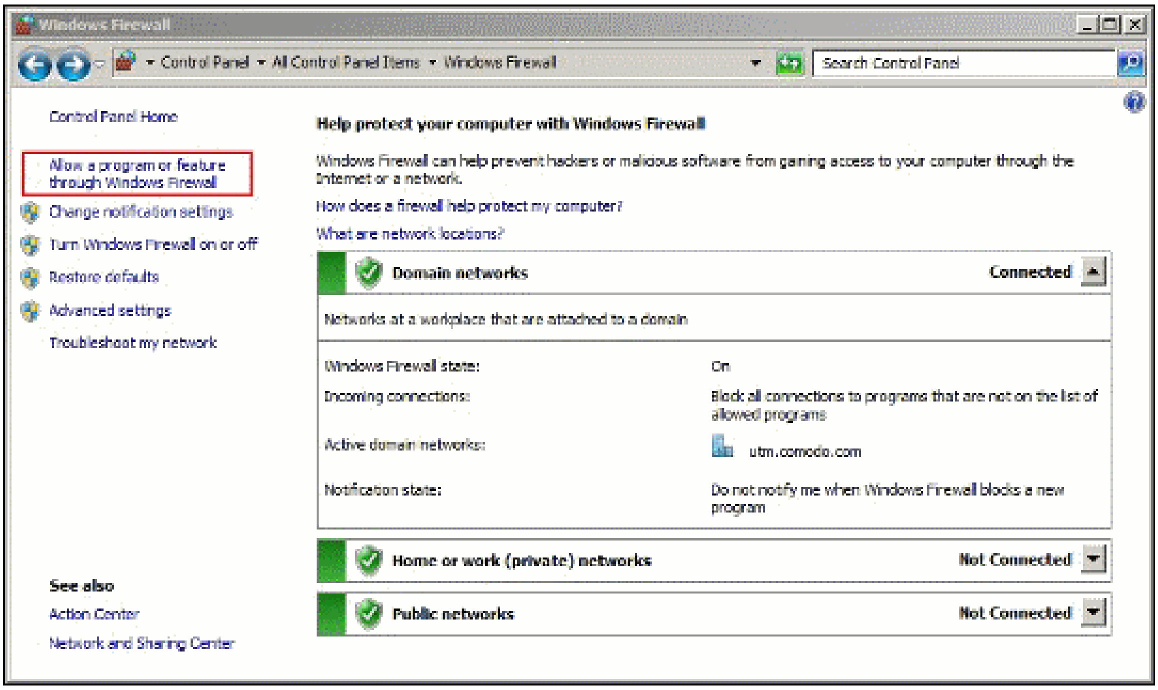
Completed the Korugan Active Directory Agent Setup Wizard

Click the Finish button to exit the Setup Wizard.

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

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 DCF.

1. Open the Windows Server Control Panel
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

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.

How does a firewall help protect my computer?

What are network locations?

Domain networks — Connected

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

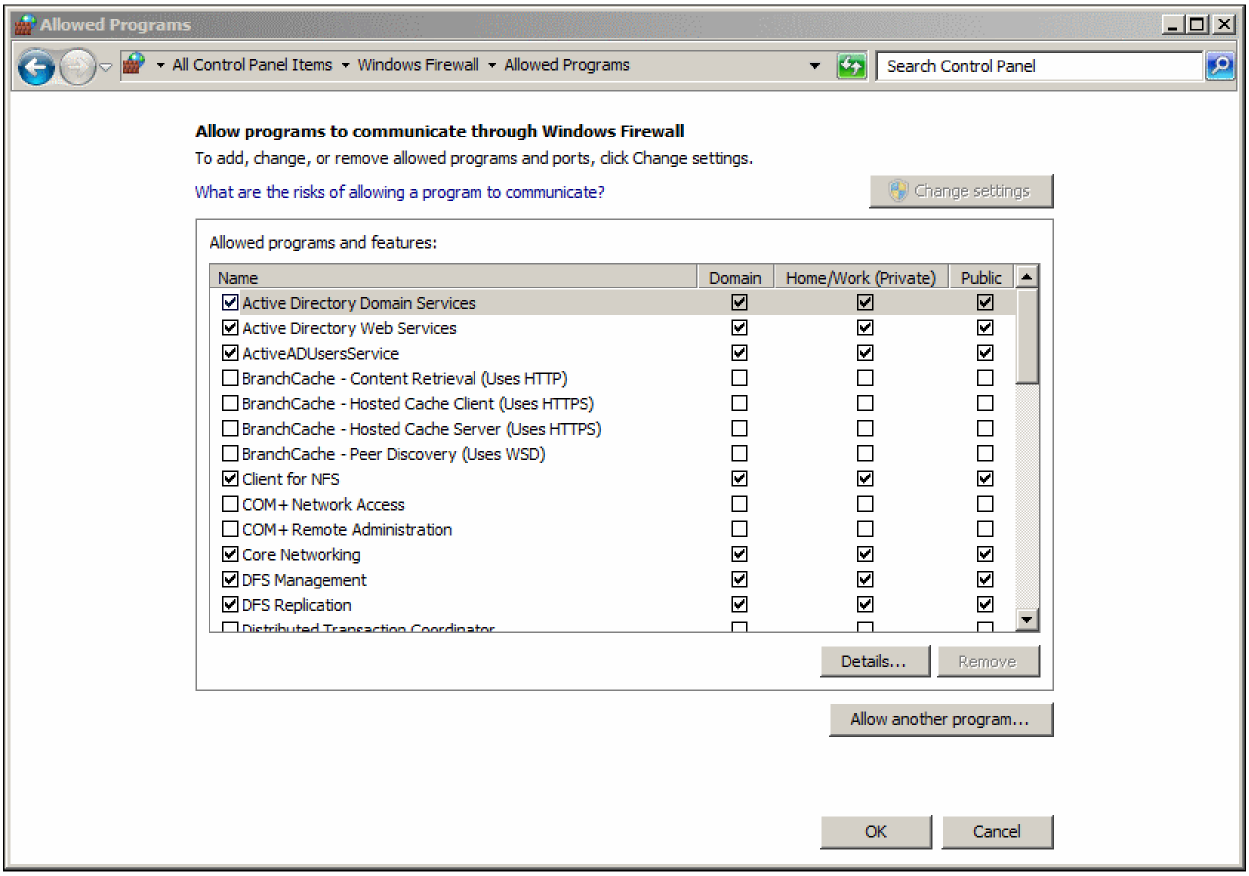
Active domain networks: utm.comodo.com

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

Home or work (private) networks — Not Connected

Public networks — Not Connected

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.

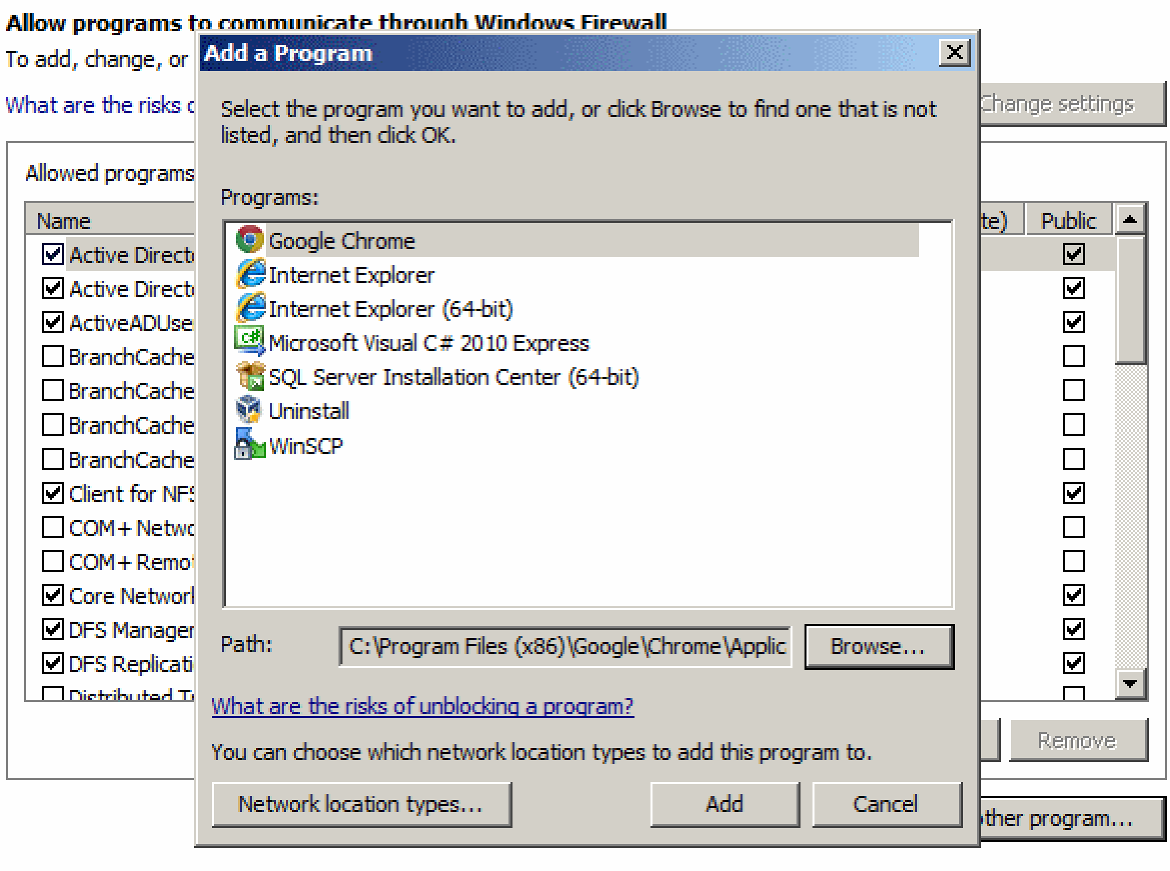
What are the risks of allowing a program to communicate?

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	☐	☐	☐

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 o

Change settings

Allowed programs

Name	te)	Public
☑ Active Directo		☑
☑ Active Directo		☑
☑ ActiveADUse		☑
□ BranchCache		□
□ BranchCache		□
□ BranchCache		□
□ BranchCache		□
☑ Client for NFS		☑
□ COM+ Netwo		□
□ COM+ Remo		□
☑ Core Networ		☑
☑ DFS Manager		☑
☑ DFS Replicati		☑
□ Distributed Tr		□

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.

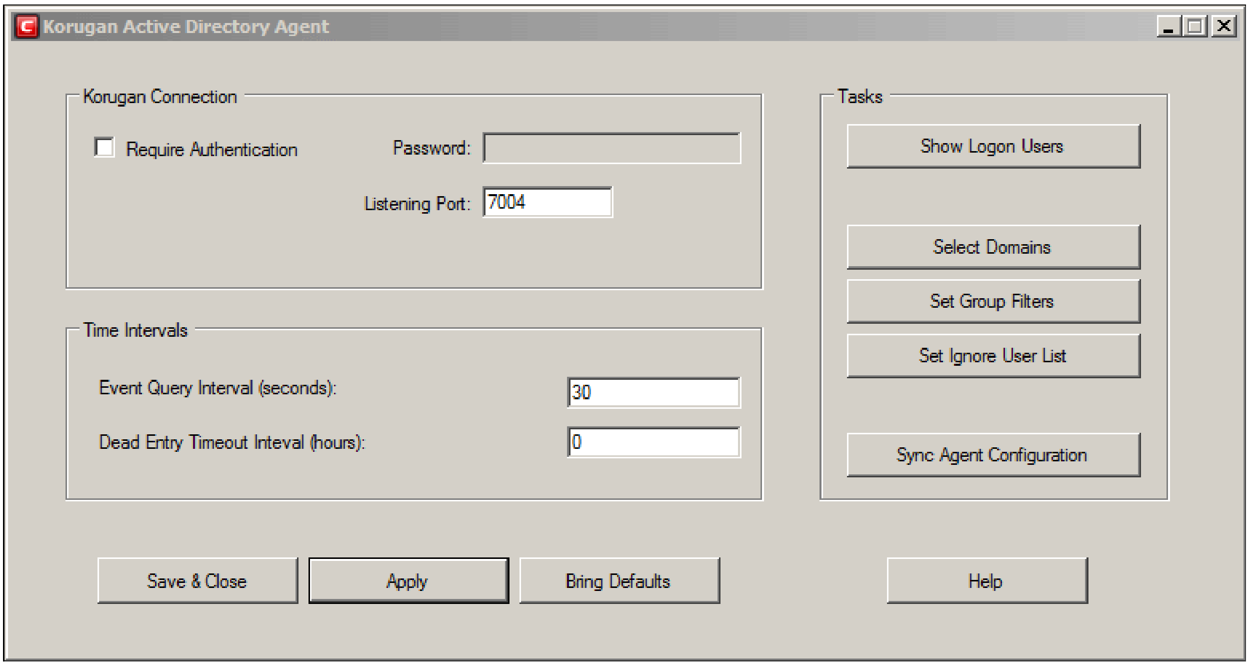
Network location types... | Add | Cancel

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 Dome Cloud Firewall.

1. Browse to the agent installation folder (C:\Program Files on 32-bit system and 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

Tasks

- Show Logon Users
- Select Domains
- Set Group Filters
- Set Ignore User List
- Sync Agent Configuration

Save & Close | Apply | Bring Defaults | Help

2. Configure the parameters as shown below:

Connection Parameters

- **Require Authentication -** If you require password authentication for DCF to connect to the server, enable 'Require Authentication' and specify the password.
- **Listening Port** - The agent communicates with DCF through port 7004 by default. 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 DCF for updates. It is recommended to set the interval according to the size of the directory. Directories with larger numbers of users should be checked more frequently.
- **Dead Entry Interval –** Dome Cloud Firewall will delete a username-IP map entry if a user has not logged-in for a certain period of time. For example, if the 'Dead Entry Interval' is set as 720 hours, then the username-IP map entry for the user will be deleted if the user does not login for 30 days.

Tasks

- **Show Logon Users –** Shows 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 specify users who should not be tracked.
- **Sync Agent Configuration -** Enables you to export the current configuration of the agent.

- Click 'Apply' to save your 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 DCF. The next step is to configure DCF to receive the connection.

Step 4 - Configure DCF

The next step is to configure DCF to communicate with the agent and the AD server.

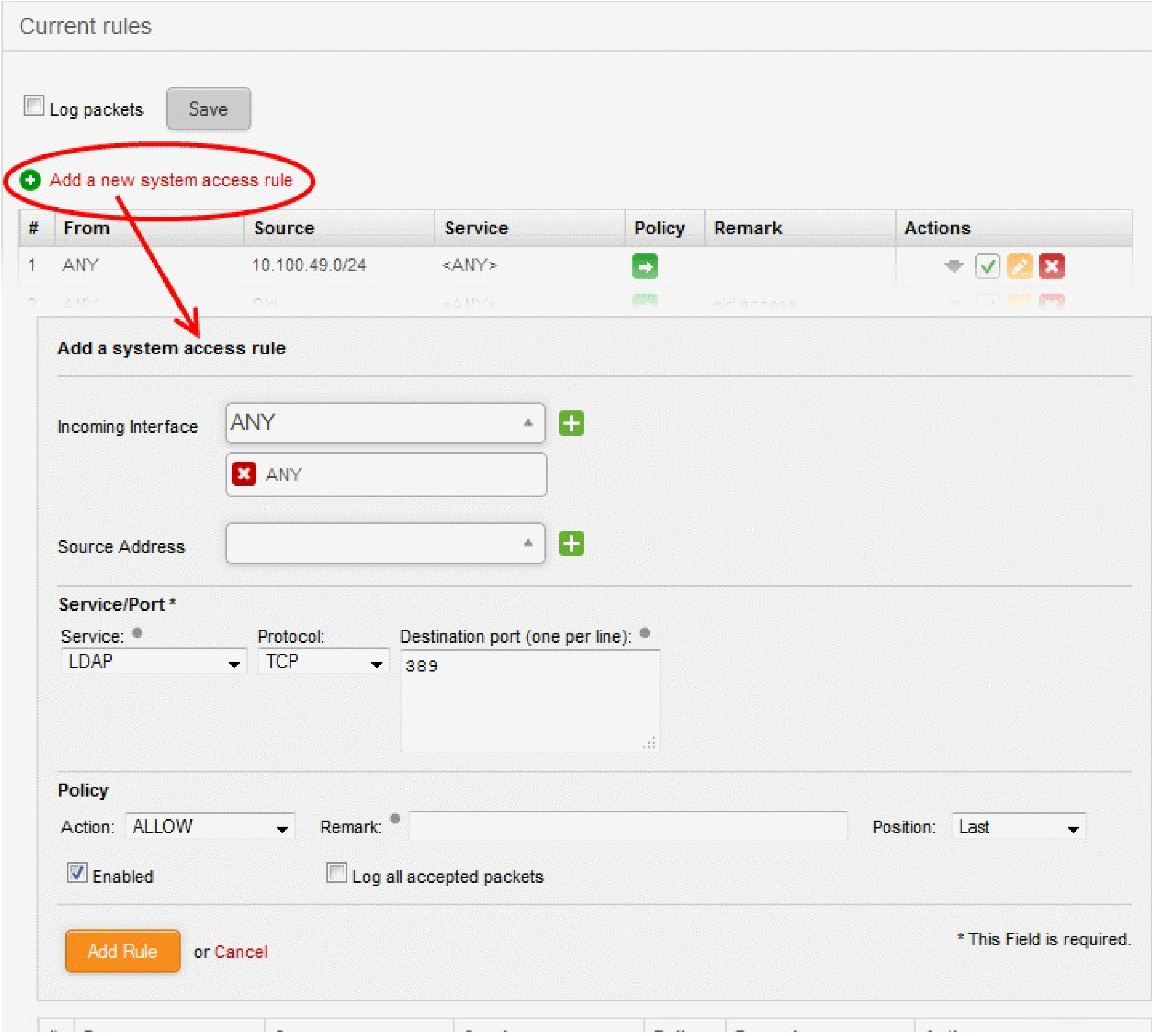
- In order to allow access to DCF, Firewall Rules are to be created under Firewall > System Access interface, specifying the IP address/port and the service details. Refer to the following section **Allowing Access to DCF** for more details on creating the system access rules. A detailed description of System Access rules can be found in the section **Configuring System Access**.
- You need to enter the IP address and port details of the server in the firewall console so it can receive the username/IP address map tables and updates from the agent. See **Configuring the Active Directory Connection** for more details.

Allow Access to DCF

'System Access' rules can be added to DCF as follows:

To add the rule for the server to access DCF

- Click 'Firewall' > 'System Access' to open the 'System Access' interface
- Click 'Add a new system access rule' link from the 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

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

- Enter the following settings:

Incoming Interface - Select 'Any' from the drop-down

Source Address - Need not select any firewall object

Service/Port - Select 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 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'

To add the rule for the agent to access DCF

- 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'.

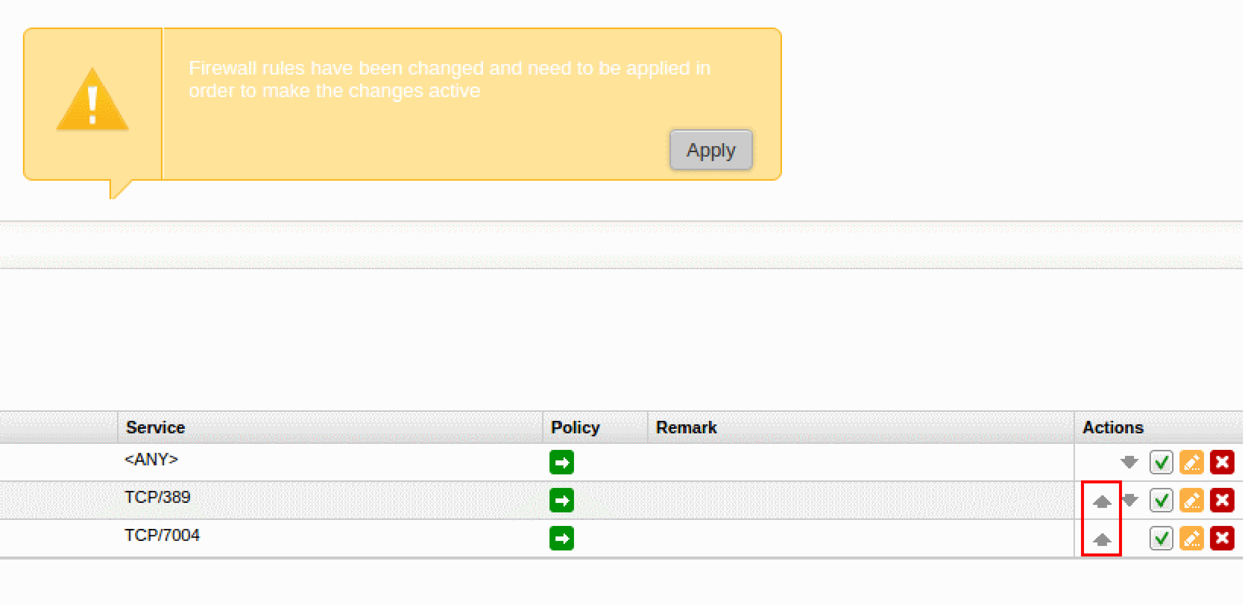
General Settings

- 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

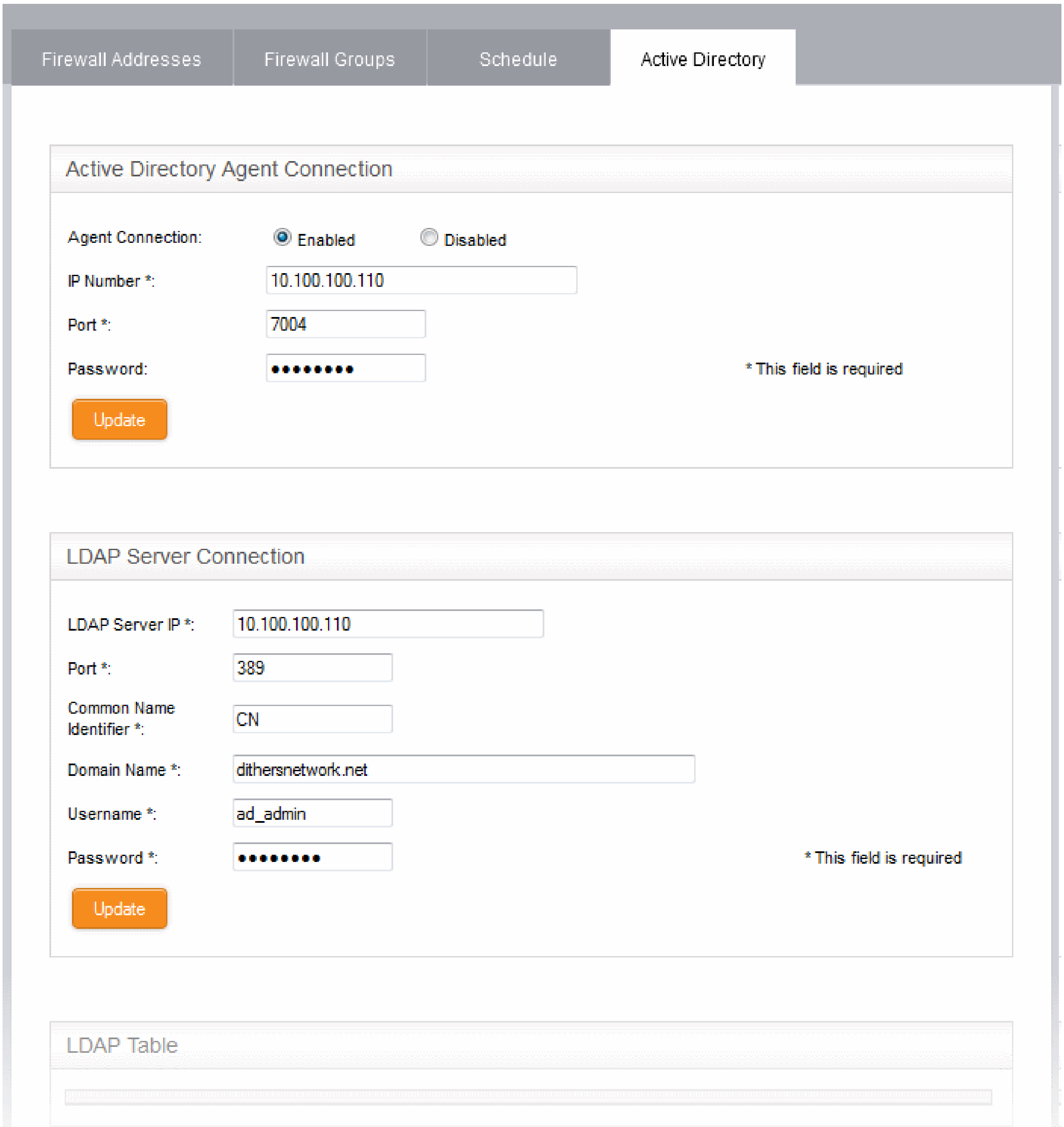
Service	Policy	Remark	Actions
<ANY>	➡		▼ ✓ ✎ ✖
TCP/389	➡		▲ ▼ ✓ ✎ ✖
TCP/7004	➡		▲ ✓ ✎ ✖

Configuring the Active Directory Connection

The Active Directory interface in the administrative console allows you to configure the 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 *: 10.100.100.110

Port *: 7004

Password: ●●●●●●●●

* This field is required

LDAP Server Connection

LDAP Server IP *: 10.100.100.110

Port *: 389

Common Name Identifier *: CN

Domain Name *: dithersnetwork.net

Username *: ad_admin

Password *: ●●●●●●●●

* This field is required

LDAP Table

- 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

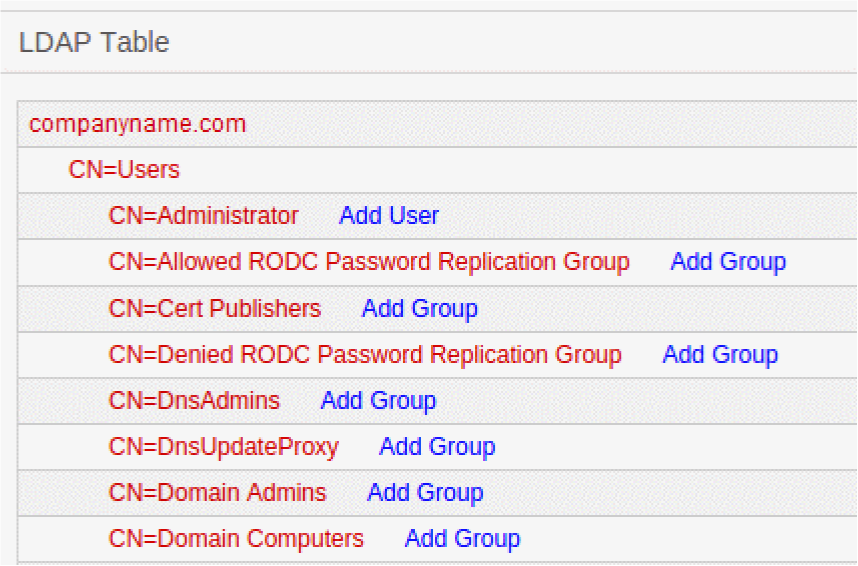
- LDAP Server IP - Enter the IP address of the AD server. The IP address is generally same with the agent's address.

- 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.

Clicking the Domain name expands the tree structure of the active directory.



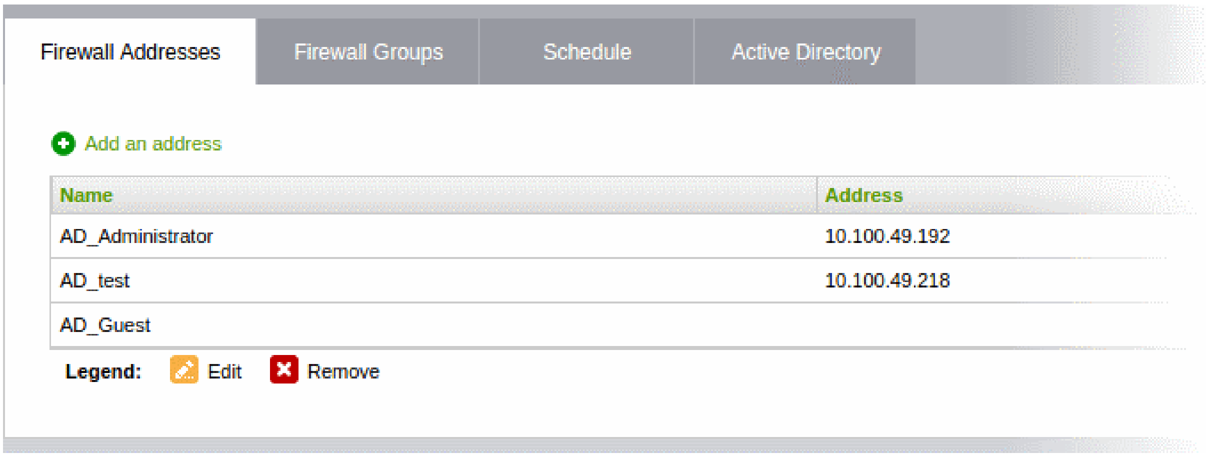
LDAP Table

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.

Adding 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.



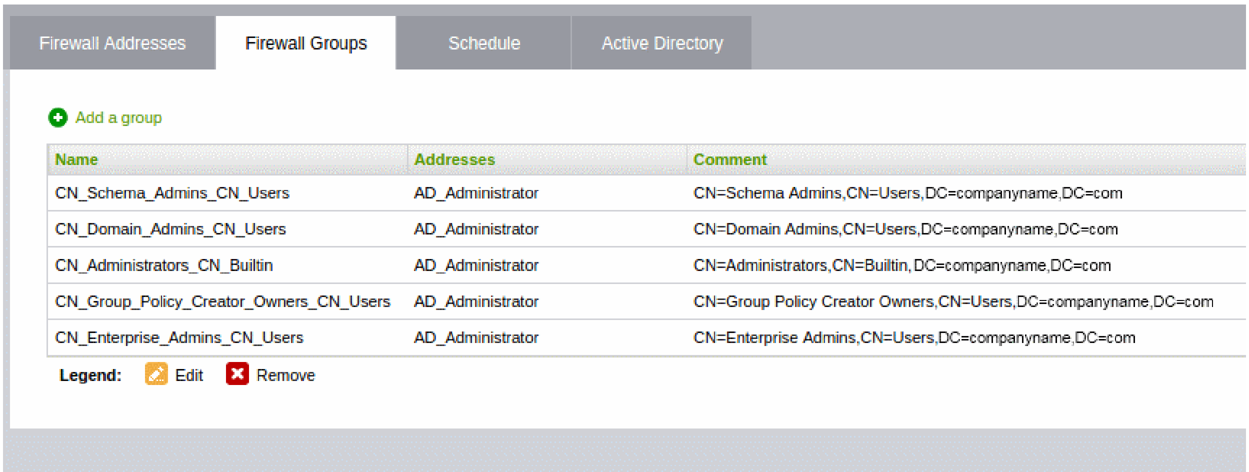
Name	Address
AD_Administrator	10.100.49.192
AD_test	10.100.49.218
AD_Guest	

Legend: Edit Remove

Adding 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

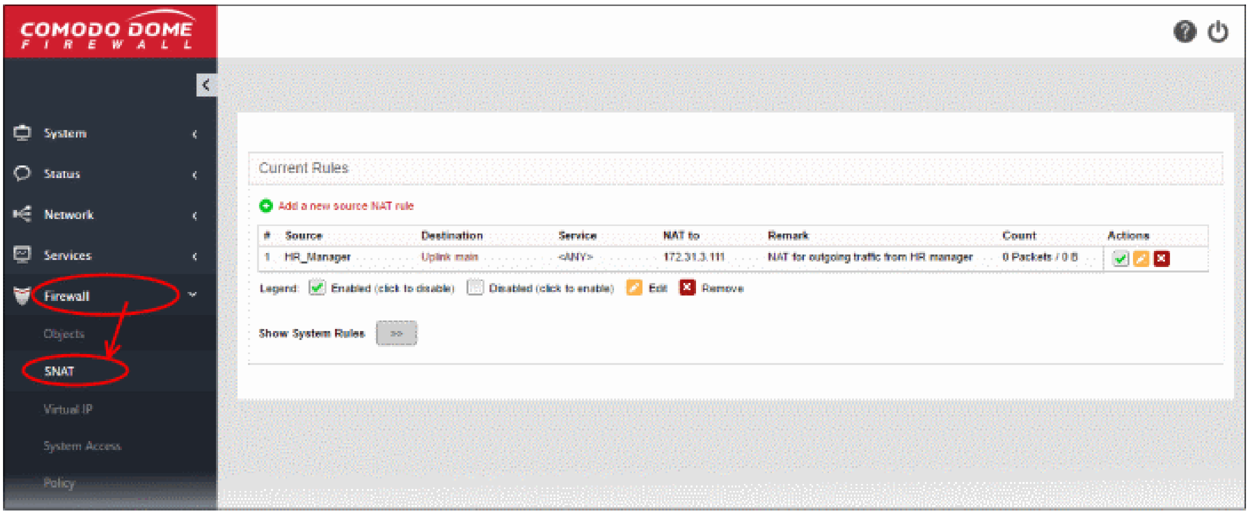
8.2 Source Network Address Translation

- By default, Dome Cloud 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 Cloud 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



#	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	✓ ✎ ☒

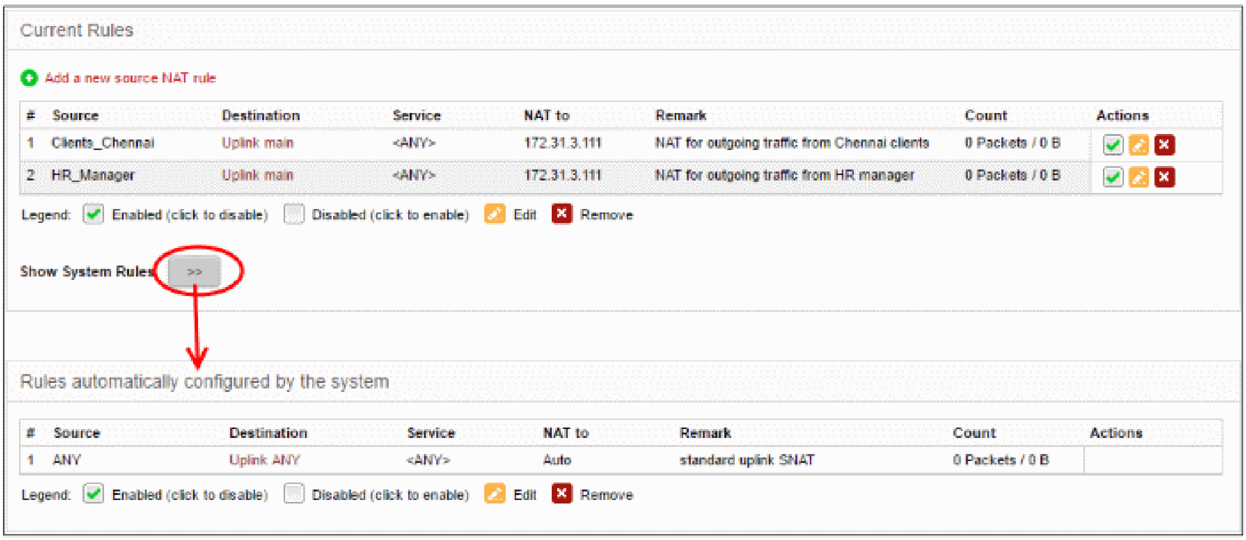
Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) Edit ☒ Remove

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 (proxy) device to which traffic is sent before being sent to the external network.
Service	The service that uses the traffic, indicated as the protocol and the port used
NAT to	The stated IP of the host. This address will be featured in the headers of 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.

- Click the button next to 'Show system rules' to view a list of SNAT rules auto generated by DCF. 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	

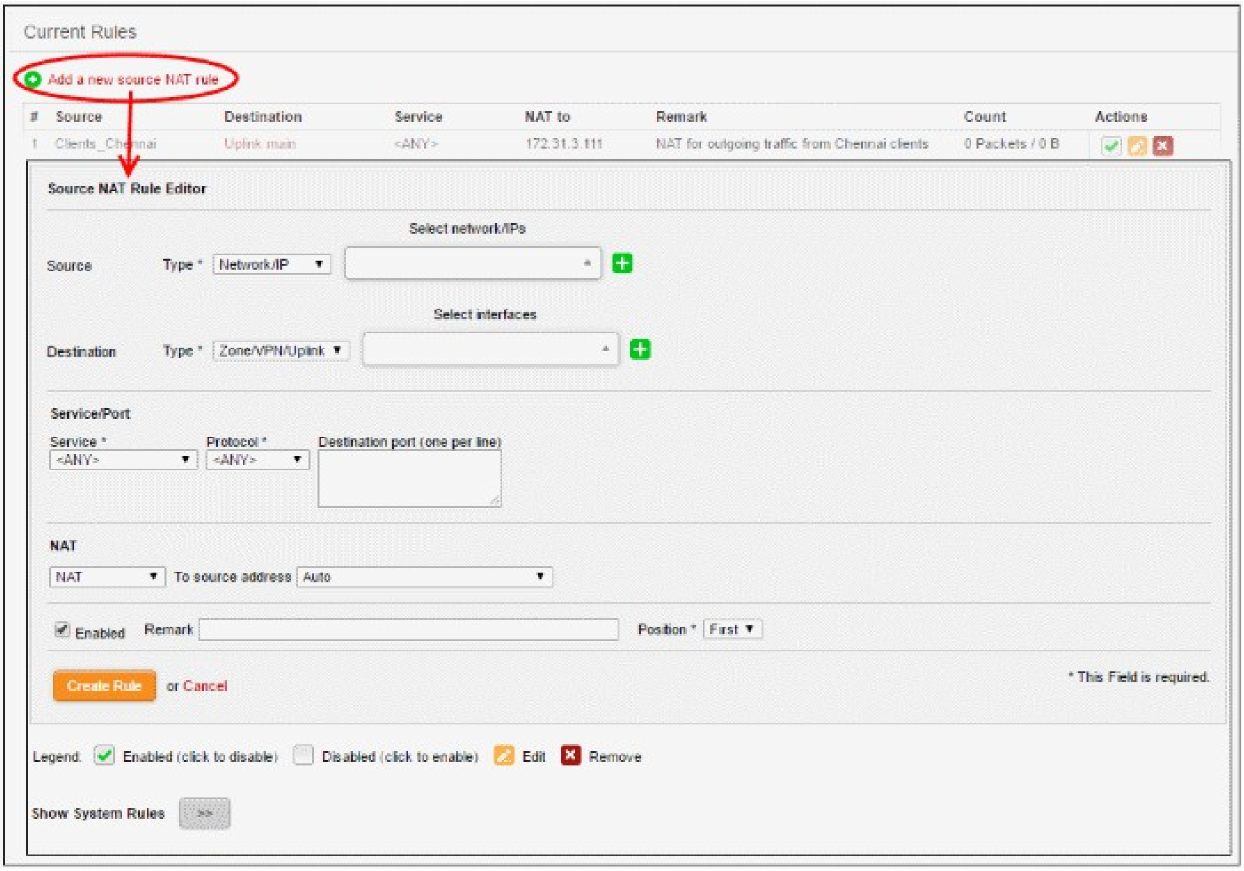
Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

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:

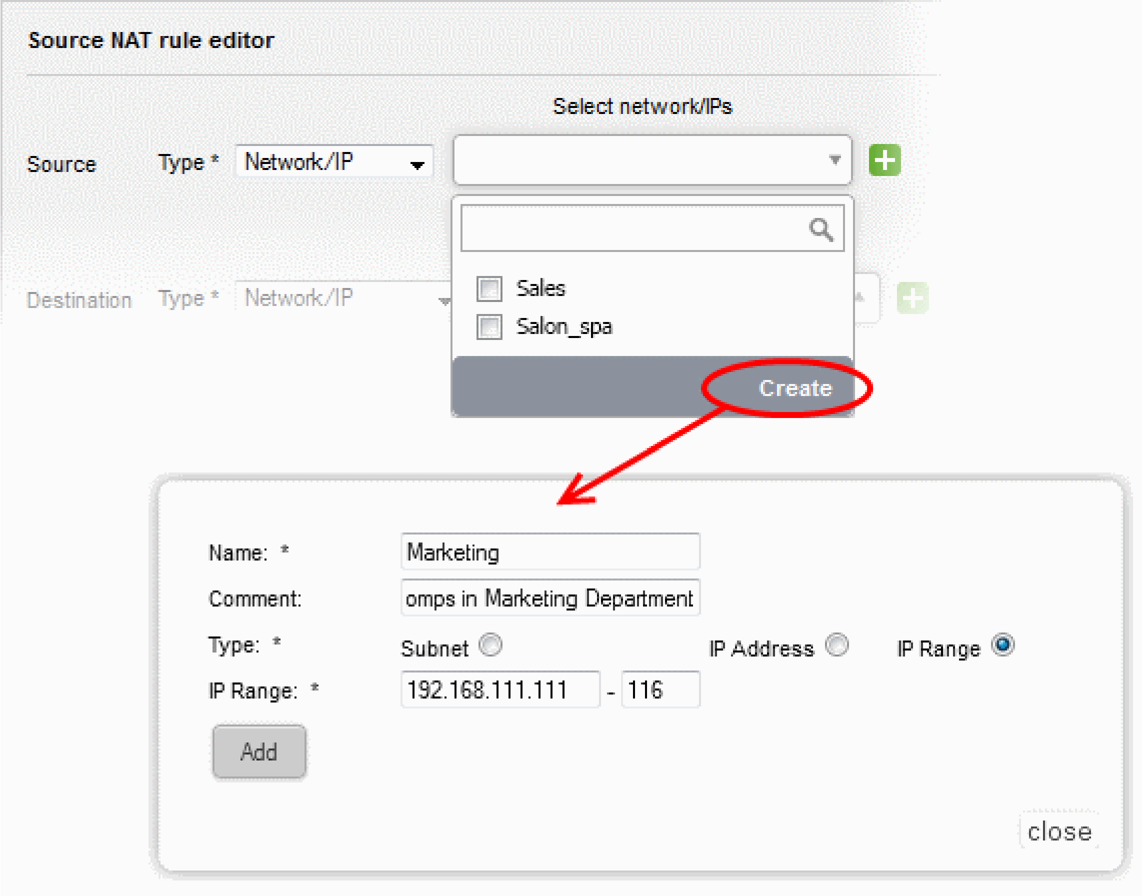
Source - Specify whether the origin of the traffic to be intercepted by this rule is a network address or an SSL VPN user.

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.



Name: * Marketing

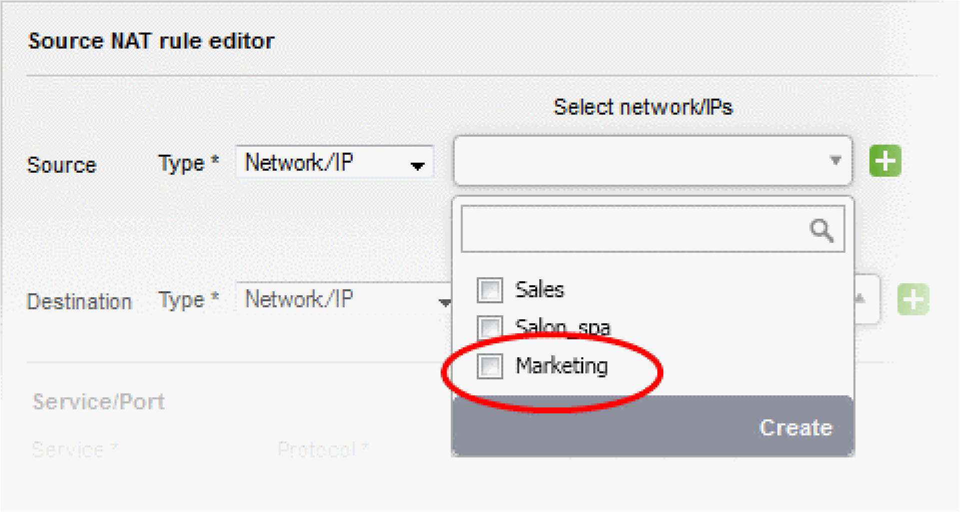
Comment: omps in Marketing Department

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: DCF 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. Refer to the section **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.

SNAT rule management activities are logged – including date, time, type of event, subject id, component name and event outcome.

8.3 Configuring Virtual IP for Destination Network Address Translation

DCF 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, it can be made accessible at the IP address/port combination of an uplink device connected to the appliance.

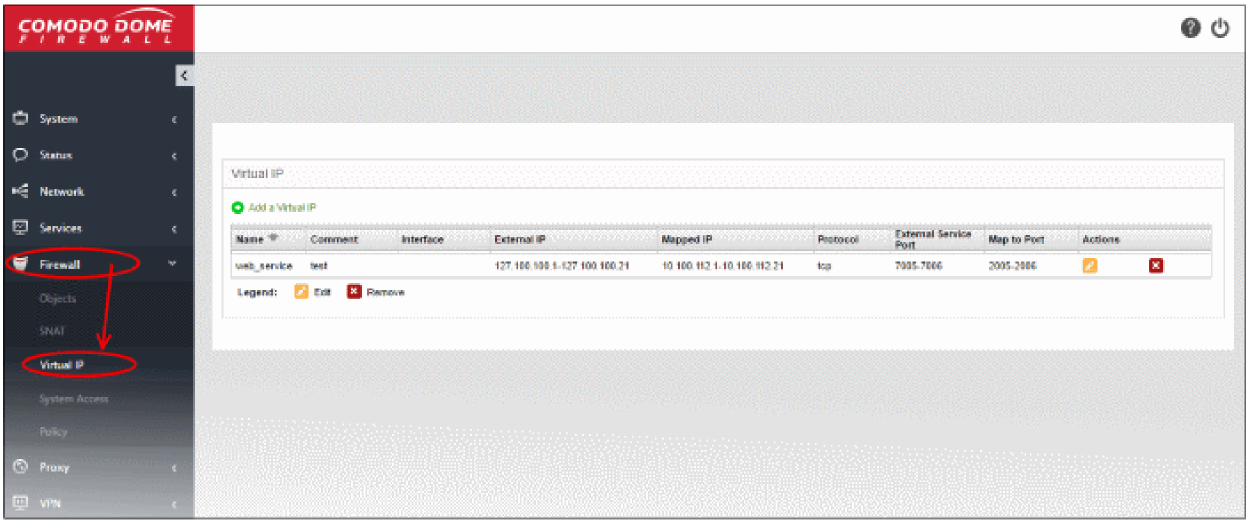
2. DCF blocks SSH connection requests from untrusted external IP addresses to any host within the DMZ zone by default. If required, rules can be created to allow SSH access to a specific host in the DMZ.

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 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 to which traffic is sent.
Mapped IP	The IP address/IP range of the destination host/device to which traffic is redirected.
Protocol	The protocol used by the service.
External Service Port	The port or port range on the host(s)/device(s) to which the traffic is directed.
Map to Port	The port or port range on the destination host to which traffic is 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. See **Creating a Virtual IP rule** for more details. ☒ - Removes the rule.

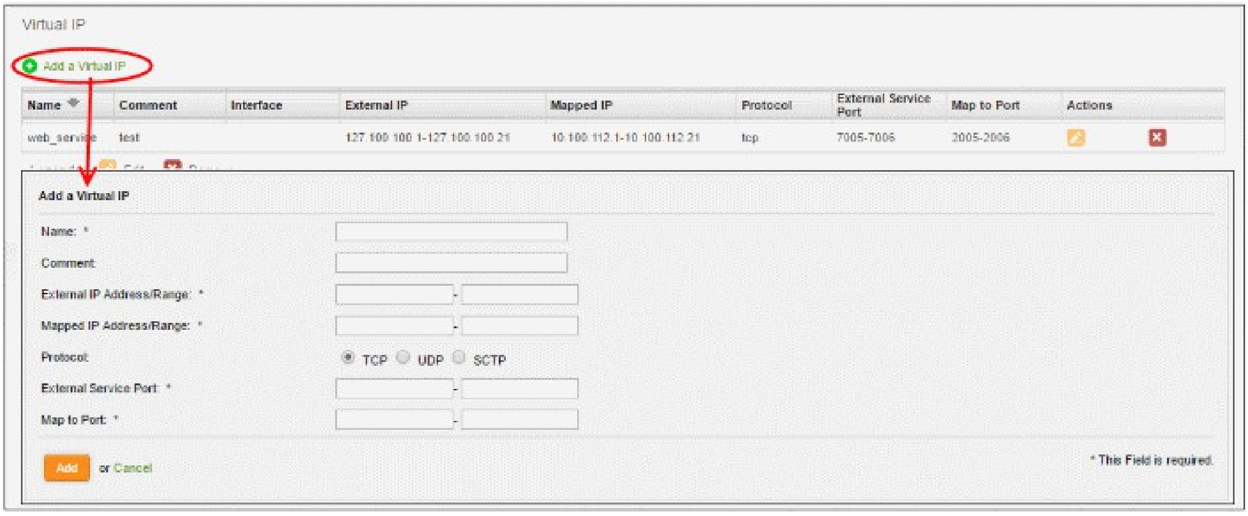
Creating a Virtual IP rule

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.



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	

Add a Virtual IP

Name: *	
Comment:	
External IP Address/Range: *	-
Mapped IP Address/Range: *	-
Protocol:	● TCP ○ UDP ○ SCTP
External Service Port: *	-
Map to Port: *	-

* This Field is required.

- 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.

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 Configuring System Access

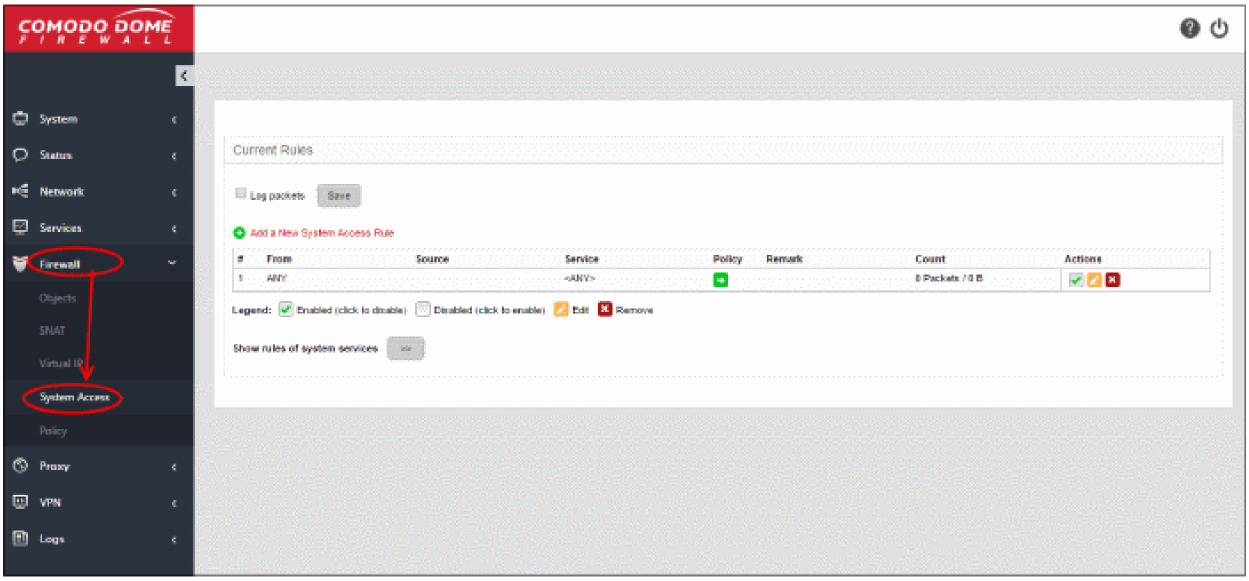
The system access firewall rules manage the access to DCF from the hosts in various internal network zones and external networks.

DCF is pre-configured with firewall rules that allow the hosts in different network zones to access it 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 DCF. Whenever a new service is enabled in the appliance, rules are auto-created to provide the service to hosts in the required network zones. The administrator can view the rules but cannot 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 DCF 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	☑ ✎ ☒

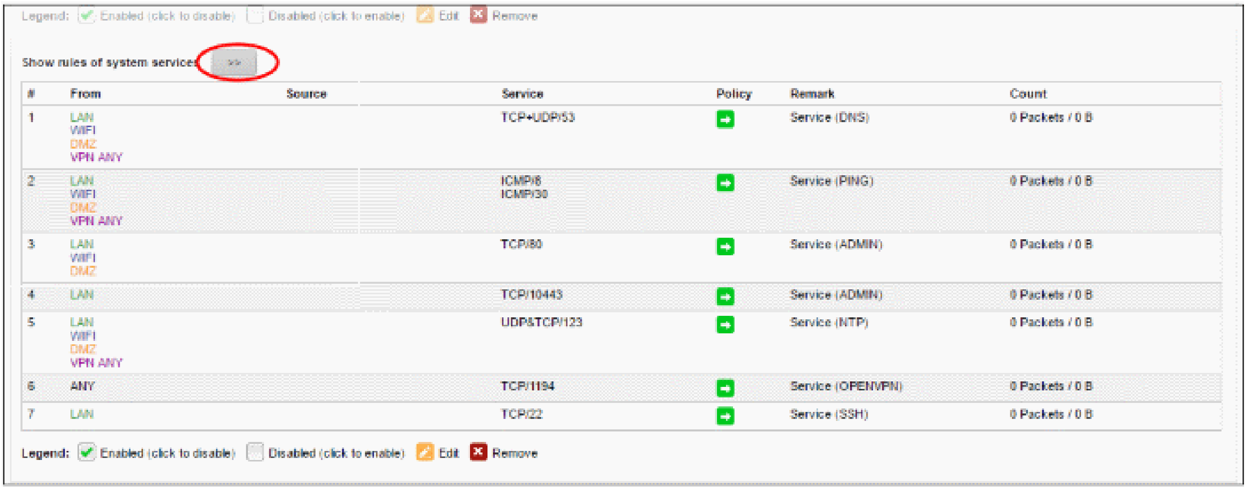
Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

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 DCF 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. See '**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.



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 VPN ANY		UDP&TCP/123	➡	Service (NTP)	0 Packets / 0 B
6	ANY		TCP/1194	➡	Service (OPENVPN)	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:

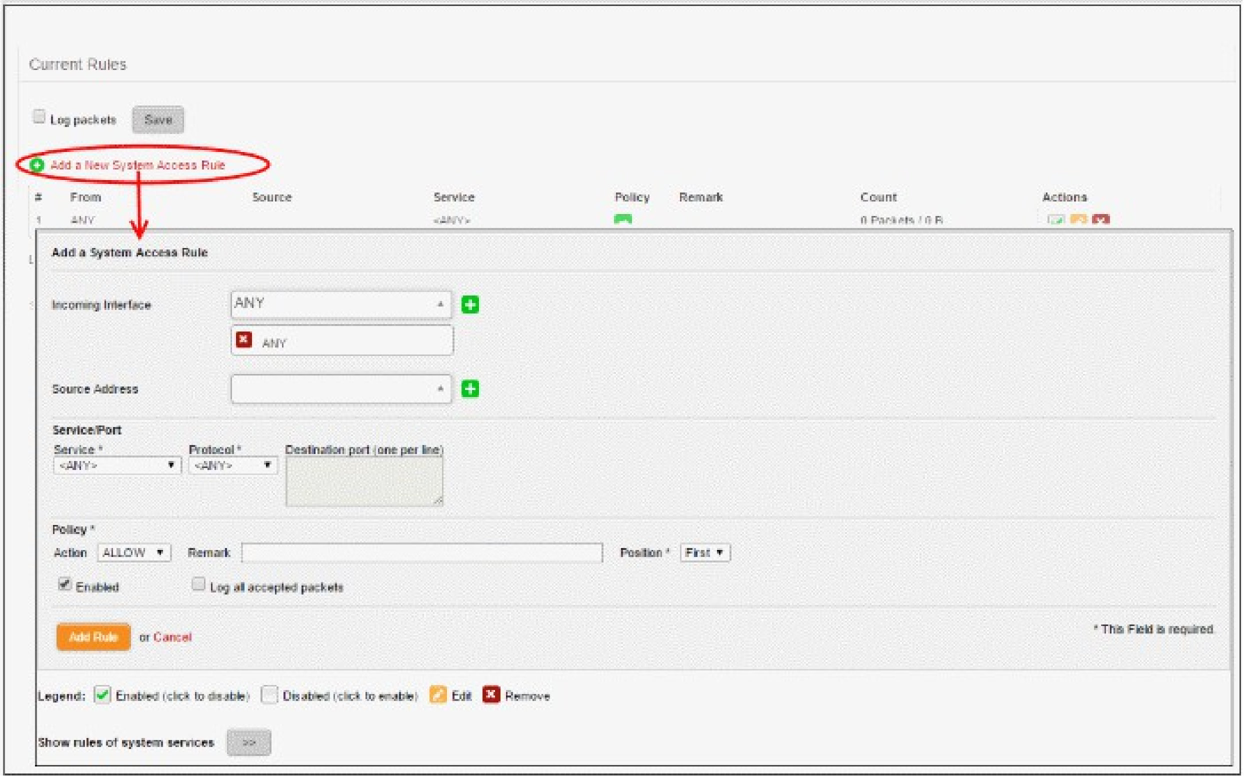
- **Create new system access firewall rules**

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 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.



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	

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

Show rules of system services >>

- Enter the parameters for the new rule as shown below:

Incoming Interface - Select the interface device(s) or 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.

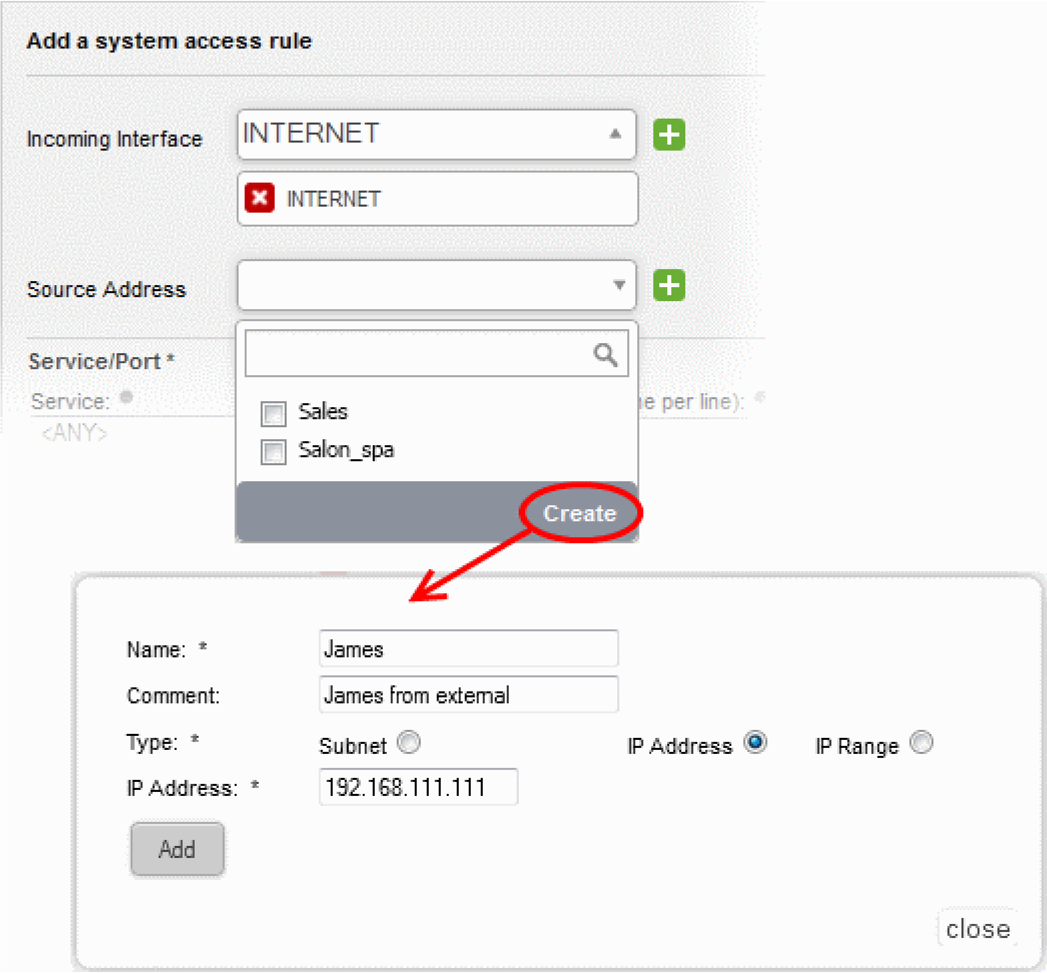
- Choose the Firewall Object(s) or Object Group(s) containing the IP address, IP Address Range or the subnet of the host(s) from the drop-down.

  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.



Add a system access rule

Incoming Interface: INTERNET

Source Address:

Name: * James

Comment: James from external

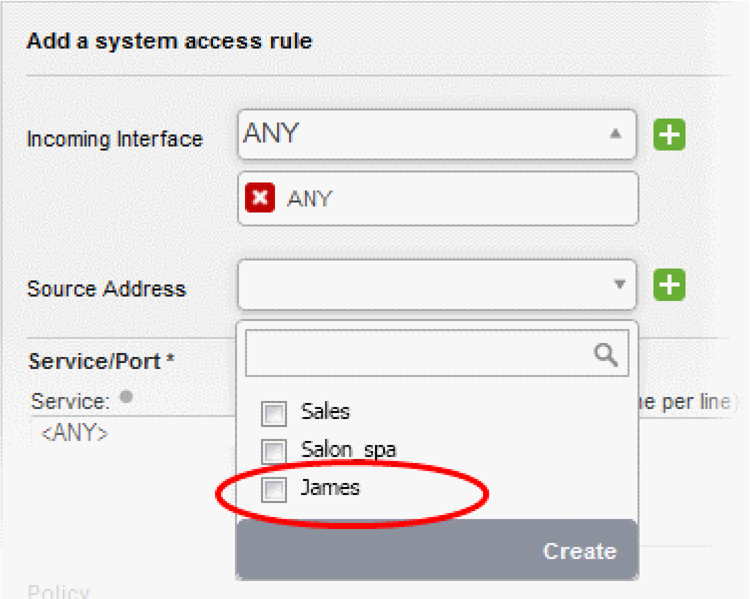
Type: * Subnet ○ IP Address ● IP Range ○

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: DCF 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
- Drop - 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. Refer to the section **Viewing Logs** for more details on configuring storage of logs and viewing the logs.
- Click 'Add Rule'.

The new rule will be added and displayed in the screen.

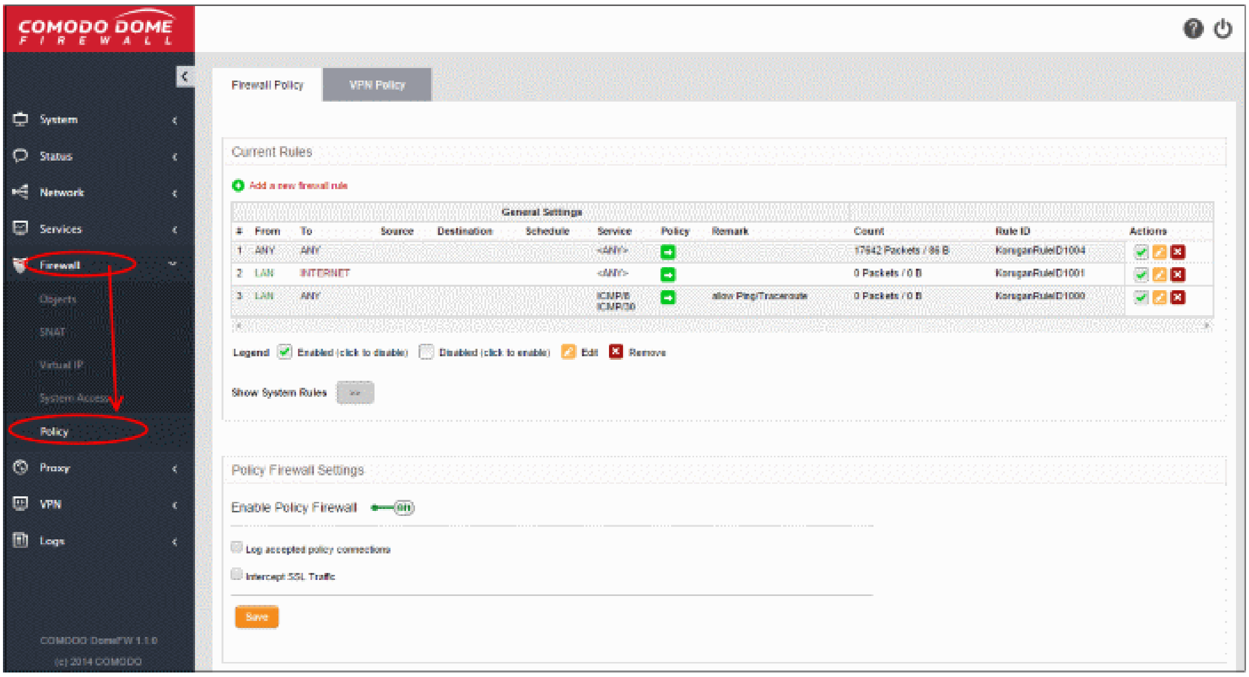
8.5 Configuring Firewall Policy Rules

DCF applies a firewall 'Policy' to manage the data traffic flowing in and out of and within your network. The policy is constructed from a series of firewall rules that are created and imposed for different types of data traffic. The rules can also be individually scheduled to be active only on specified time periods.

- Incoming traffic - Traffic from external network zones to specified 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 DCF
- VPN traffic - Traffic generated by VPN users

The Firewall Rules interface allows the administrator to enable/disable the policy firewall and to create and manage the firewall rules with granular configuration.

To open the 'Firewall Rules' interface, click 'Firewall' > 'Policy' from the left hand side navigation.



Current Rules

Add a new firewall rule

General Settings											
#	From	To	Source	Destination	Schedule	Service	Policy	Remark	Count	Rule ID	Actions
1	ANY	ANY				<ANY>	➡		17642 Packets / 86 B	KoruganRuleID1004	✓ ✎ ☒
2	LAN	INTERNET				<ANY>	➡		0 Packets / 0 B	KoruganRuleID1001	✓ ✎ ☒
3	LAN	ANY				ICMP/8 ICMP/30	➡	allow Ping/Traceroute	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

□ Intercept SSL Traffic

Save

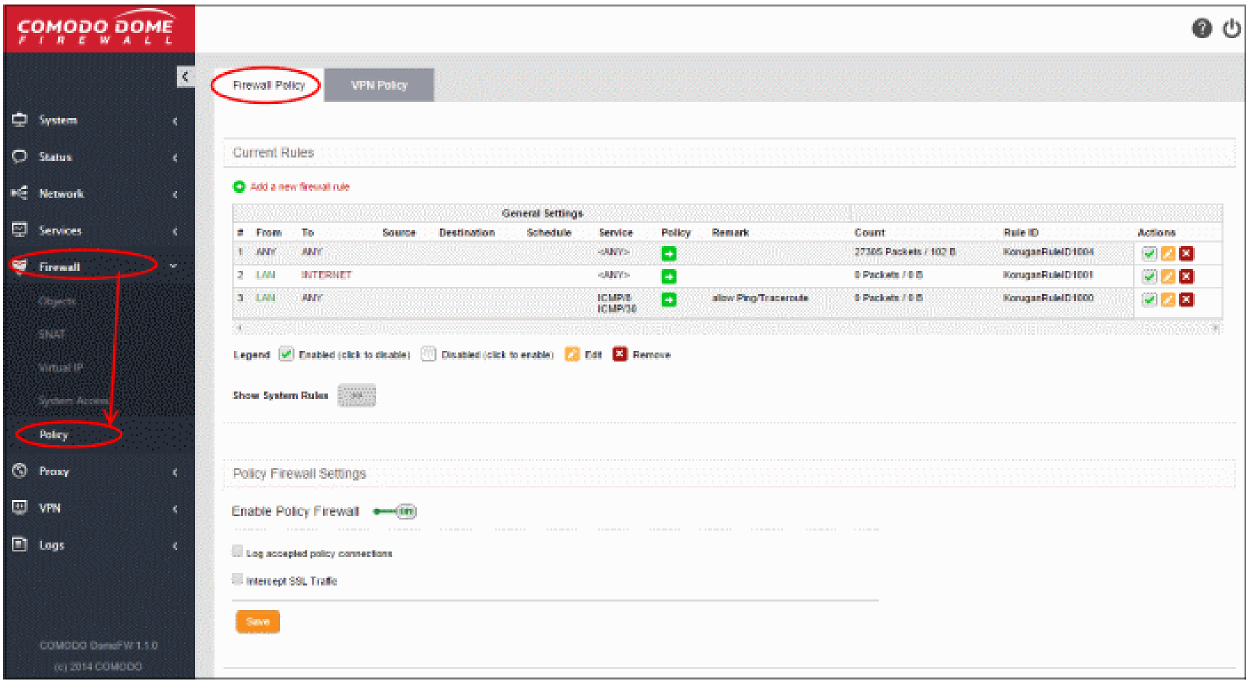
The interface contains two tabs:

- **Firewall Policy** - Allows the administrator to create and manage firewall policy rules for incoming, outgoing and inter-zone traffic. See '**Managing Firewall Policy Rules**' for more details.
- **VPN Policy** - Allows the administrator to create and manage firewall rules for regulating traffic from/to VPN users.. See '**Managing VPN Firewall Rules**' for more details.

8.5.1 Managing Firewall Policy Rules

The Firewall Policy interface allows the administrator to enable/disable the firewall policy and to create and manage the firewall rules for outgoing, incoming and inter-zone traffic.

To open the 'Firewall Policy' interface, click 'Firewall' > 'Policy' from the left hand side navigation and select the 'Firewall Policy' tab.



General Settings											
#	From	To	Source	Destination	Schedule	Service	Policy	Remark	Count	Rule ID	Actions
1	ANY	ANY				<ANY>	➡		27305 Packets / 102 B	KoruganRuleID1004	✓ ✎ ☒
2	LAN	INTERNET				<ANY>	➡		0 Packets / 0 B	KoruganRuleID1001	✓ ✎ ☒
3	LAN	ANY				ICMP/8 ICMP/30	➡	allow Ping/Traceroute	0 Packets / 0 B	KoruganRuleID1000	✓ ✎ ☒

□ Log accepted policy connections

□ Intercept SSL Traffic

The interface displays two panes:

- **Current Rules** - The upper 'Current Rules' pane displays a list of rules in action and allows the administrator to add new rules and edit existing 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 '**Configuring the Policy Firewall Settings**' for more details.

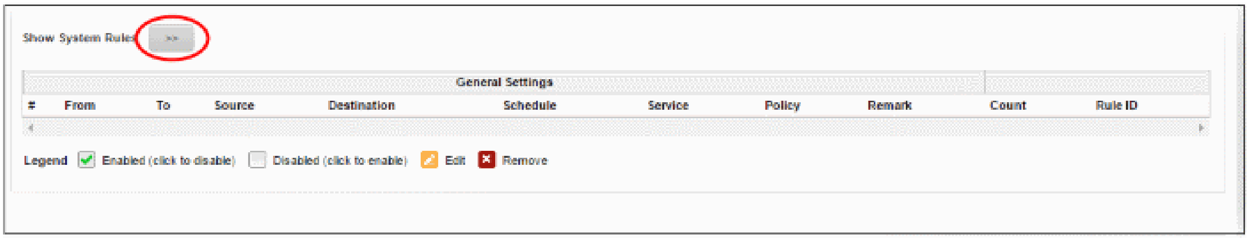
Managing Firewall Rules

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 device or the network zone from which the traffic originates.
	To	The interface device or the network zone to which the traffic is directed.
	Source	The Firewall Object or Object Group containing the IP address, IP Address Range or the subnet of the host(s) from which the traffic originates.

	Destination	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.
	Schedule	The schedule object that covers the time period for which the rule is active.
	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.
	Rule ID	Identity number of the rule as per the order of creation in DCF. The traffic is allowed or denied based on the first matching rule in the ascending order of the ID numbers, regardless of order of the rules as displayed in the table.
	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 'Policy Firewall Rule Editor' interface from which the new rules are created. See '**Creating Policy Firewall rules'** for more details. ☒ - Removes the rule.

- Clicking the right arrow button beside 'Show system rules' displays a list of firewall rules auto generated by DCF. These rules cannot be modified or removed.

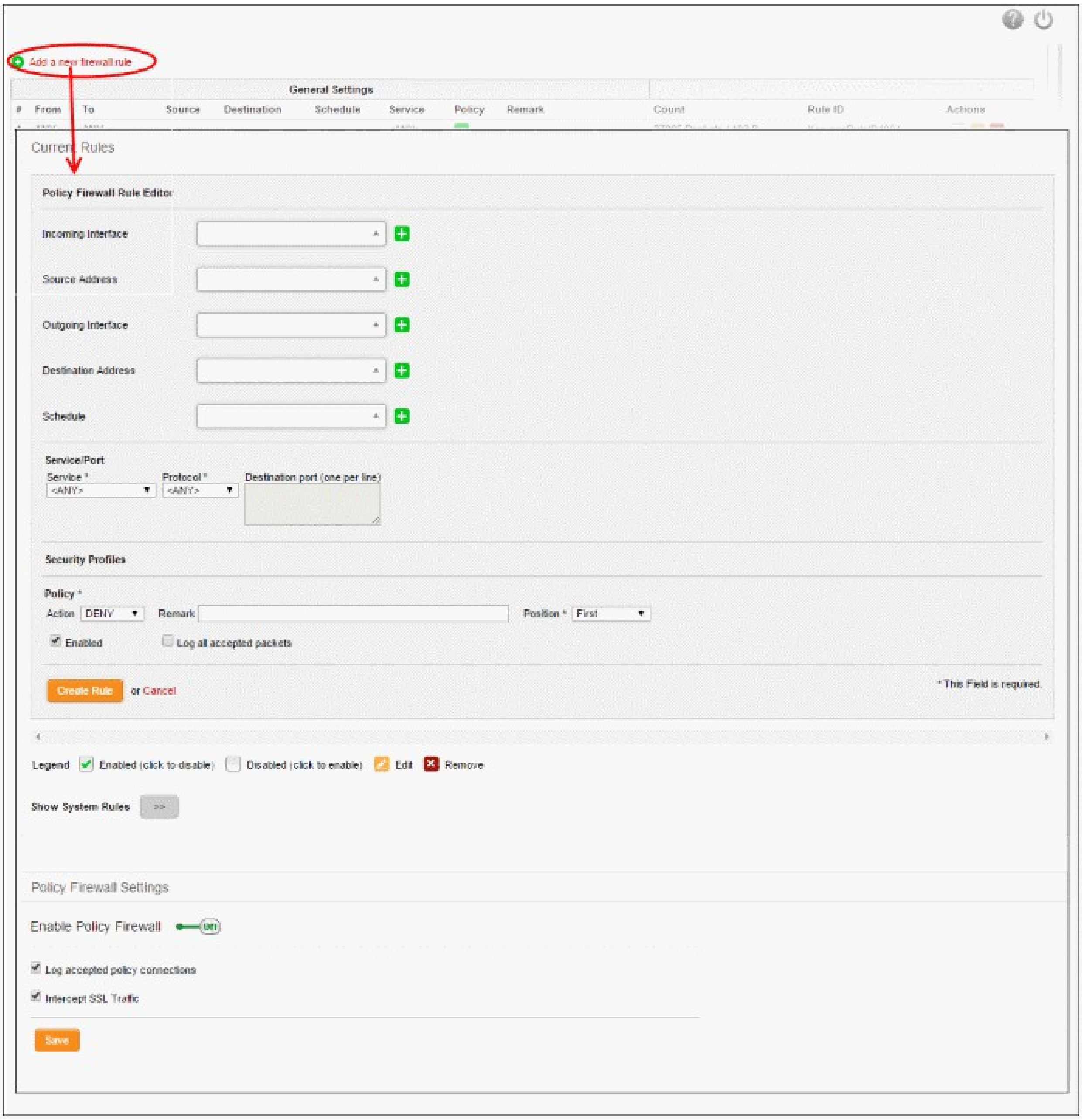

Show System Rules
>>
General Settings
# From To Source Destination Schedule Service Policy Remark Count Rule ID
Legend ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

Creating Policy Firewall rules

A firewall rule for the firewall policy can be created from the 'Policy Firewall Rule Editor' pane by defining the source , destination, the service used by the traffic, selecting security profiles and the action to be taken on the traffic.

To create a new firewall rule

- Open the 'Firewall Policy' interface by clicking 'Firewall' > 'Policy' from the left hand side navigation and selecting 'Firewall Policy' tab.
- Click the 'Add a new firewall rule' link at the top left. The 'Policy Firewall Rule Editor' will open.



Add a new firewall rule

General Settings

#	From	To	Source	Destination	Schedule	Service	Policy	Remark	Count	Rule ID	Actions

Current Rules

Policy Firewall Rule Editor

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service/Port

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

Security Profiles

Policy *

Action DENY ▾ Remark Position * First ▾

☑ Enabled □ Log all accepted packets

Create Rule or Cancel

* This Field is required.

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

☑ Intercept SSL Traffic

Save

The 'Policy Firewall Rule Editor' interface is divided into three areas for specifying the different components of the rule:

- **Address Settings and Schedule** - Choose the source and destination of the traffic and set a schedule for the rule to be active.
- **Service/Port** - Specify the service pertaining to the traffic to be intercepted by the rule.
- **Policy Settings** - Configure to allow or block the traffic intercepted by the rule.

Address Settings and Schedule

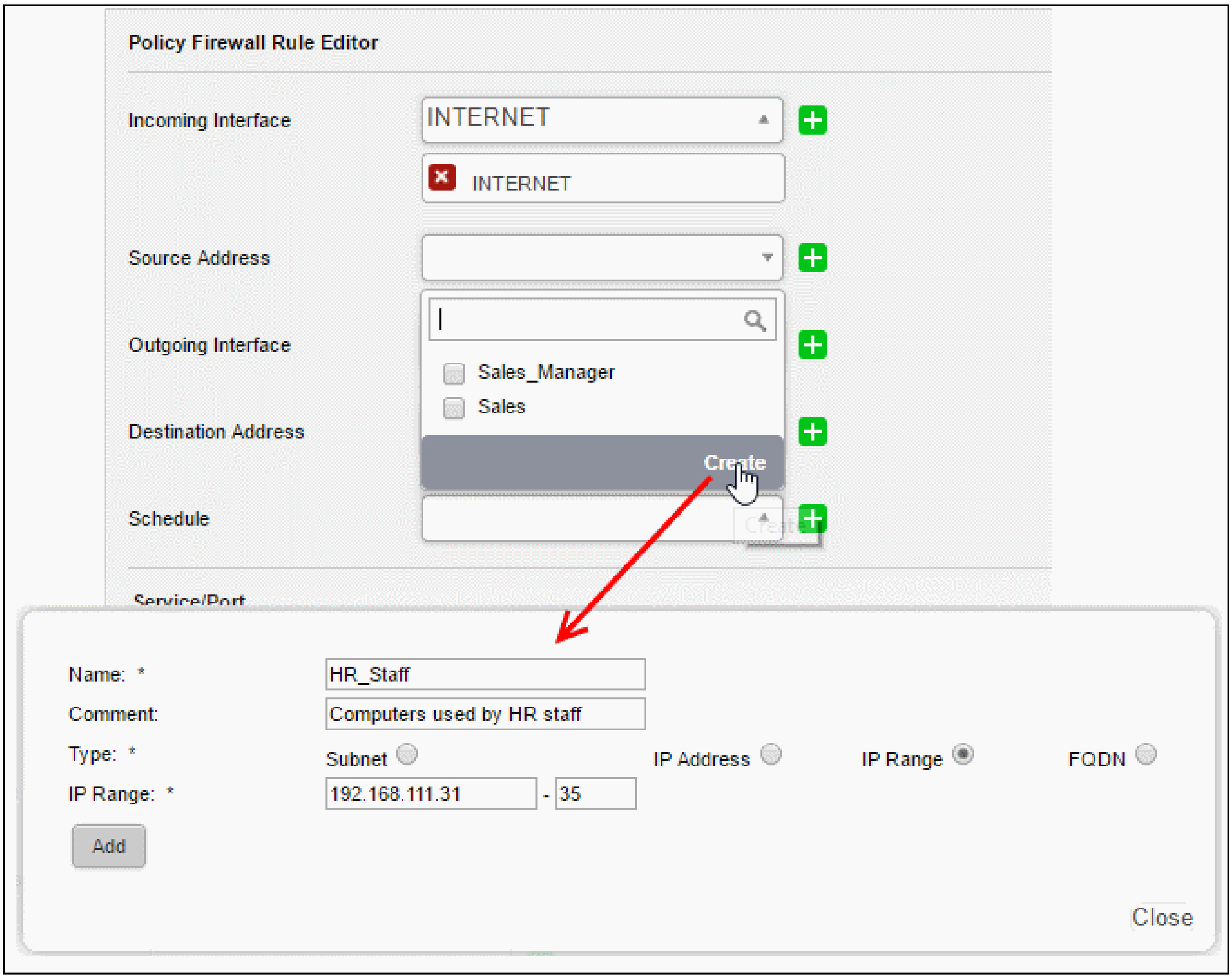
- **Incoming Interface -** Choose the interface device or the physical port at which the traffic is received, from the drop-down.
- **Source Address -** Choose the firewall object or the object group that covers the IP address, IP address

range or the subnet, at 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.



Name: * HR_Staff

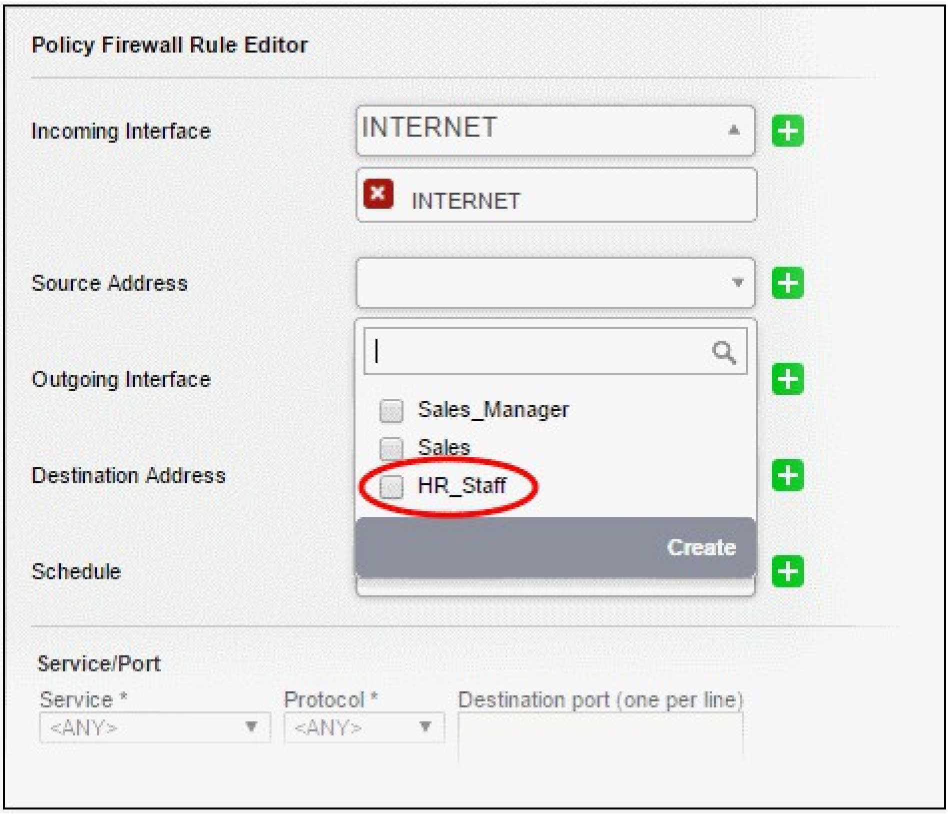
Comment: Computers used by HR staff

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

IP Range: * 192.168.111.31 - 35

- **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 a fully qualified domain name is to be covered by the object and enter the same.
- 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.

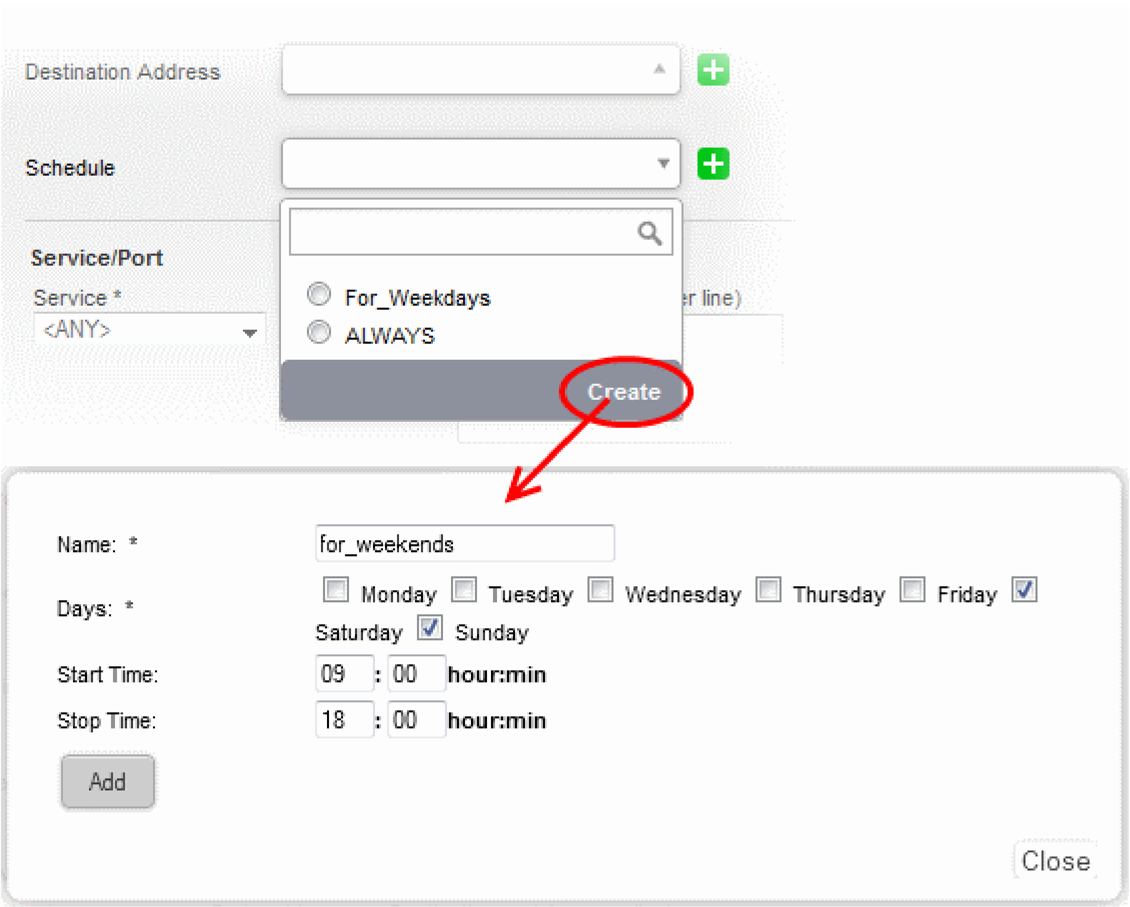
- **Outgoing Interface** - Choose the interface device or the physical port to which the traffic is directed, from the drop-down.
- **Destination Address** - Choose the 'Firewall Object' or 'Object Group' containing the IP address, IP Address Range or the subnet of the host(s) to which the traffic is 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. Refer to the **explanation above** for more details.
- **Schedule** - The Schedule Objects added to the **Firewall Objects > Schedule** interface will be available in the drop-down. Choose the schedule object(s) that cover the time period(s) for which the rule needs to be active from the drop-down.

  If the schedule object covering the required time period P to be specified has not been created under the Firewall Objects > Schedule previously and hence not available in the drop-down, you can create a new object from this interface too.

  To create a new schedule 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: * for_weekends

Days: * □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday ☑ Saturday ☑ Sunday

Start Time: 09 : 00 hour:min

Stop Time: 18 : 00 hour:min

- **Name** - Specify a name for the schedule.
- **Days** - Select the days of the week at which the firewall should be active.
- **Start Time and Stop Time** - Enter a time at which the firewall should be started and stopped at the selected days in 24 Hrs time format.

- Click 'Add' for the new schedule to be created.

The new schedule object will also be available for selection in the drop-down and also will be added to the list of schedule objects under **Firewall Objects > Schedule** interface. The new object will be available for selection for creating other firewall rules too.

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.

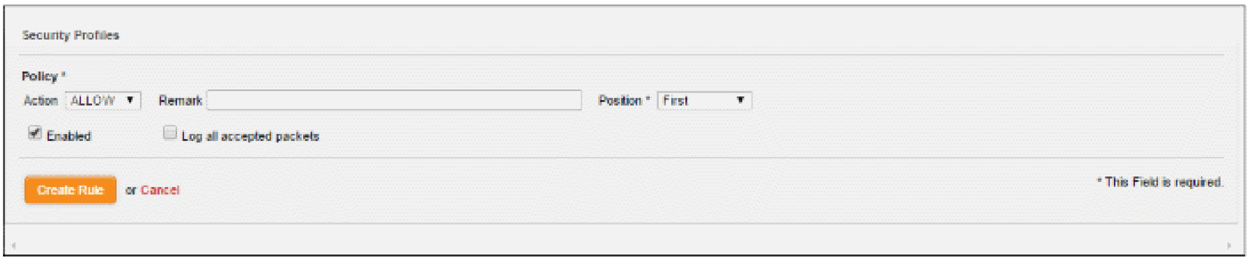
Tip: DCF is configured with predefined combinations of service/protocol/port, like HTTP/TCP/80, <ALL>/TCP+UDP/0:65535, or <ANY>, which is a shortcut for all services, protocols, and ports. If you want to specify custom protocol/port combination, then select 'User Defined' from the service. You can also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

Policy 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. Refer to the section **Viewing Logs** for more details on viewing the logs.



Security Profiles

Policy *

Action: ALLOW ▾ Remark: Position *: First ▾

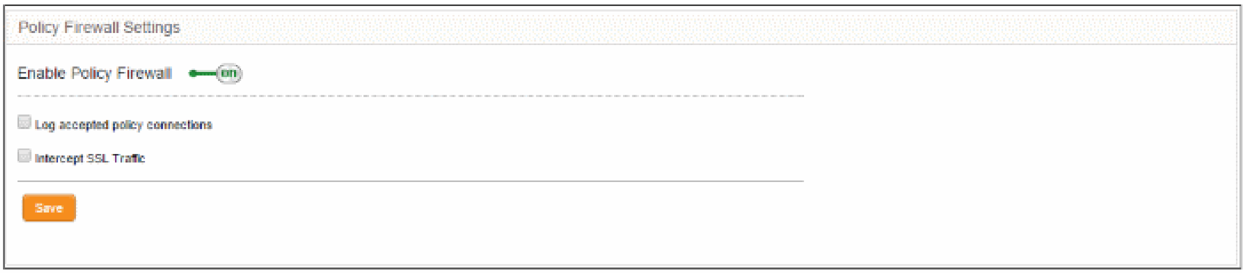
☑ Enabled □ Log all accepted packets

* This Field is required.

- Click 'Create Rule'. A confirmation dialog will appear.

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 and analysis of HTTPS sites.



Policy Firewall Settings

Enable Policy Firewall: on

□ Log accepted policy connections

□ Intercept SSL Traffic

- Use the 'Enable policy firewall' toggle switch to switch the state of the VPN firewall.
- Select the 'Log accepted policy connections' check box to log the packets that has passed the Firewall Policy. See section '**Viewing Logs**' for more details on viewing the logs.
- Select the 'Intercept SSL Traffic' check box in order for analysis of HTTPS sites. Please note the SSL certificate of DCF should be installed on endpoints for this feature to work.
- Click 'Save' for your settings to take effect .

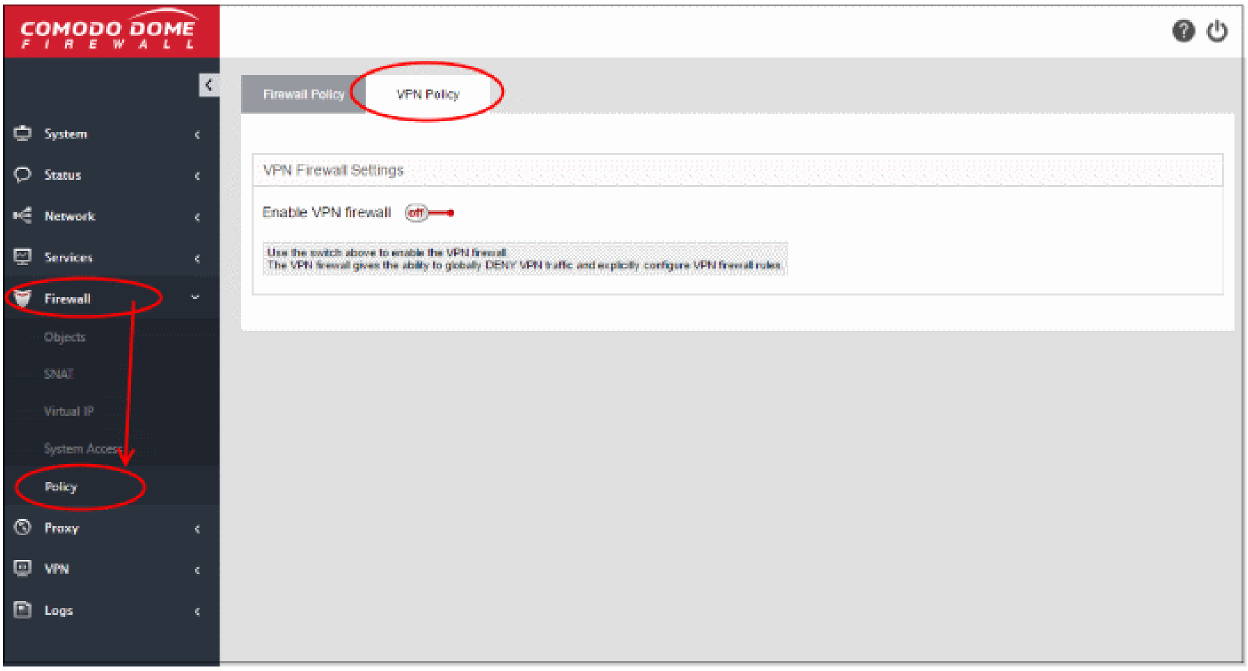
Policy firewall rule activities are logged, including date, time, type of event, subject id, component name and event outcome.

8.5.2 Managing VPN Firewall Rules

VPN firewall rules allow you to set traffic limits for users and hosts who are connected through SSL VPN and IPsec tunnels.

- See **SSL VPN Server** and **SSL VPN Client** if you need help to configure VPN connections and SSL VPN accounts.
- See **IPsec Configuration** if you need help to configure secure IPsec tunnel connections between external networks/sites and internal networks,

- The VPN firewall is disabled by default, allowing both incoming and outgoing traffic between hosts without filtering. Traffic from hosts is not subject to filtering by the outgoing traffic firewall or the Inter-Zone traffic firewall rules.
- The VPN firewall can be enabled in the 'VPN policy' interface. You can also create and manage VPN traffic rules from this interface.
- Click 'Firewall' > 'Policy' > 'VPN Policy' to open the settings interface:



VPN Firewall Settings

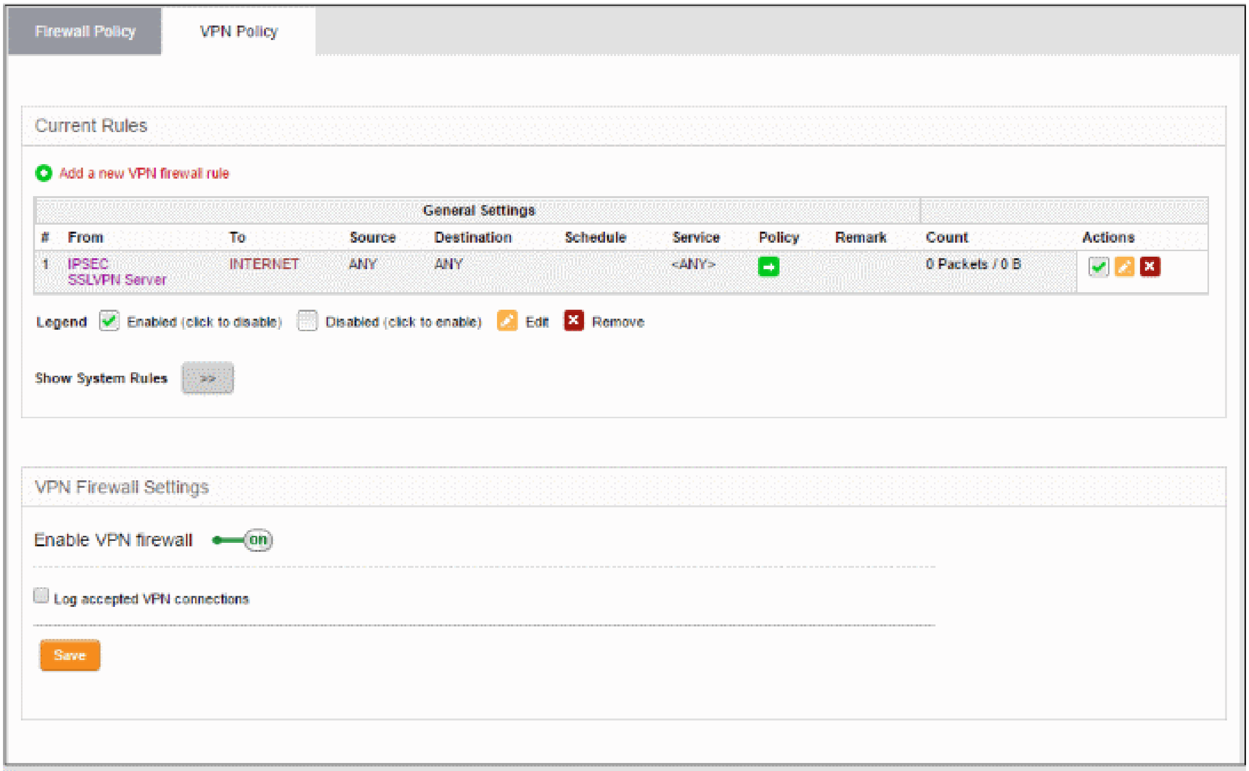
Enable VPN firewall off

Use the switch above to enable the VPN firewall
The VPN firewall gives the ability to globally DENY VPN traffic and explicitly configure VPN firewall rules

By default, the VPN firewall is disabled.

- Use the 'Enable VPN firewall' switch to turn the firewall on or off.

Enabling the rule will reveal the VPN firewall rules interface:



Current Rules

Add a new VPN firewall rule

General Settings										
#	From	To	Source	Destination	Schedule	Service	Policy	Remark	Count	Actions
1	IPSEC SSLVPN Server	INTERNET	ANY	ANY		<ANY>	➡		0 Packets / 0 B	☑ ✎ ☒

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

Show System Rules >>

VPN Firewall Settings

Enable VPN firewall on

□ Log accepted VPN connections

Save

- **Current Rules** - Displays a list of existing rules and allows you to add/edit rules. See **Managing VPN Traffic Rules** for more details.
- **VPN Firewall Settings** - Displays the current status of the VPN firewall and allows you to change configure the firewall logging. See **Configuring the VPN Firewall Settings** for more details.

Managing VPN Traffic Rules

The 'Current Rules' pane displays a list of existing rules. You can add, edit and manage rules from this interface.

	VPN Firewall Rules Table - Column Descriptions	
Category	**Column**	**Description**
General Settings	#	Serial number of the rule.
	From	The interface device, the VPN tunnel or the network zone from which the traffic originates.
	To	The interface device, the VPN tunnel or the network zone to which the traffic is directed.
	Source	The Firewall Object or Object Group containing the IP address, IP Address Range, the subnet of the host(s) or VPN user(s) from which the traffic originates.
	Destination	The Firewall Object or Object Group containing the IP address, IP Address Range, the subnet of the host(s) or the VPN user(s) to which the traffic is directed.
	Schedule	The schedule object that covers the time period for which the rule is active.
	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.
	Actions	Displays rule controls: ☑ - Enabled or disable the rule ✎ - Edit the rule. The edit interface is similar to the 'Add Rule' interface. See **Creating Firewall rules for VPN Traffic** for more details. ☒ - Removes the rule.

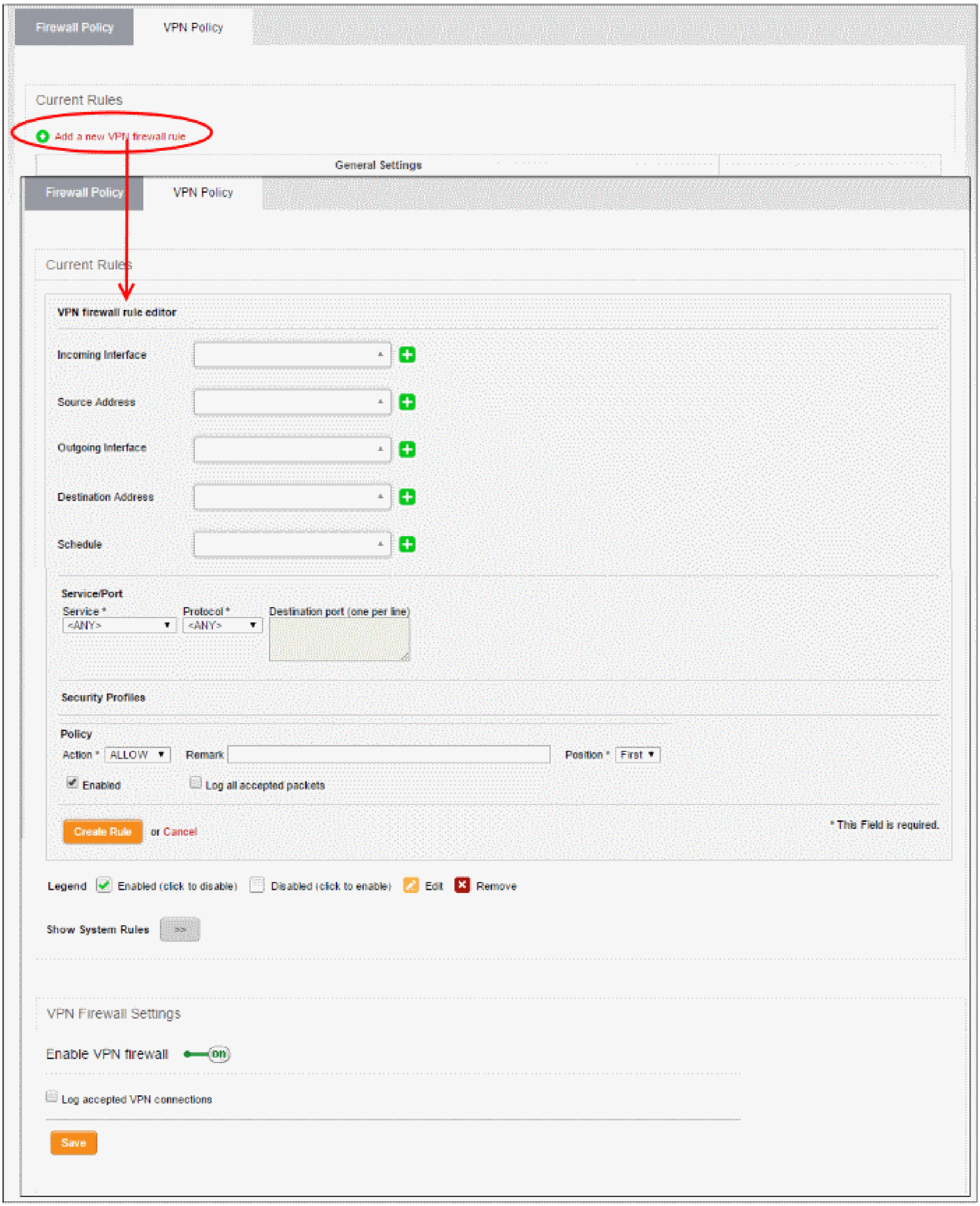
- Clicking the right arrow button beside 'Show system rules' displays a list of firewall rules auto generated by DCF. These rules cannot be modified or removed.

Creating Firewall rules for VPN Traffic

The firewall rules for VPN traffic can be created from the 'VPN firewall rule editor' pane by defining the source, destination, the service used by the traffic, selecting security profiles and the action to be taken on the traffic.

To create a new firewall rule

- Open the 'VPN Policy' interface by clicking 'Firewall' > 'Policy' from the left hand side navigation and selecting the 'VPN Policy' tab.
- Click the 'Add a new VPN firewall rule' link at the top left. The 'VPN firewall rule editor' will open.



VPN firewall rule editor

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service/Port

Service * <ANY>

Protocol * <ANY>

Destination port (one per line)

Security Profiles

Policy

Action * ALLOW Remark Position * First

☑ Enabled □ Log all accepted packets

Create Rule or Cancel

* This Field is required.

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

Show System Rules >>

VPN Firewall Settings

Enable VPN firewall ON

□ Log accepted VPN connections

Save

The 'VPN Firewall Rule Editor' interface is divided into three areas for specifying the different components of the rule:

- **Address Settings and Schedule** - Choose the source and destination of the traffic and set a schedule for the rule to be active.
- **Service/Port** - Specify the service pertaining to the traffic to be intercepted by the rule.
- **Policy Settings** - Configure to allow or block the traffic intercepted by the rule.

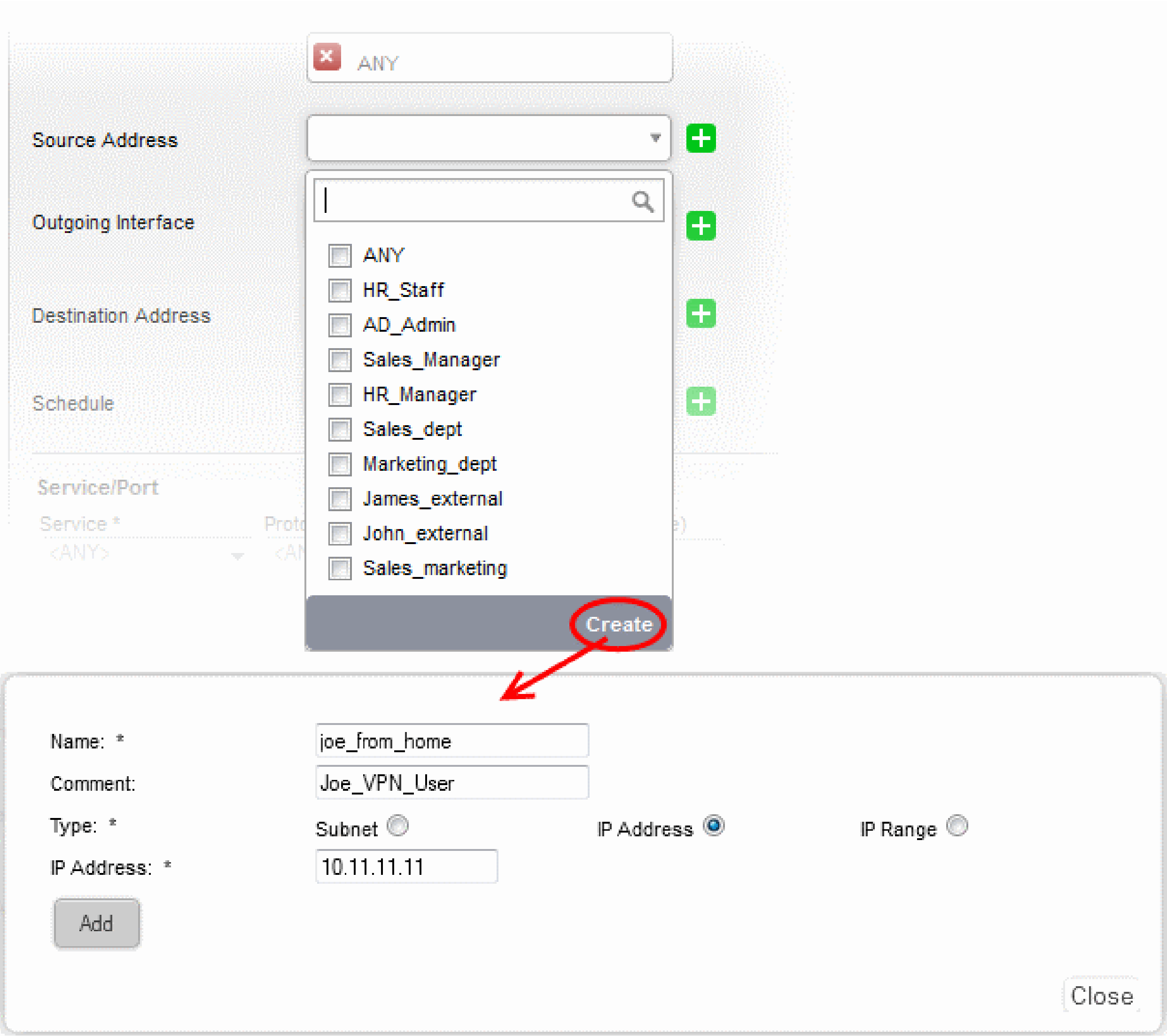
Address Settings and Schedule

- **Incoming Interface** - Choose the interface device, VPN tunnel or the physical port at 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, the subnet or the VPN user(s), at 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 can 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.



Name: * joe_from_home

Comment: Joe_VPN_User

Type: * Subnet ○ IP Address ● IP Range ○

IP Address: * 10.11.11.11

  - **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.

- **Outgoing Interface** - Choose the interface device or the physical port to 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.

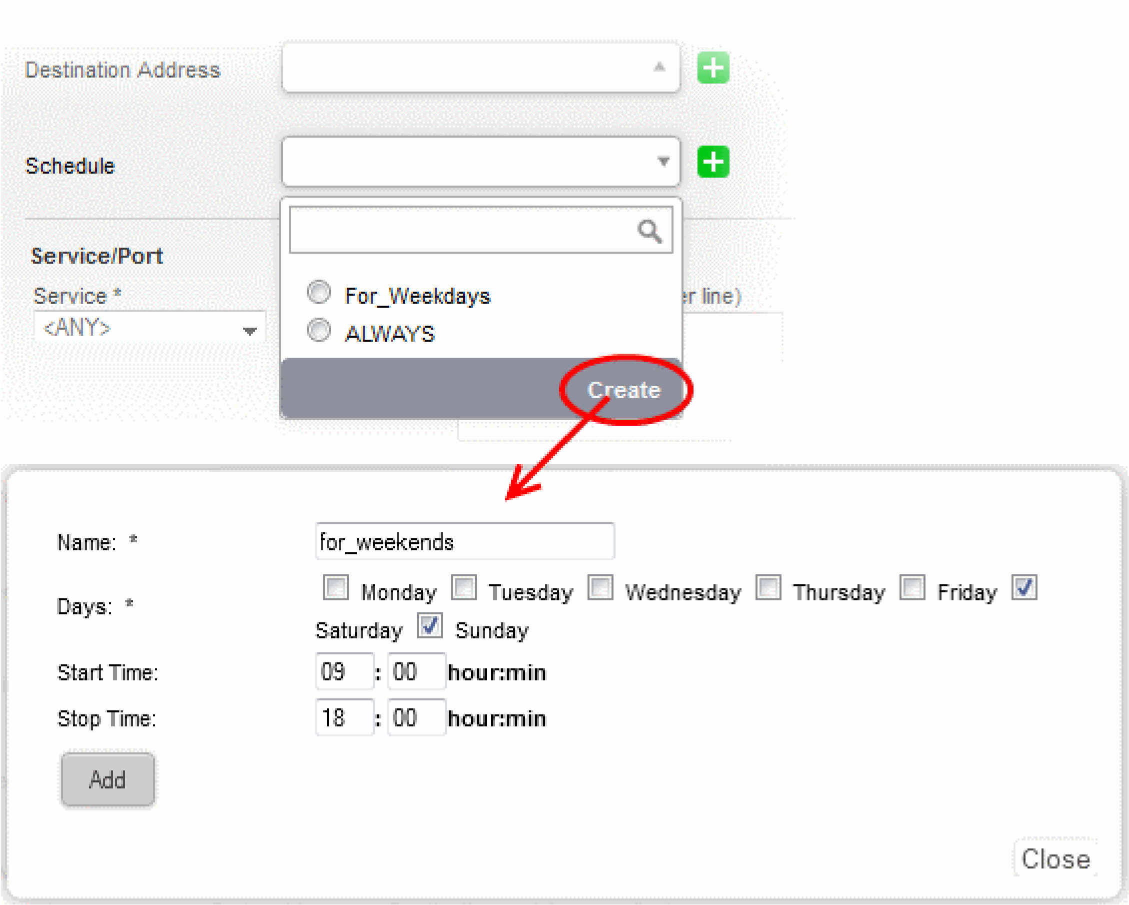
  If a firewall object covering the IP address/IP Address range or the subnet to be specified has not been created under the Firewall Objects interface previously, you an create a new object from this interface too. Refer to the **explanation above** for more details.

- **Schedule** - The Schedule Objects added to the **Firewall Objects > Schedule** interface will be available in the drop-down. Choose the schedule object(s) that cover the time period(s) for which the rule needs to be active from the drop-down.

  If the schedule object covering the required time period P to be specified has not been created under the Firewall Objects > Schedule previously and hence not available in the drop-down, you can create a new object from this interface too.

  To create a new schedule 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.



Destination Address

Schedule

For_Weekdays

ALWAYS

Service/Port

Service * <ANY>

Name: * for_weekends

Days: * □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday ☑ Saturday ☑ Sunday

Start Time: 09 : 00 hour:min

Stop Time: 18 : 00 hour:min

- **Name** - Specify a name for the schedule.
- **Days** - Select the days of the week at which the firewall should be active.
- **Start Time and Stop Time** - Enter a time at which the firewall should be started and stopped at the selected days in 24 Hrs time format.

- Click 'Add' for the new schedule to be created.

The new schedule object will also be available for selection in the drop-down and also will be added to the list of schedule objects under **Firewall Objects > Schedule** interface. The new object will be available for selection for creating other firewall rules too.

Service/Port

Service/Port - Select the type or the service hosted by the source, the protocol and the port used by the service.

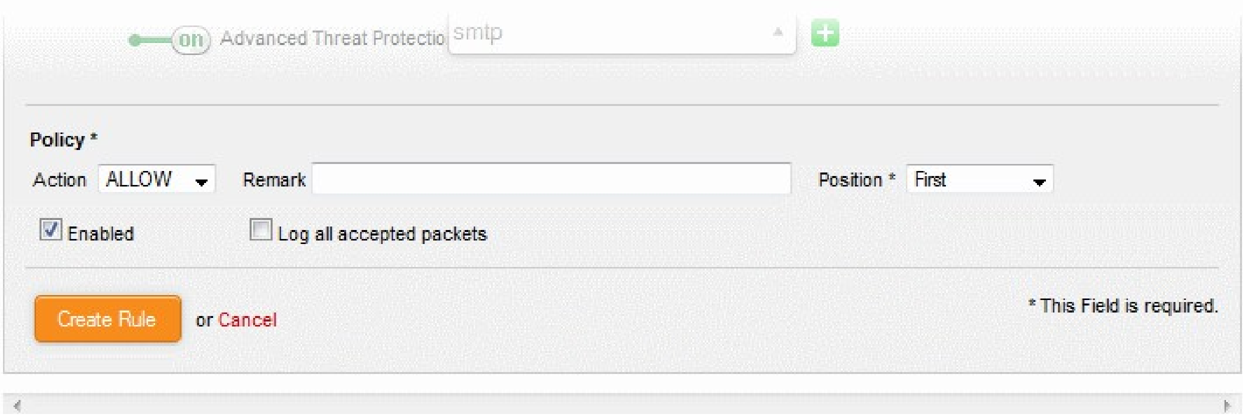
- Service - Choose the type of service from the drop-down
- Protocol - Choose the protocol used by the service
- Destination port - Specify the destination port(s) of the service one by one, in the 'Destination Port' text box.

Tip: DCF has 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 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 section '**Viewing Logs**' for more details on viewing the logs.



on Advanced Threat Protectio smtp

Policy *

Action ALLOW Remark Position * First

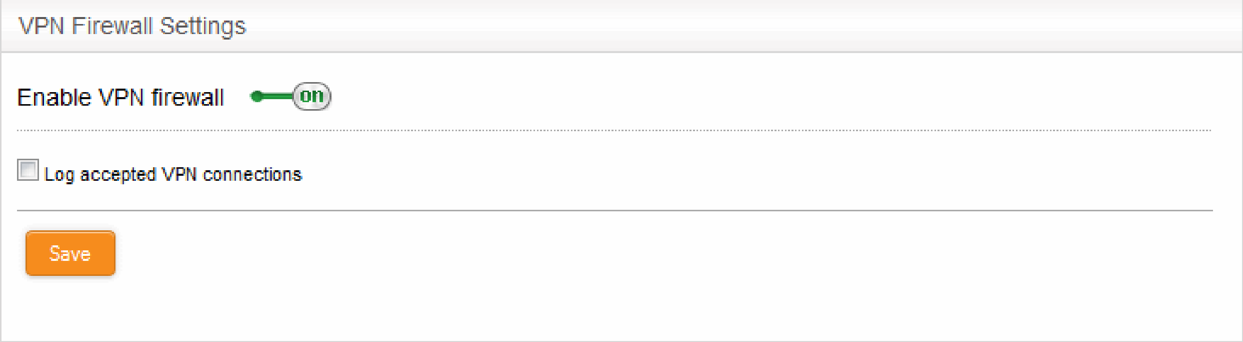
☑ Enabled ☐ Log all accepted packets

* This Field is required.

- Click 'Create Rule'. A confirmation dialog will appear.

Configuring the VPN Firewall Settings

The lower 'VPN Firewall Settings' pane allows the administrator to enable/disable the VPN firewall rule and to opt for logging the packets that pass the rule.



VPN Firewall Settings

Enable VPN firewall on

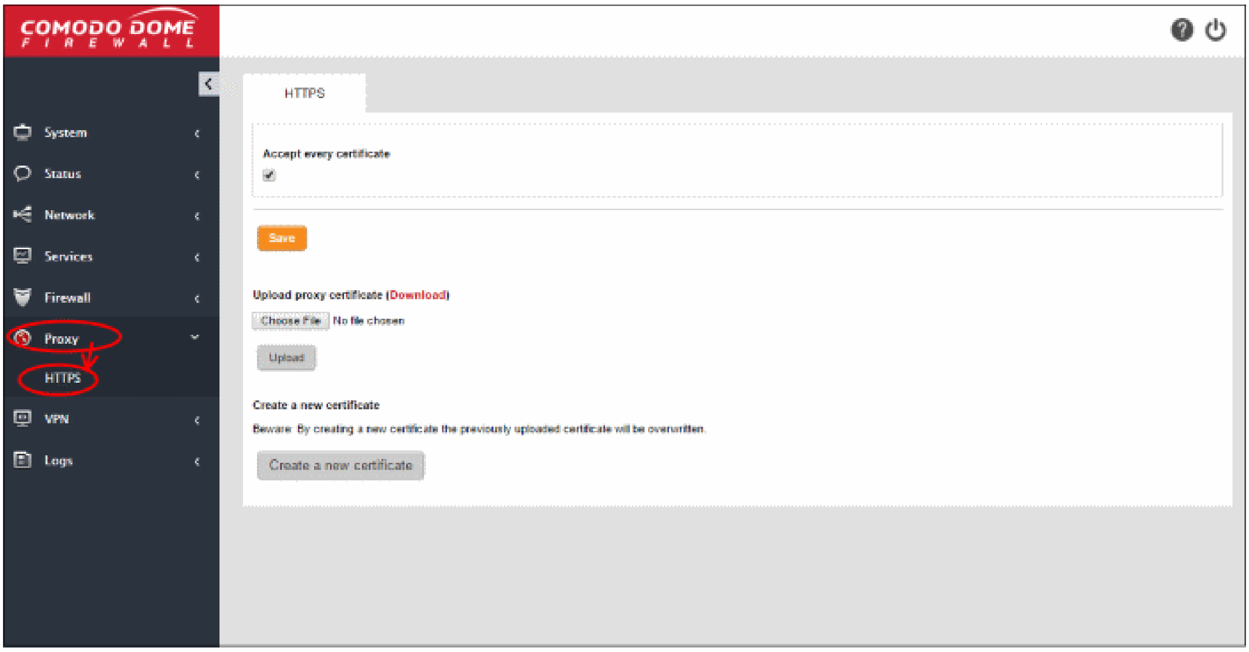
☐ Log accepted VPN connections

- Use the 'Enable VPN firewall' toggle switch to switch the state of the VPN firewall.
- Select the 'Log accepted VPN connections' checkbox to log the packets that has passed the VPN Policy. See section '**Viewing Logs**' for more details on viewing the logs.
- Click 'Save' for your settings to take effect .

9 Configuring HTTPS Proxy Services

- Dome Cloud 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 Cloud Firewall intermediate SSL certificate needs to be installed on endpoints in order to analyze SSL traffic and to authenticate themselves to the HTTPS proxy.
- Click 'Proxy' > 'HTTPS' on the left to configure the HTTPS proxy:



HTTPS

Accept every certificate

☑

Save

Upload proxy certificate (Download)

Choose File No file chosen

Upload

Create a new certificate

Beware: By creating a new certificate the previously uploaded certificate will be overwritten.

Create a new certificate

The interface allows you to enable the proxy service and upload the intermediate certificate.

Note: It is mandatory to install an intermediate certificate on client computers if you wish to use the HTTPS Proxy service. See **Certificate Settings** for more details.

- Accept every certificate - This option appears only if the HTTPS proxy service is enabled. If left unselected, DCF will only accept valid SSL certificates from remote servers. If enabled, the proxy will accept all certificates from 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 certificate needs be deployed to those endpoints in your network which will use the HTTPS proxy.

Using an existing certificate

If you already have an intermediate certificate you wish to use, you can upload and install it on client computers.

To upload an existing certificate

Prerequisite: Ensure the intermediate certificate is stored locally on the computer from which you are accessing the DCF admin console.

- Click the 'Choose File' button under the 'Upload proxy certificate' option, navigate to the location where the certificate is stored and click 'Open'.
- Click 'Upload'

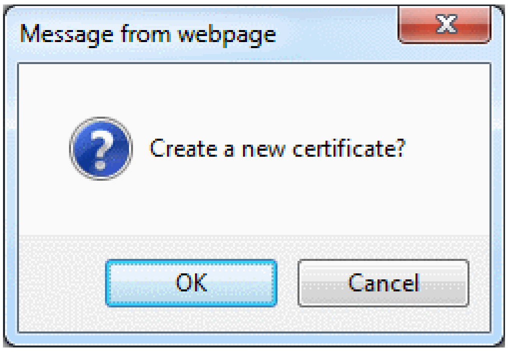
The certificate will be uploaded to DCF and deployed.

Creating a New Certificate

DCF is capable of creating a new self signed intermediate certificate with one year validity. Any existing certificates will be replaced by the new certificate. The certificate will then need to be installed on endpoints that need to authenticate themselves to the HTTPS proxy service.

To create a certificate

- Click the 'Create a new certificate' button. A confirmation dialog will be displayed.



Message from webpage

Create a new certificate?

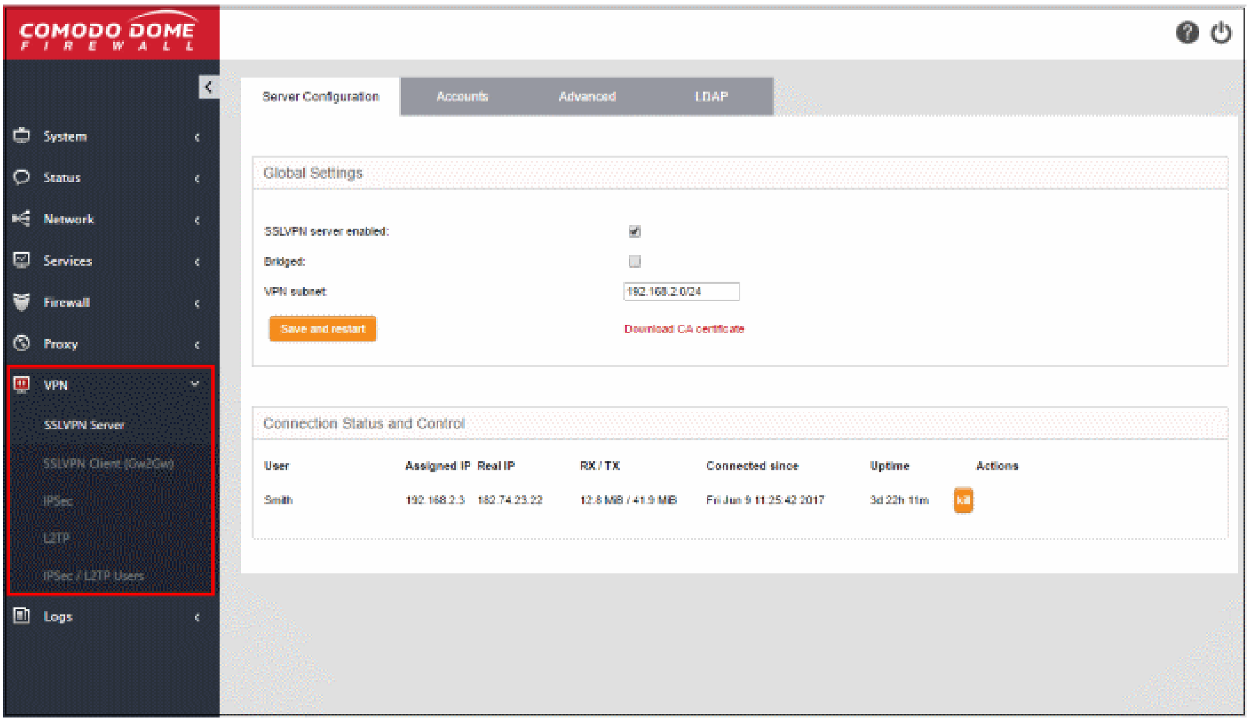
- Click 'OK'
- Click the 'Download' link so you can export the certificate to network endpoints.

10 Configuring Virtual Private Network Settings

The VPN section allows administrators to configure network and client settings in order to connect to Dome Cloud Firewall. Other settings that can be configured include user accounts, LDAP integration and more.

- SSLVPN Server – Allows you to configure client to site VPN connection to DCF. It also allows another DCF account and/or another VPN server configured as clients to connect in a gateway to gateway (Gw2Gw) setup.
- SSLVPN Client - DCF can act as a OpenVPN client to connect to other DCF accounts configured as SSLVPN server through Gw2Gw setup.
- IPsec – Allows you to configure and connect network and clients to DCF.
- L2TP Server - DCF 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: □

VPN subnet: 192.168.2.0/24

Save and restart

Download CA certificate

Connection Status and Control

User	Assigned IP	Real IP	RX / TX	Connected since	Uptime	Actions
Smith	192.168.2.3	182.74.23.22	12.8 MiB / 41.9 MiB	Fri Jun 9 11:25:42 2017	3d 22h 11m	kill

The following sections provide more information about configuring the services:

- **SSLVPN Server**
- **SSLVPN Client**
- **IPsec Configuration**
- **L2TP Server Configuration**
- **IPsec / L2TP Users Configuration**

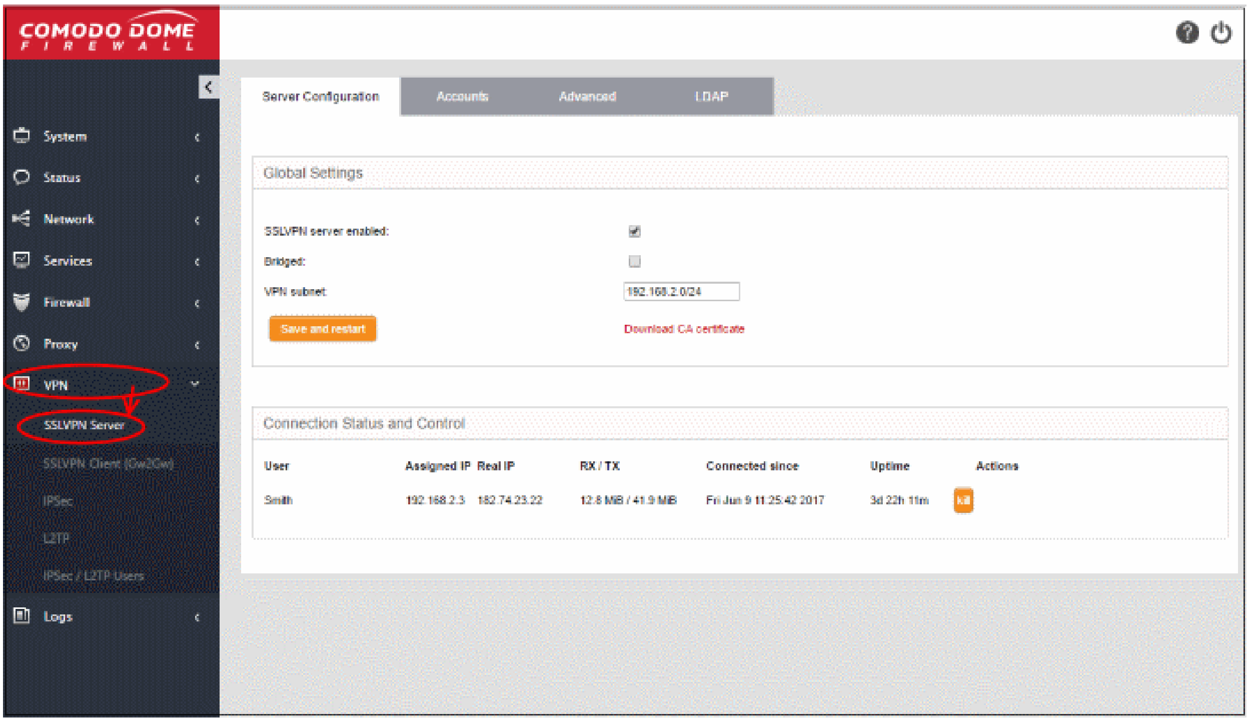
10.1 SSL VPN Server

The 'SSL VPN Server' interface allows you to enable/disable the service, configure connection settings, manage user accounts and integrate an LDAP server.

- Dome Cloud Firewall 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 DCF.
- Once configured, the server allows you to download the authentication certificate and client configuration file for deployment onto remote SSL VPN clients.

The SSL VPN server also accepts connection requests from another DCF account configured as an SSL VPN client as a gateway to gateway (Gw2Gw) connection. This allows remote networks to connect to other network zones.

To open the 'SSL VPN' interface, click 'VPN' > 'SSLVPN Server ' on the left hand menu:



Global Settings

SSLVPN server enabled: ☑

Bridged: □

VPN subnet: 192.168.2.0/24

Connection Status and Control

User	Assigned IP	Real IP	RX / TX	Connected since	Uptime	Actions
Smith	192.168.2.3	182.74.23.22	12.8 MiB / 41.9 MiB	Fri Jun 9 11:25:42 2017	3d 22h 11m	kill

The interface contains four tabs:

- **Server Configuration** - Enable/disable the SSL VPN server and configure general settings like dynamic IP address pool for assignment of IP addresses to the clients and so on. 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 advanced settings like 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 DCF. See '**Configuring Clients to Connect to DCF**' for more details.

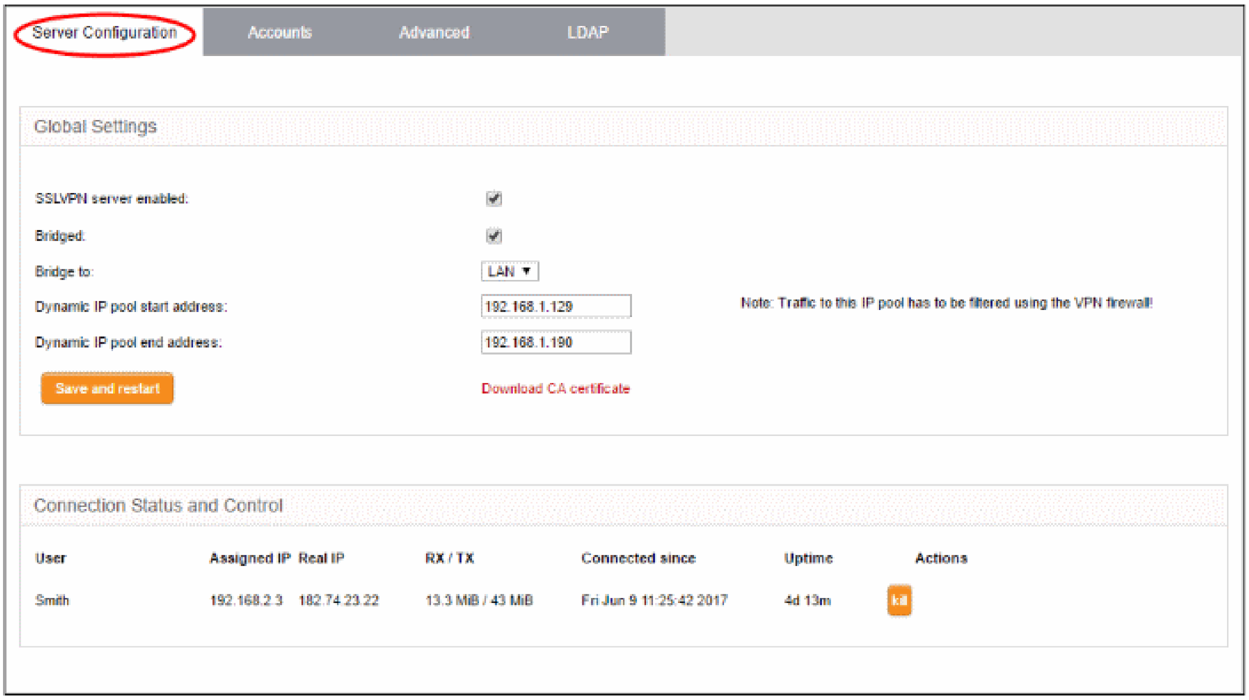
10.1.1 Configuring General SSL VPN Server Settings

This sections allows you to:

- Enable/disable the SSL VPN server
- Configure general 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 DCF. See '**Configuring Clients to Connect to DCF**' for more details about how to establish connection between individual clients and Dome Cloud 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:	192.168.1.129
Dynamic IP pool end address:	192.168.1.190

Note: Traffic to this IP pool has to be filtered using the VPN firewall!

Connection Status and Control

User	Assigned IP	Real IP	RX / TX	Connected since	Uptime	Actions
Smith	192.168.2.3	182.74.23.22	13.3 MiB / 43 MiB	Fri Jun 9 11:25:42 2017	4d 13m	kill

- 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 VPN firewall, if enabled. See '**Managing VPN Firewall 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 'Server Certificate' settings, refer to '**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. The list also allows the administrator to terminate unwanted VPN connections.

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.

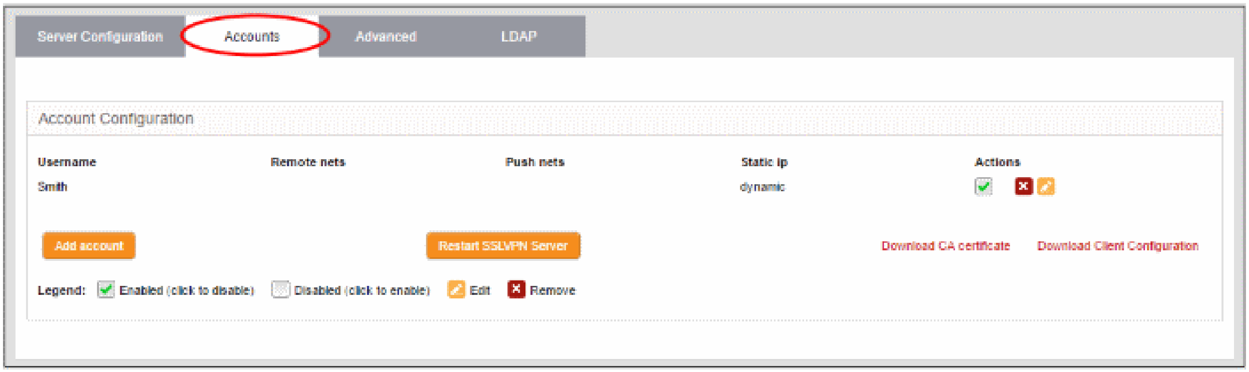
See '**Configuring Clients to Connect to DCF**' for more details about how to connect individual clients to DCF.

10.1.2 Managing SSL VPN Client Accounts

The 'Accounts' interface allows you to 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 DCF. See '**Configuring Clients to Connect to DCF**' for more details on how to connect individual clients to DCF.

To manage user accounts

- Click 'VPN' > 'SSLVPN Server' from the left hand side navigation
- Click the 'Accounts' tab.



Account Configuration

Username	Remote nets	Push nets	Static ip	Actions
Smith			dynamic	✓ ☒ ✎

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

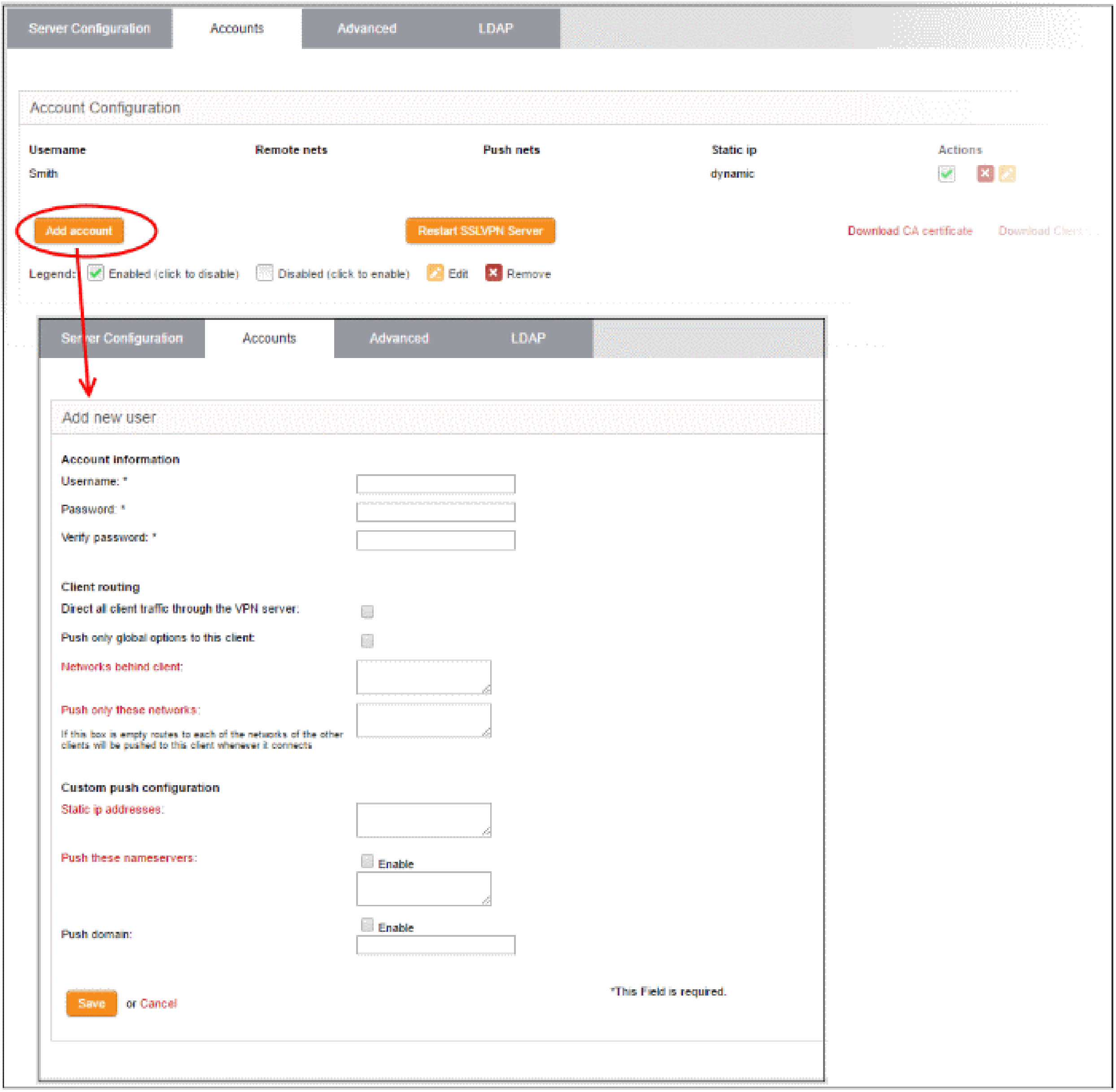
A list of existing user accounts will be displayed.

SSL VPN Server Account Configuration table - Column Descriptions	
Column	**Description**
Username	The user name of the account with which the client can log-in to the server.
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 the account. ✎ - Edit/configure the account. Editing/configuring an account is similar to 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 information



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: □

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.

Admins should specify the username and password for the account. These credentials will need to be entered in the SSL VPN client to authenticate 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 this option 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 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. Both items should be installed on your remote workstations to enable the connection. The server certificate type for authentication can be configured under '**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 DCF, 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).

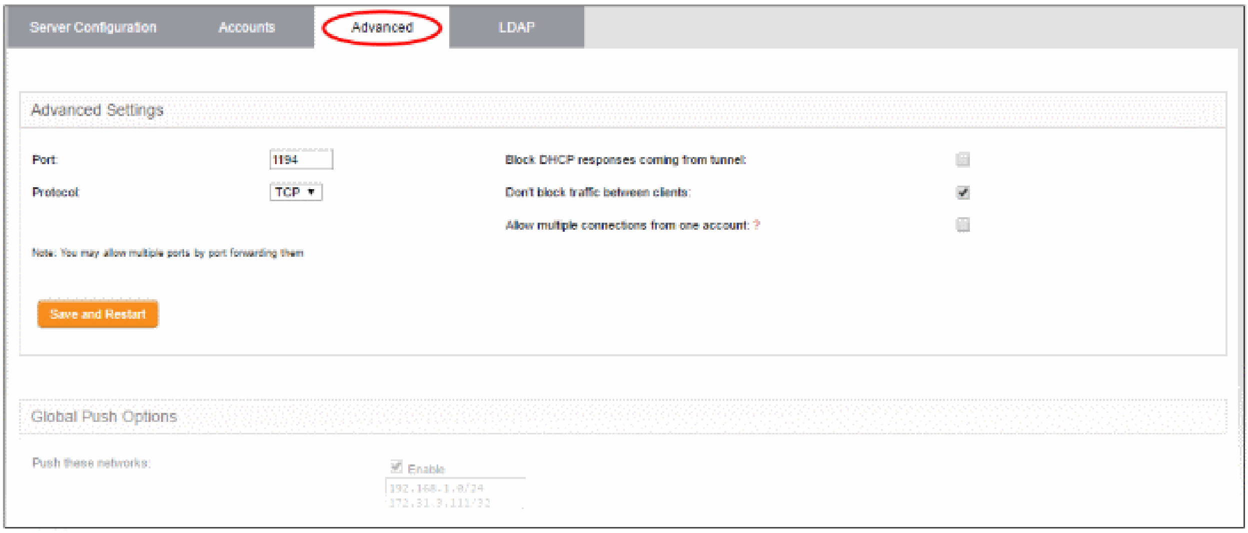
See '**Configuring Clients to Connect to DCF**' for more details about how to connect individual clients to DCF.

10.1.3 Configuring Advanced SSL VPN Server Settings

The 'Advanced' interface allows you to 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' from the left hand side navigation
- Click the 'Advanced' tab.



Advanced Settings

Port: 1194

Protocol: TCP ▾

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

Global Push Options

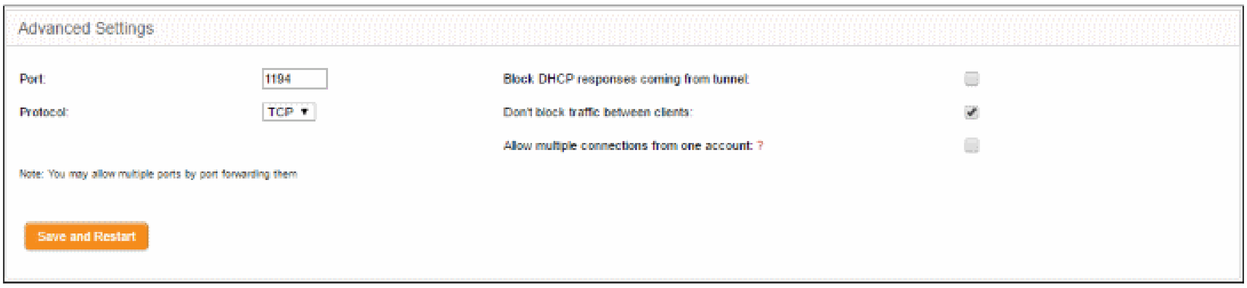
Push these networks: ☑ Enable
192.168.1.0/24
172.31.3.111/32

The 'Advanced' interface contains three areas:

- **Advanced Settings**
- **Global Push Options**

- **Authentication Settings**

Advanced Settings



Advanced Settings

Port: 1194

Protocol: TCP ▾

Note: You may allow multiple ports by port forwarding them

Block DHCP responses coming from tunnel: ☐

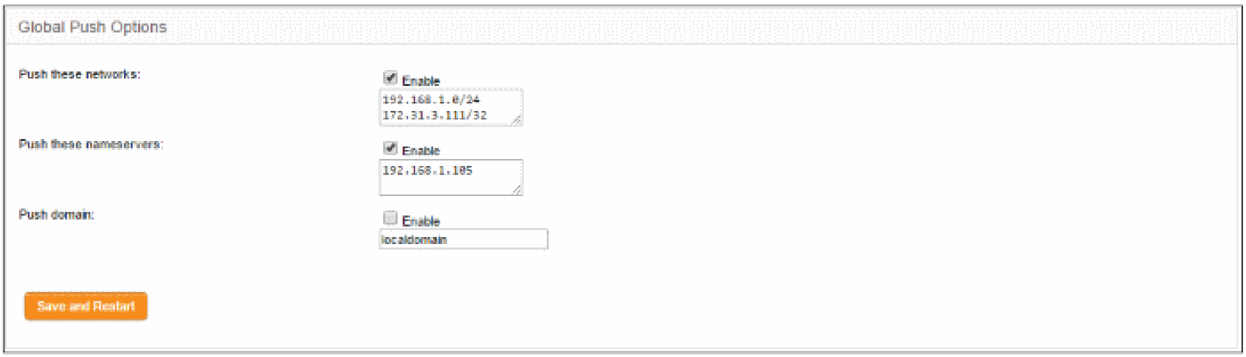
Don't block traffic between clients: ☑

Allow multiple connections from one account: ? ☐

- Port - Specify the port for listening to the VPN client requests. (***Default = 1194***). The administrator can also create port forwarding rules under **Firewall > SNAT**, to allow multiple ports to listen to the requests and forward them to the default port.
- Protocol - Choose the protocol to be used for VPN connections. (***Default = UDP***)
- 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.
- Don't block traffic between clients - By default, the VPN server does not allow the data traffic between the VPN clients connected to it. If you wish to allow the data transfer among the VPN clients, select this check box.
- Allow multiple connections from one account - By default, for a single user account, only one client can connect to the VPN server. If you wish to allow several clients at different locations to connect to the server using the same account, select this option. However, if several clients are using a single account, the '**VPN 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
192.168.1.0/24
172.31.3.111/32

Push these nameservers: ☑ Enable
192.168.1.105

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.

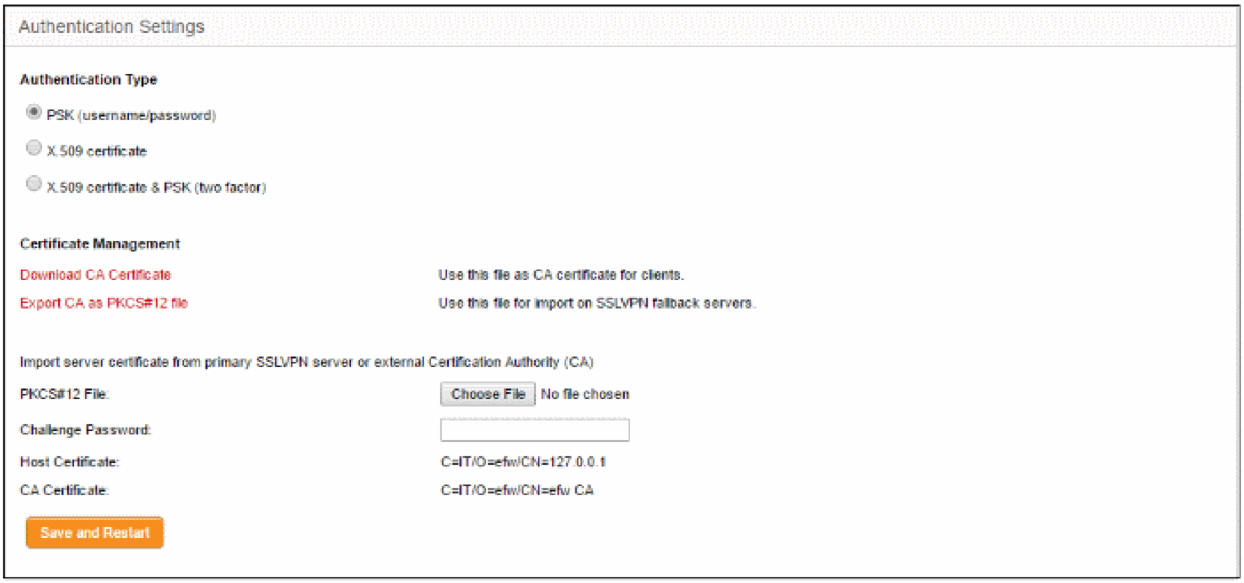
- **Pre-Shared Key (PSK)** (***Default***)
- **X.509 certificate**
- **X.509 certificate and PSK (two factor)**

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 DCF 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 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 DCF administrative console is accessed.

To import the certificate

- Click 'Choose File' 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'.

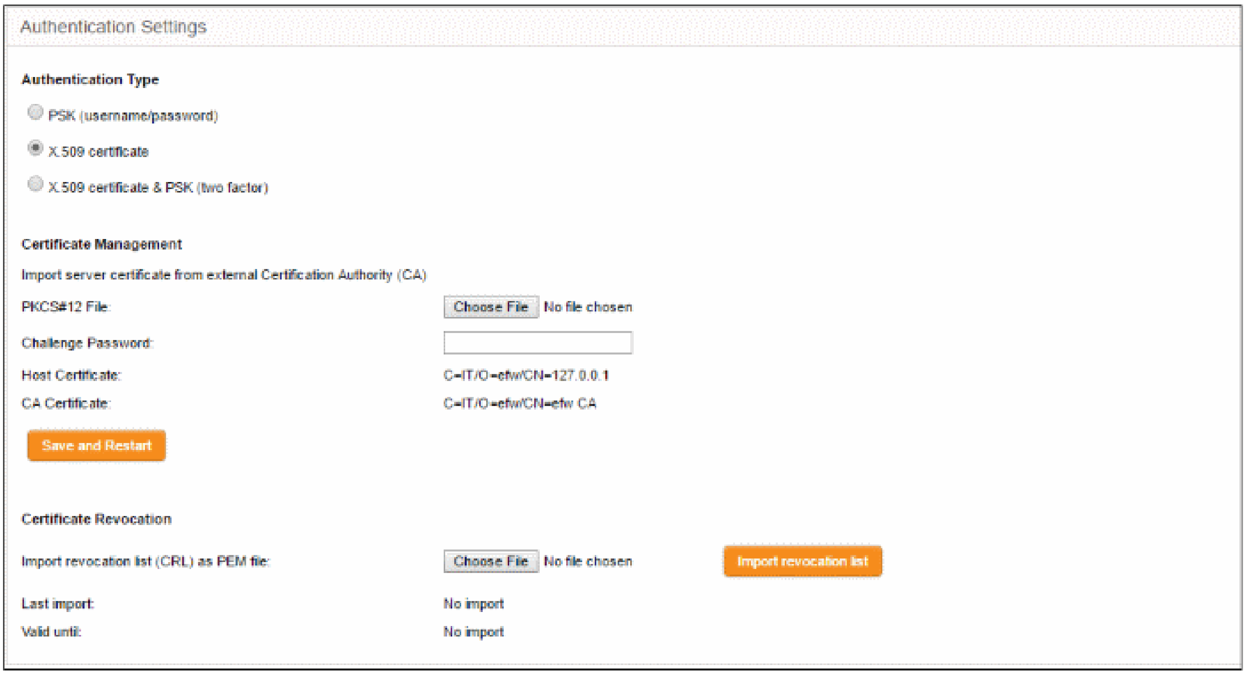
The certificate will be imported and the VPN server will be restarted for your configuration to take effect.

X.509 certificate

DCF 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 = ecf and CN = 127.0.01 from an external CA for uploading to the SSL VPN server.
- 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:	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 Revocation

Import revocation list (CRL) as PEM file:	Choose File No file chosen	Import revocation list
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 DCF administrative console is accessed.

- To import the server certificate obtained from an external CA click 'Choose File', 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

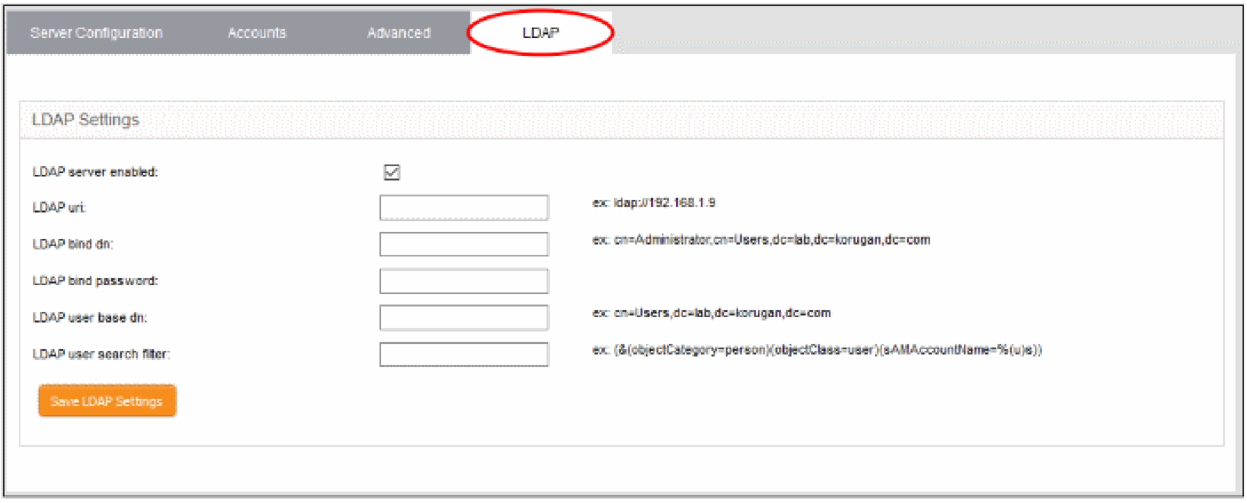
There are two ways you can configure Dome Cloud Firewall to authenticate users:

- Add users in the DCF 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))

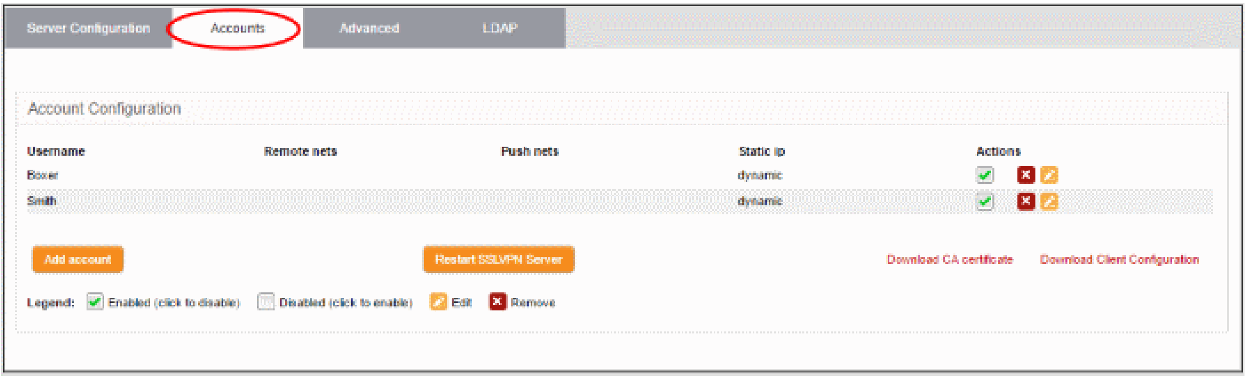
  - LDAP server enabled – Enable or disable user authentication via LDAP
  - LDAP uri – The URI of your LDAP server.
  - LDAP bind dn – Bind DN of the LDAP server
  - LDAP bind password – Password associated with the bind DN
  - LDAP user base dn – User base DN of the LDAP server
  - LDAP user search filter – Filter by user or group
- Click 'Save LDAP Settings' for your changes to take effect.

10.1.5 Configuring Clients to Connect to Dome Cloud Firewall

This section explains how to establish a 'Client-to-site VPN' connection to DCF 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 Cloud Firewall

- Click 'VPN' on the left then 'SSLVPN Server'
- Click the 'Accounts' tab:



Account Configuration

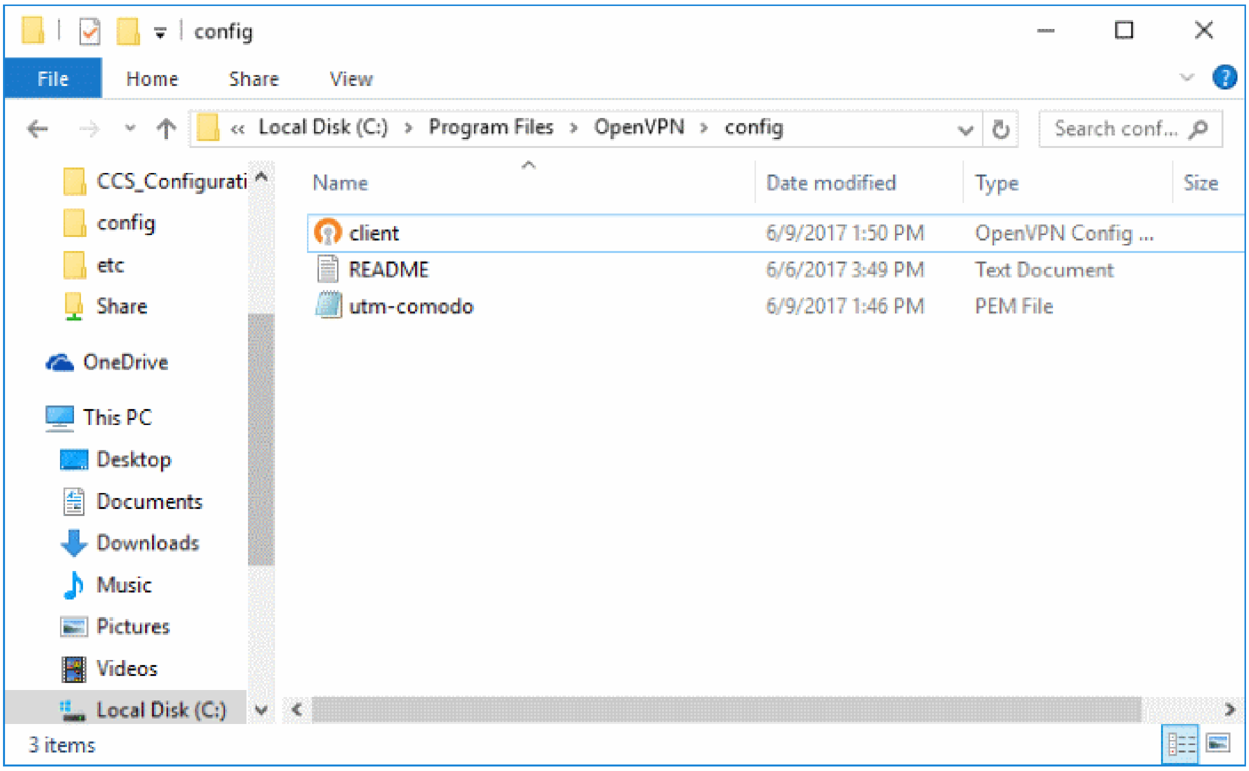
Username	Remote nets	Push nets	Static ip	Actions
Boxer			dynamic	✓ ☒ ✎
Smith			dynamic	✓ ☒ ✎

Add account | Restart SSLVPN Server | Download CA certificate | Download Client Configuration

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

Users added via DCF will be displayed.

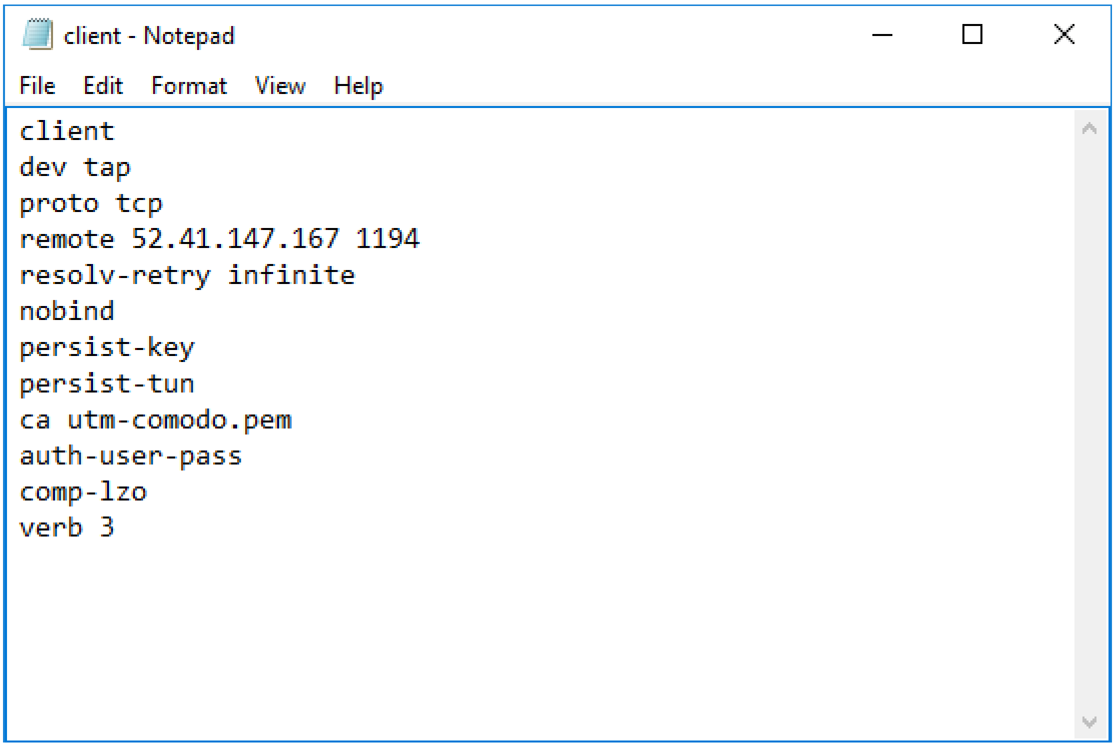
- Click the 'Download CA certificate' link to download the server certificate.
- Click the 'Download Client Configuration' link to download the SSL VPN client configuration file in .ovpn format.
- Download and install OpenVPN GUI client on computers that you want to connect to DCF. You can download the 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	

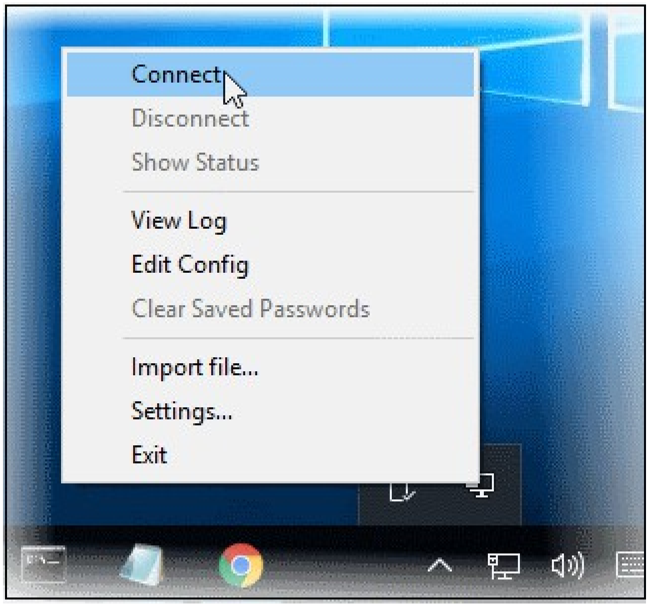
3 items

- Open the configuration file and make sure the parameters are as shown below:

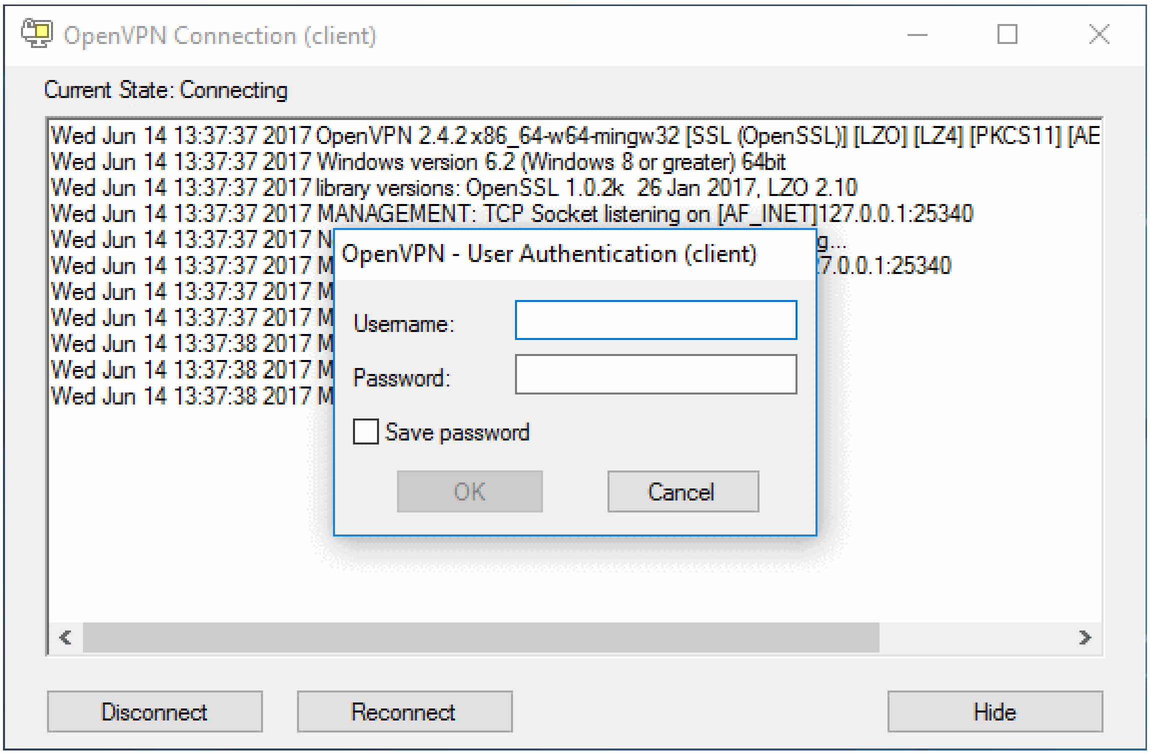


```
client
dev tap
proto tcp
remote 52.41.147.167 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca utm-comodo.pem
auth-user-pass
comp-lzo
verb 3
```

- 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 DCF 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 DCF, 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:



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
```

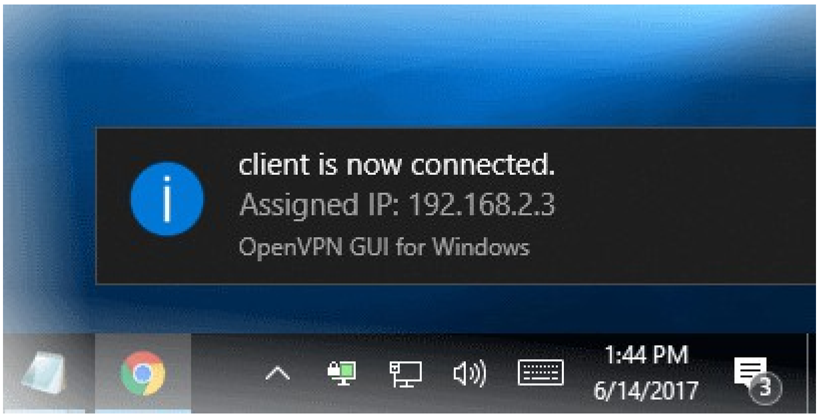
OpenVPN - User Authentication (client)

Username:

Password:

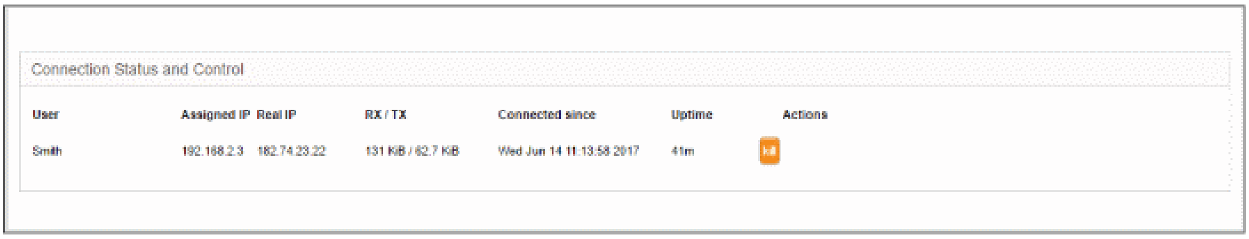
□ Save password

- Complete the 'Username' and 'Password' fields and click 'OK'.
- After successful authentication, the client will be connected to DCF 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 DCF 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

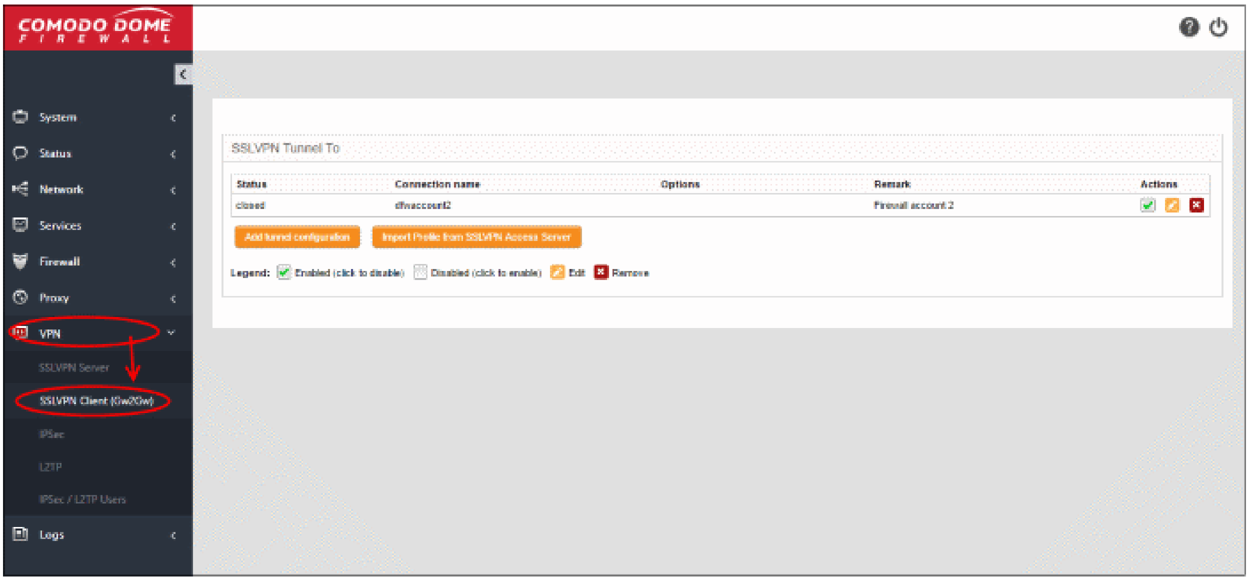
See '**IPsec Configuration**' for details about connecting networks to DCF.

10.2 SSLVPN Client

The firewall can be configured to create secure tunnels to other SSL VPN servers and/or other DCF 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.

To open the 'SSLVPN Client' interface, click 'VPN' > 'SSLVPN Client (Gw2Gw)' on the left menu:



SSLVPN Tunnel To

Status	Connection name	Options	Remark	Actions
closed	dfwaccount2		Firewall account 2	✓ ✎ ✖

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

SSL VPN Clients table - Column Descriptions	
Column	**Description**
Status	Indicates the 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 name given to the connection for identification.
Options	Additional connection options, if any, specified during creation of the tunnel.
Remark	A short description of the tunnel.
Actions	Displays control buttons for enabling, editing and deleting the tunnel. ✓ - The checkbox 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 . 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 configured in two ways:

- **Creating a new tunnel configuration**

- Importing the configuration from the SSL VPN server

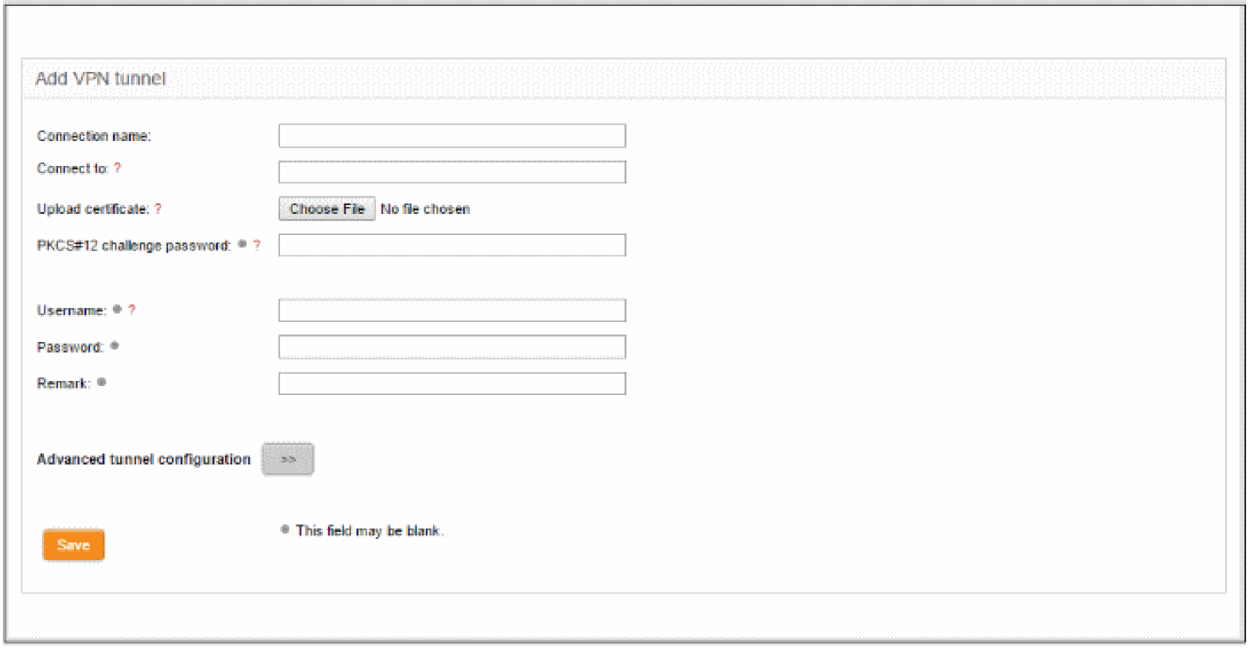
Creating a New Tunnel Configuration

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 as a PKCS#12 certificate and stored locally in the computer from which the DCF administrative 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:

Connect to: ?

Upload certificate: ? Choose File No file chosen

PKCS#12 challenge password: * ?

Username: * ?

Password: *

Remark: *

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

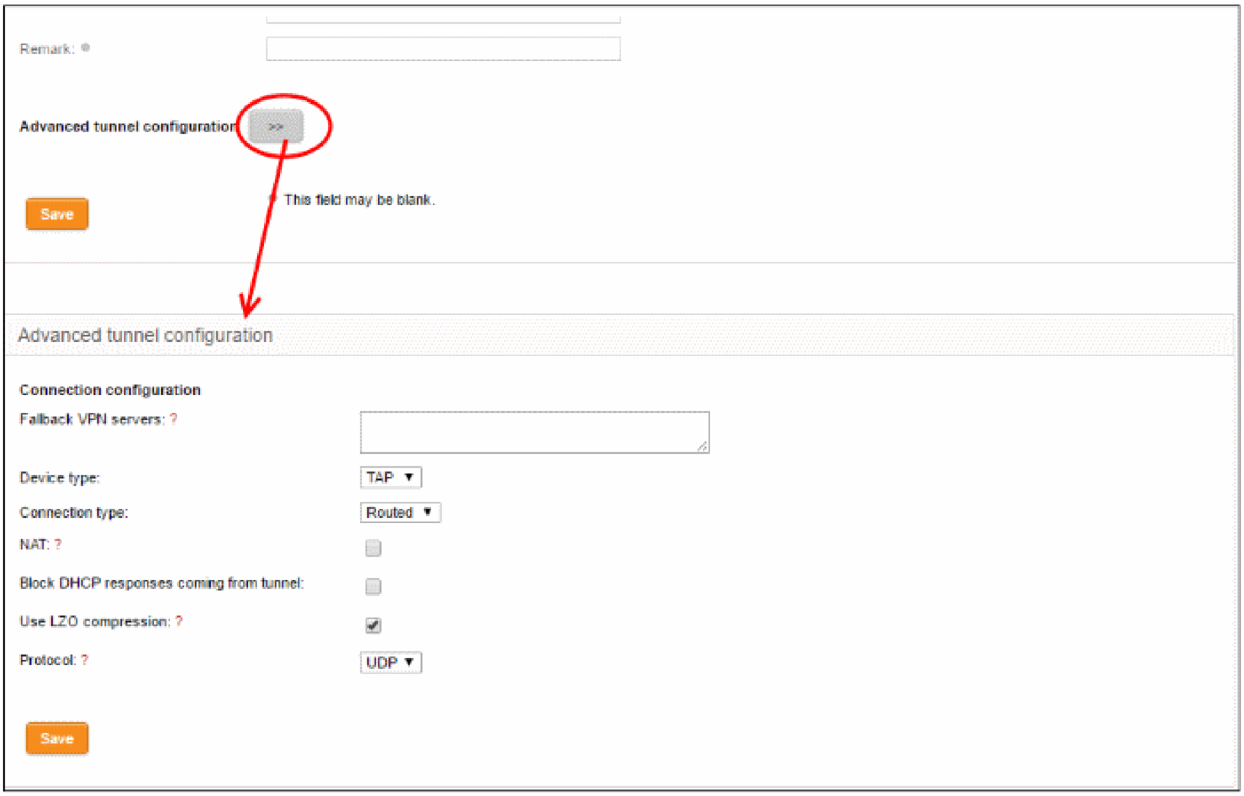
  Specify the protocol in lowercase letters. If the default protocol UDP is used, you need not specify the protocol
- Upload certificate - The server certificate of the external VPN server needs to be imported into the client.
  - If the external VPN server uses PSK type authentication, then the server's 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 'Choose File' 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: ●

Advanced tunnel configuration >>

Save

● This field may be blank.

Advanced tunnel configuration

Connection configuration

Fallback VPN servers: ?

Device type: TAP

Connection type: Routed

NAT: ? □

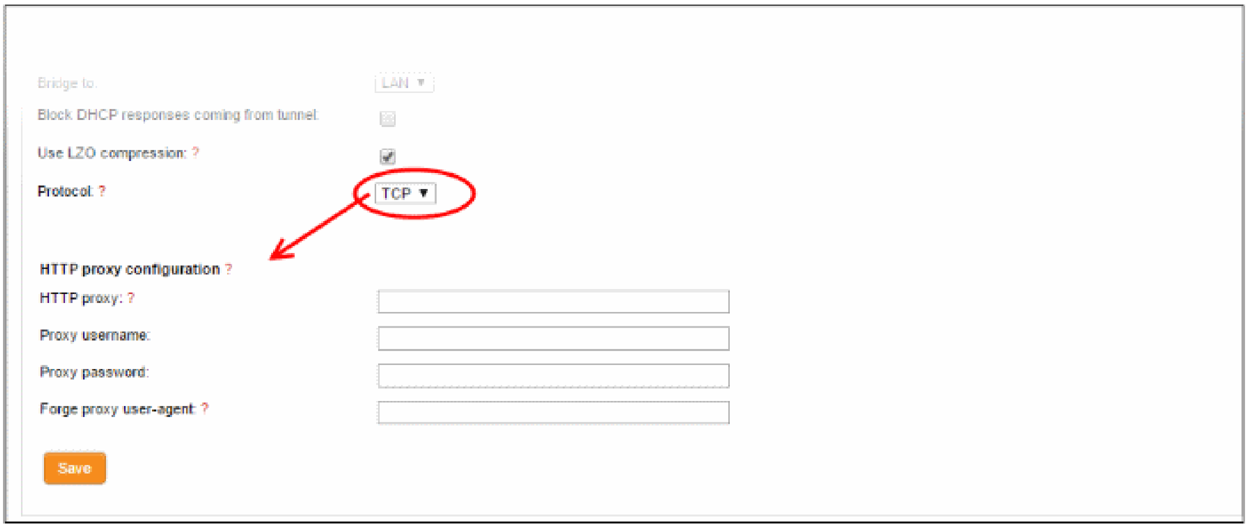
Block DHCP responses coming from tunnel: □

Use LZO compression: ? ☑

Protocol: ? UDP

Save

- 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 UTM 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.



Bridge to: LAN ▾

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 UTM 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'.

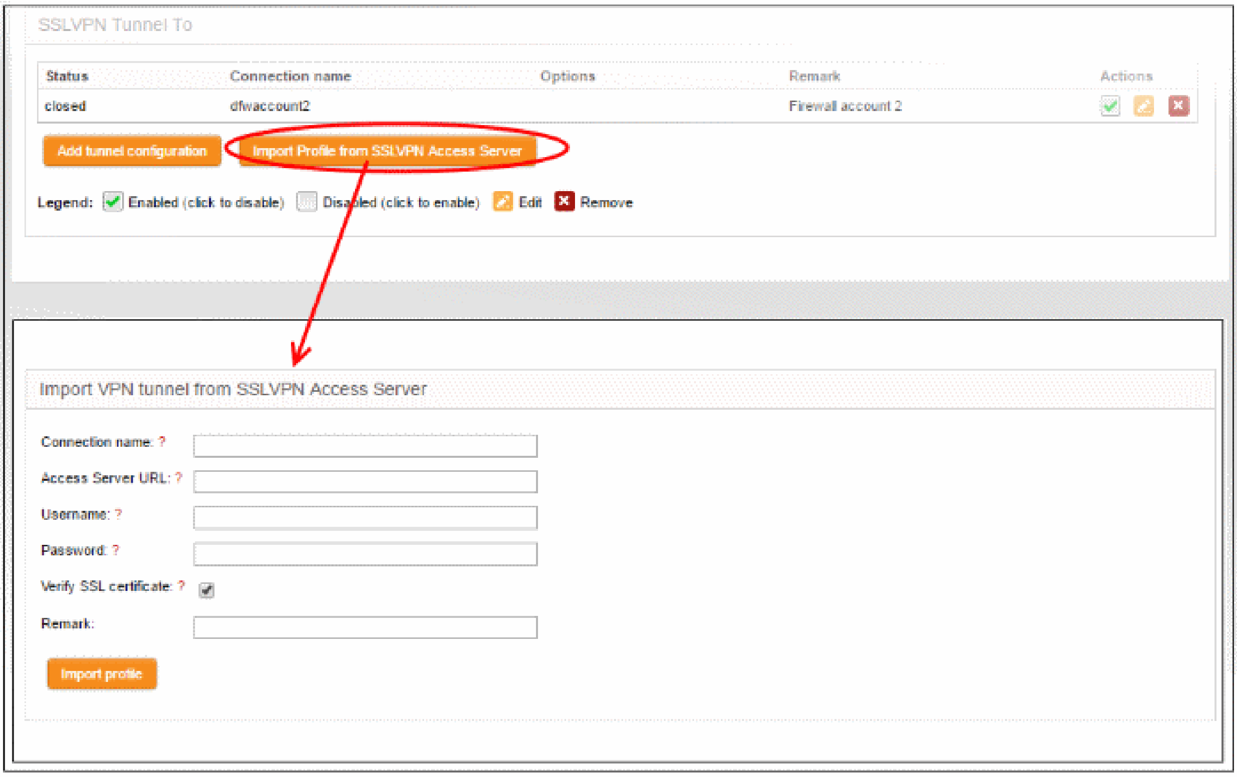
The new advanced parameters for the tunnel configuration will be saved.

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
closed	dfwaccount2		Firewall account 2	☑ ✎ ☒

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

Import VPN tunnel from SSLVPN Access Server

Connection name: ?	
Access Server URL: ?	
Username: ?	
Password: ?	
Verify SSL certificate: ?	☑
Remark:	

- 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.

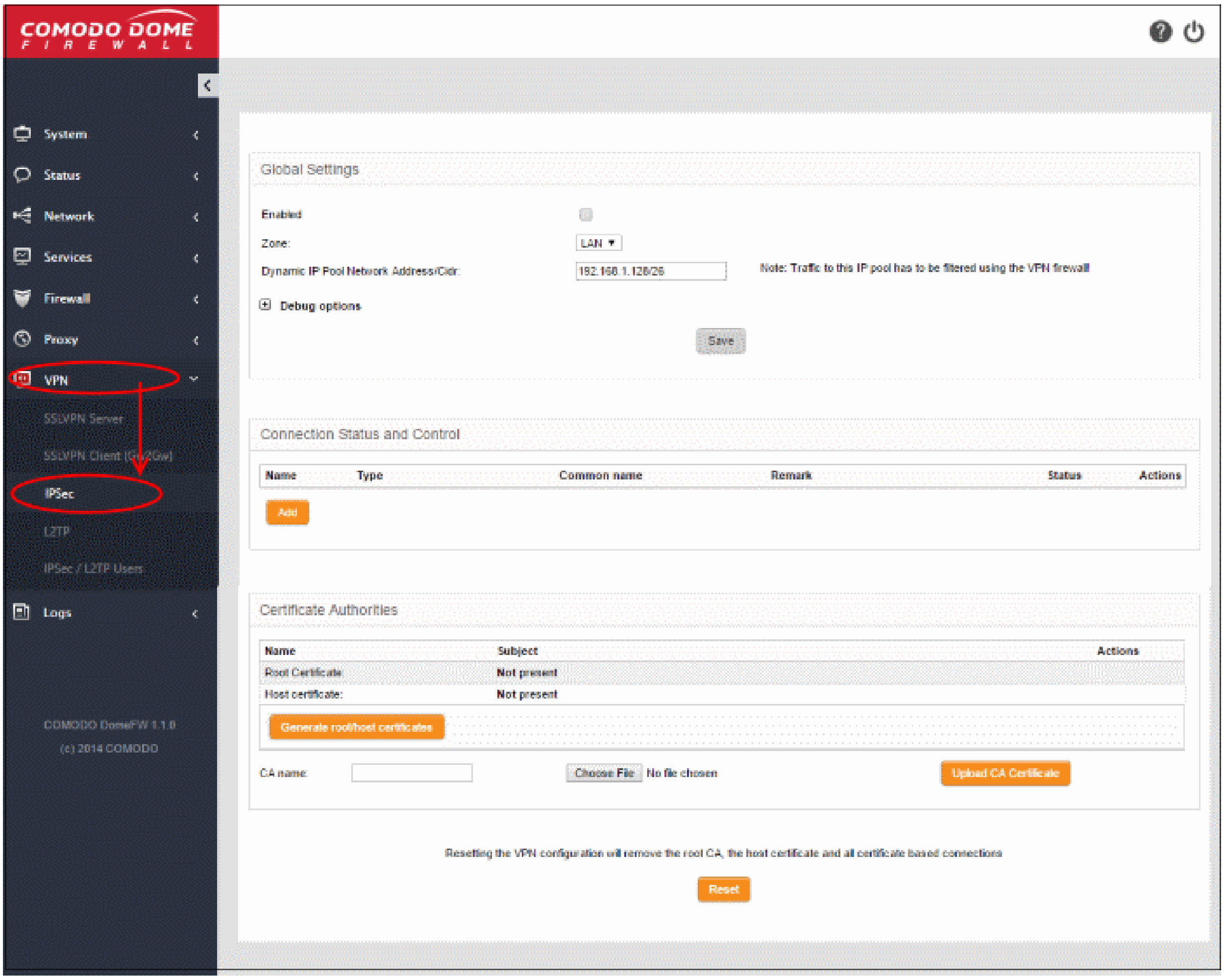
- Click 'Import Profile' after entering the details. The client will connect to the server and import the client configuration file. A new tunnel will be configured with the imported configuration profile.

10.3 IPSec Configuration

This area allows administrators to configure IPsec tunnels between different networks and sites. Dome Cloud 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' on the left menu:



Global Settings

Enabled □

Zone: LAN

Dynamic IP Pool Network Address/Cidr: 192.168.1.128/26

Note: Traffic to this IP pool has to be filtered using the VPN firewall

⊞ Debug options

Save

Connection Status and Control

Name	Type	Common name	Remark	Status	Actions

Add

Certificate Authorities

Name	Subject	Actions
Root Certificate:	Not present	
Host certificate:	Not present	

Generate root/host certificates

CA name: Choose File No file chosen Upload CA Certificate

Resetting the VPN configuration will remove the root CA, the host certificate and all certificate based connections

Reset

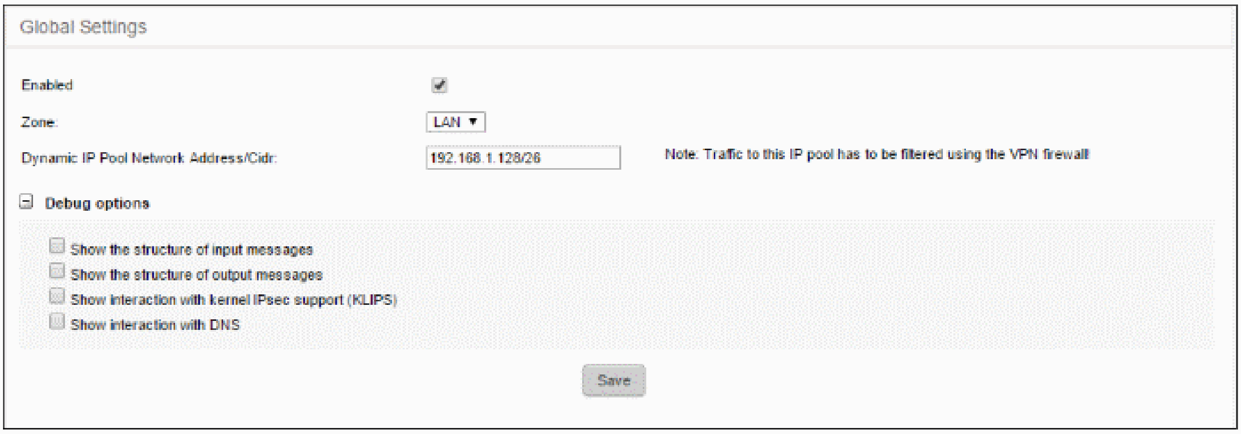
Administrators can use the interface to create, enable, configure and monitor IPsec connections, and to configure authentication preferences. Authentication between IPsec connected interfaces can be implemented via certificate-based authentication or by pre-shared key.

The interface contains three areas:

- Global Settings
- Connection status and control
- Certificate authorities

Global Settings

The 'Global Settings' area allows administrators to enable or disable the IPsec VPN service, to configure which internal network zones can be accessed over IPsec and to specify the dynamic IP address pool that should be used when assigning addresses to external clients. The 'Debug Options' area allows administrators to choose how much information is included in IPsec events in debugging logs.



Global Settings

Enabled ☑

Zone: LAN ▾

Dynamic IP Pool Network Address/Cidr: 192.168.1.128/26

Note: Traffic to this IP pool has to be filtered using the VPN firewall!

⊟ Debug options

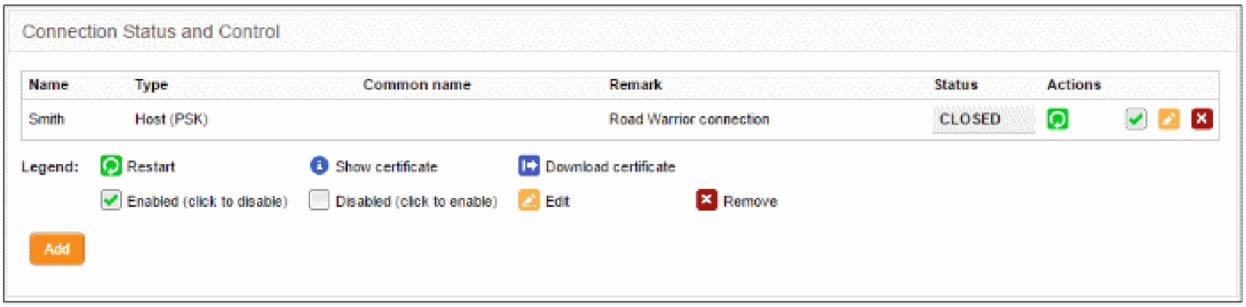
- □ Show the structure of input messages
- □ Show the structure of output messages
- □ Show interaction with kernel IPsec support (KLIPS)
- □ Show interaction with DNS

- 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 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 displays a list of IPsec tunnels that have been added, their connection status and controls for enabling, disabling and editing them.



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

IPsec Connection Status and Control table - Column Descriptions	
Column	**Description**
Name	The name for identifying 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 the client certificate to be installed on the client and entering username and password. The client certificate can be generated from DCF and deployed in the client device.
Common Name	If certificate type authentication is used, the Common Name fields included in the certificate is displayed here.

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 administrators to re-establish closed connections. ℹ - Available only for connections with certificate type authentication. Click this icon to view 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 . See **adding a new IPsec tunnel configuration** for more details. ☒ - Removes the tunnel configuration.

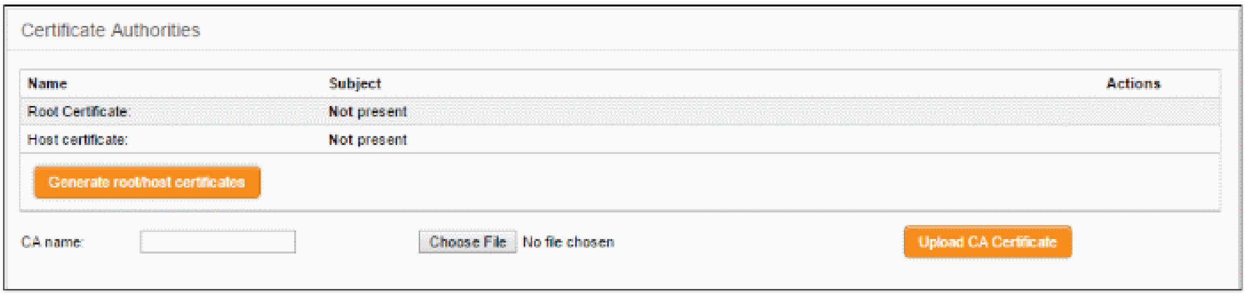
Certificate Authorities

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 DCF and sent to the client ;
- Generated by DCF by signing the certificate request received from the client; or
- Obtained from an external CA.

Initially, no certificate will be available with DCF. 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 DCF. 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	

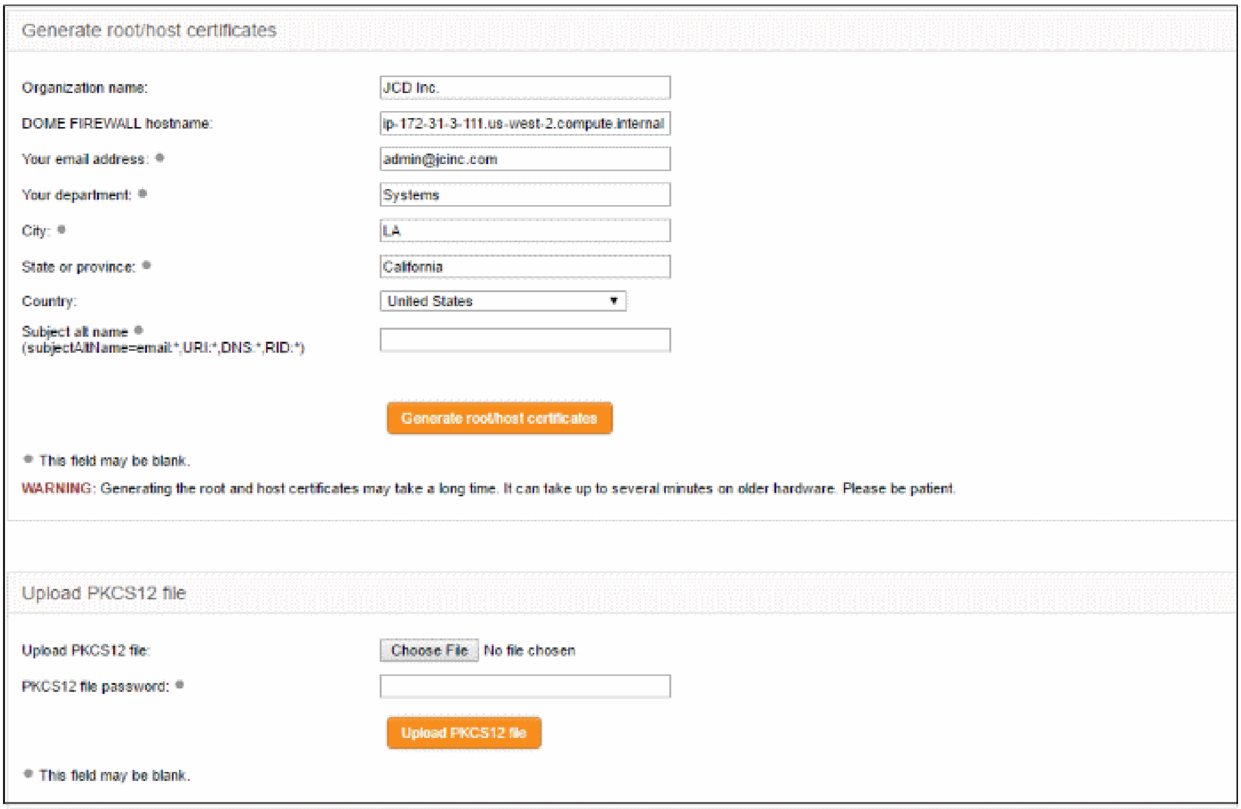
The following sections explain on:

- **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 DCF.
- 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 DCF, if any.

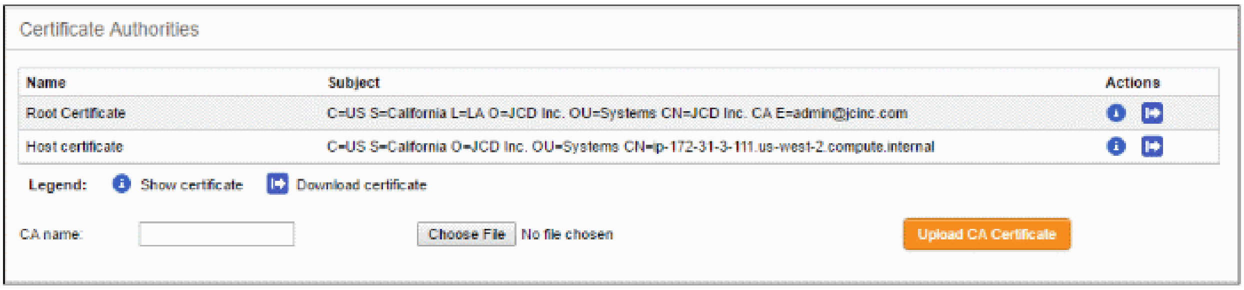
- Click 'Generate root/host certificate'

Alternatively, if the administrator has any of the previously generated certificates stored in PKCS12 format, then the certificate can be uploaded to the appliance, instead of creating new certificates.

To upload an existing certificate

- Click the 'Choose File' button beside 'Upload PKCS12 file' and navigate to the location in the local storage or the network where the certificate was exported and stored'
- Enter the password entered while exporting the certificate
- Upload 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

At a time only one certificate can be stored which serves 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 DCF 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 DCF.

Adding a New Tunnel Configuration

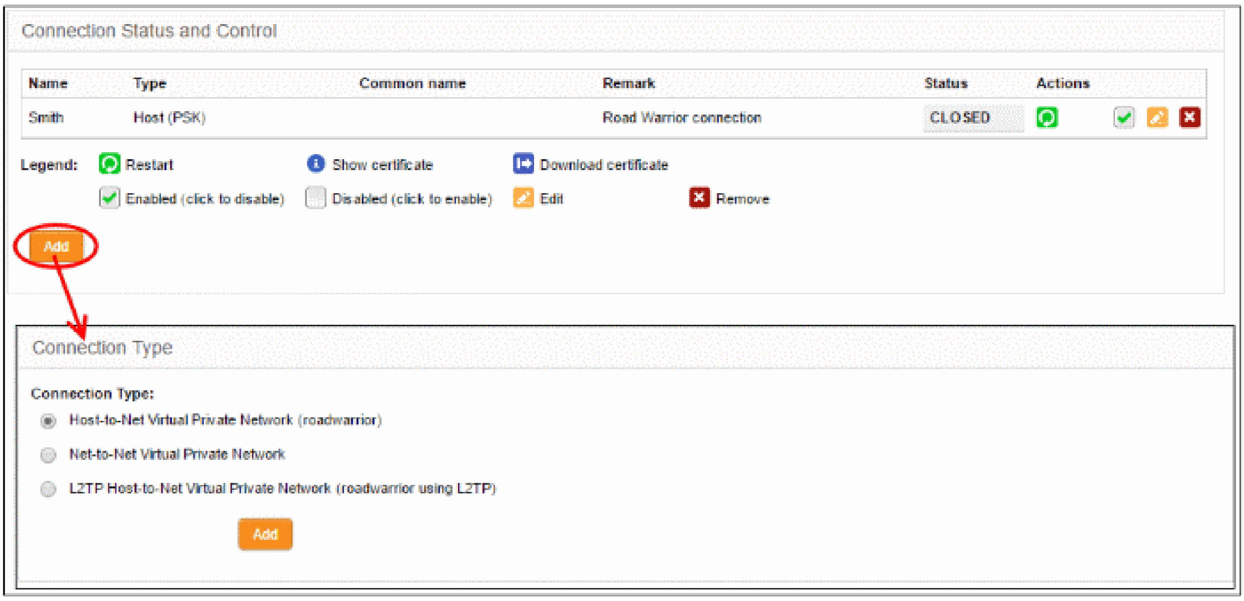
Three types of IPsec VPN Tunnels can be created in Comodo Dome Cloud Firewall:

- 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 DCF. 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)

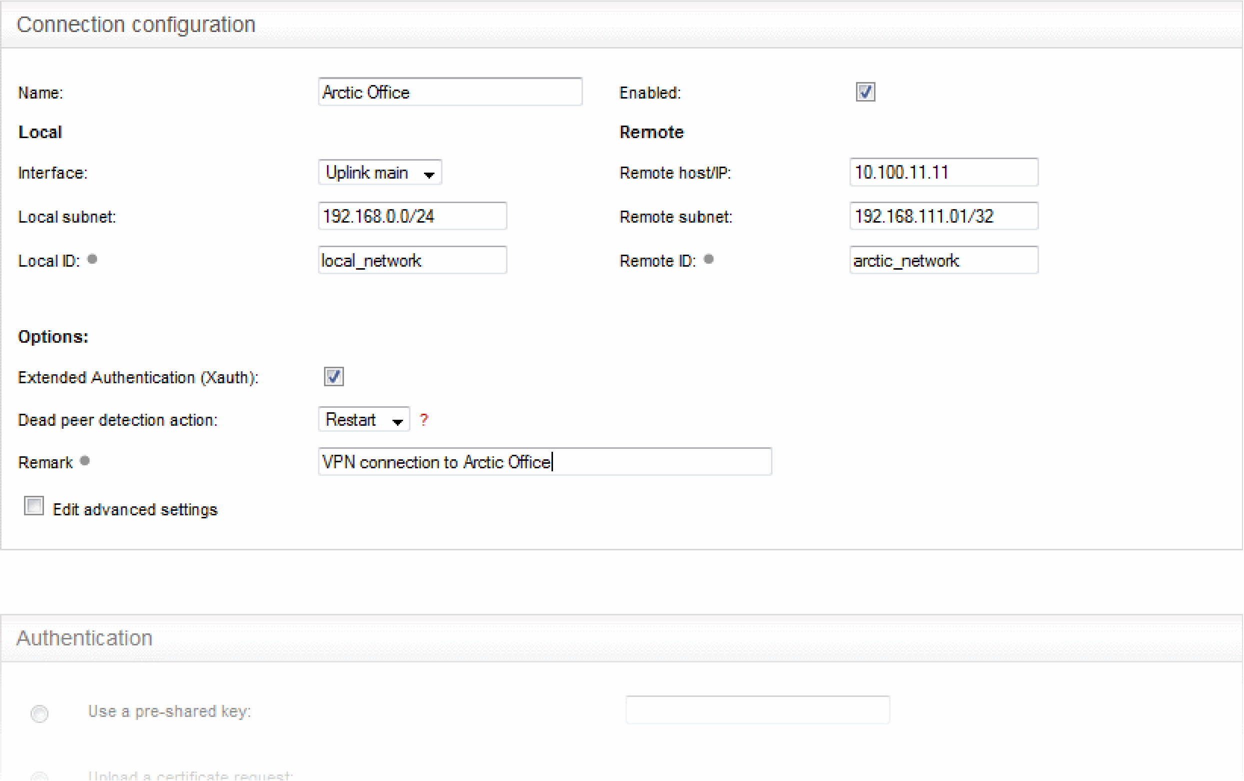
○ Net-to-Net Virtual Private Network

○ 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 DCF, 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

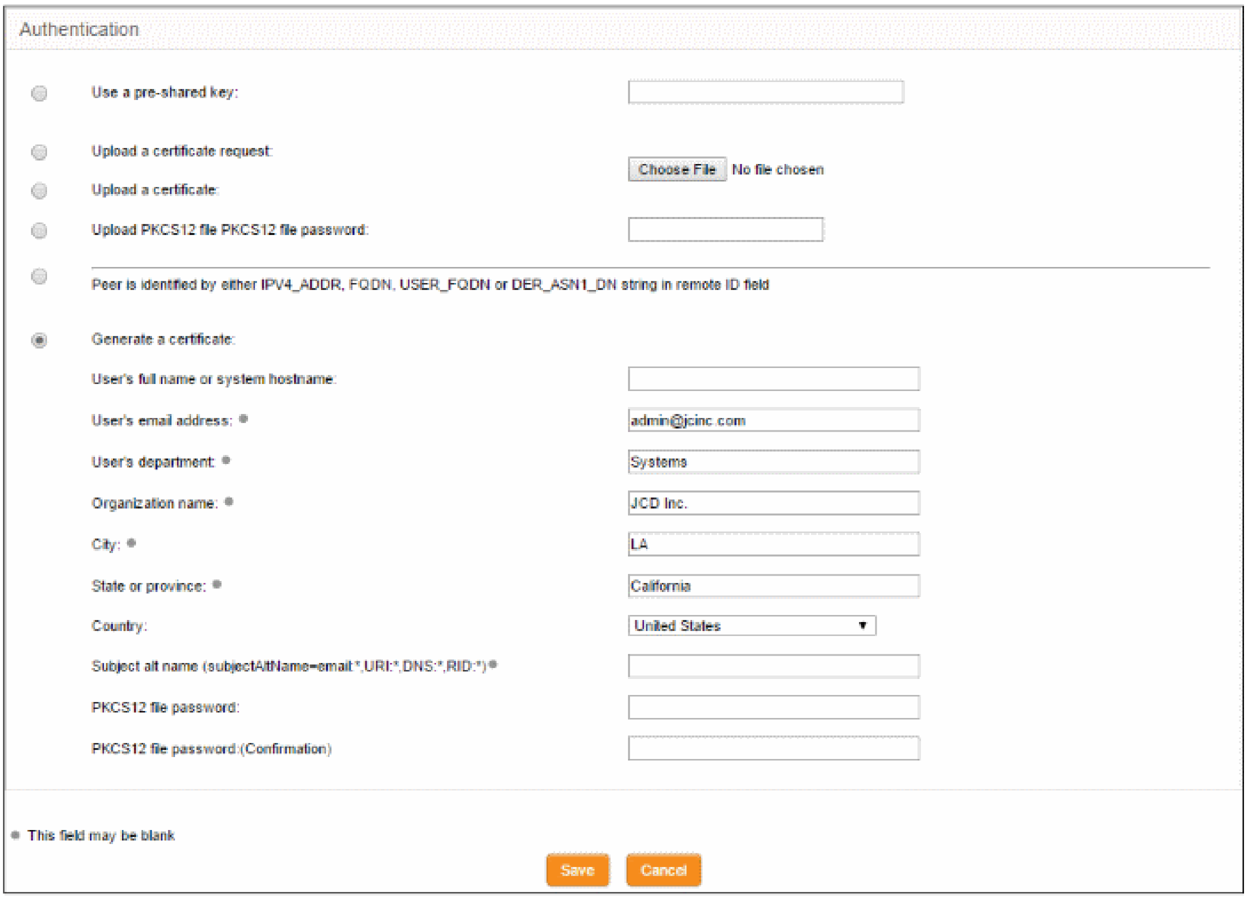
- Remote host/IP - Enter the IP address or hostname of the external host or network
- Remote subnet - The option is available only if you are creating 'Net to Net' connection type. Specify the sub network of the external network that can connect through the tunnel
- Remote ID - Enter an identification 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 DCF 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:	Choose File No file chosen
○	Upload a certificate:	
○	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 DCF. 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 DCF. Dome Cloud Firewall 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 'Choose File' 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 DCF. To upload the certificate, select this option and click the 'Choose File' 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 DCF. To upload the certificate, select this option and click the 'Choose File' 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.

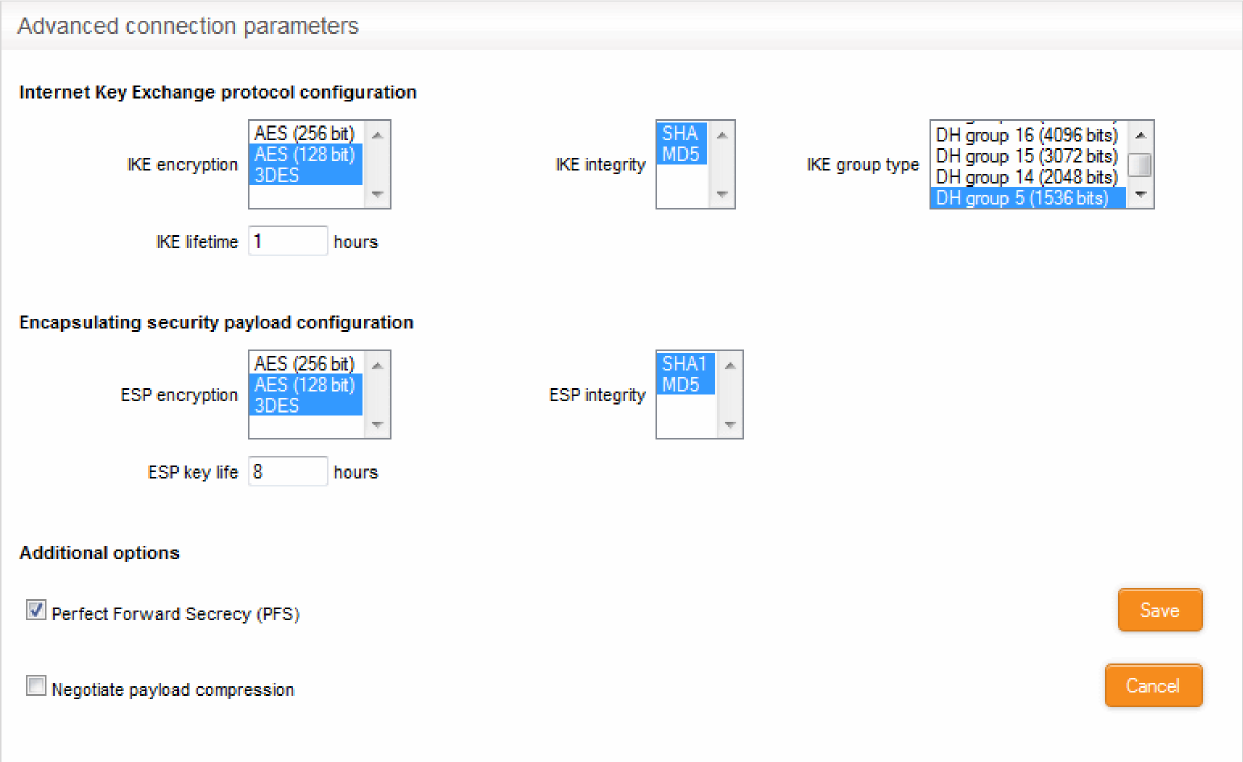
- Generate Certificate - Select this option if you wish to generate a new client certificate for the remote host signed by the Root certificate of IPsec server in DCF. Enter the parameters for the certificate in the fields below. Upon generation, the client certificate will be available for download 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), 3DES

IKE integrity: SHA, MD5

IKE group type: DH group 16 (4096 bits), DH group 15 (3072 bits), DH group 14 (2048 bits), DH group 5 (1536 bits)

IKE lifetime: 1 hours

Encapsulating security payload configuration

ESP encryption: AES (256 bit), AES (128 bit), 3DES

ESP integrity: SHA1, MD5

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.

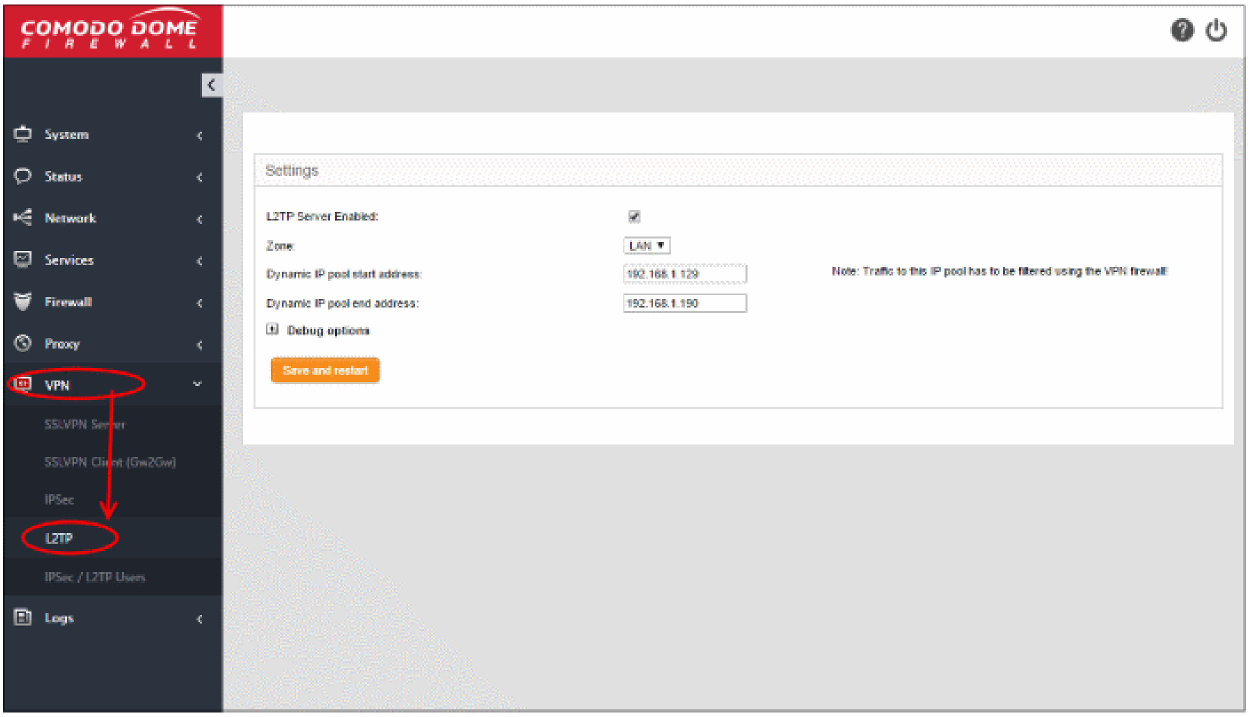
- Click 'Save' for your configuration to take effect.

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 Cloud 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.

- To open the 'L2TP' interface, click 'VPN' > 'L2TP' on the left menu:



Settings

L2TP Server Enabled: ☑

Zone: LAN ▾

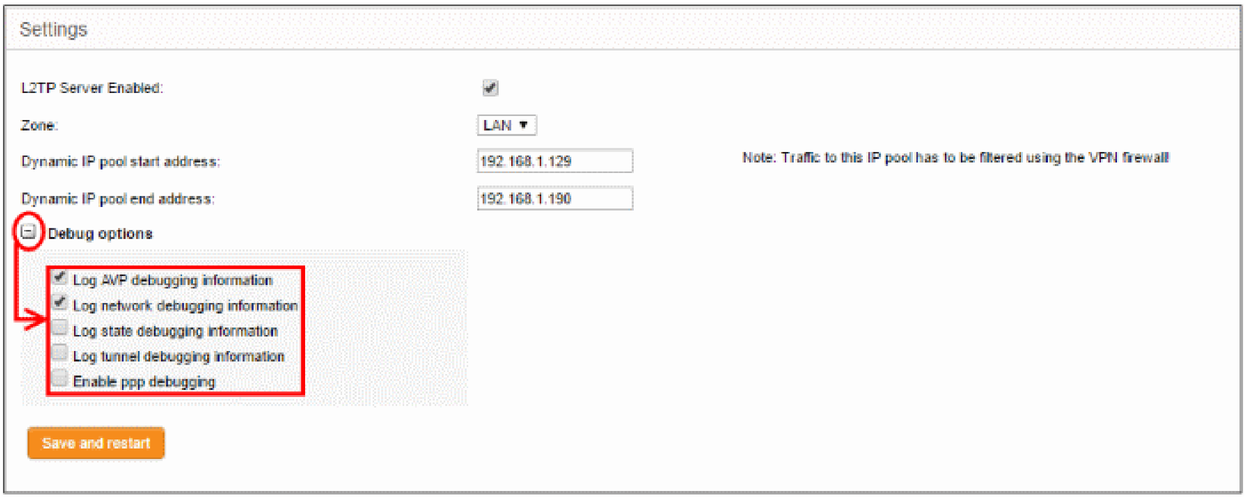
Dynamic IP pool start address: 192.168.1.129 Note: Traffic to this IP pool has to be filtered using the VPN firewall

Dynamic IP pool end address: 192.168.1.190

⊞ Debug options

Save and restart

- 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 - Configure the level of detail recorded about L2TP events in the event of connection failures. The log file is located at /var/log/messages in the internal storage of the 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 Note: Traffic to this IP pool has to be filtered using the VPN firewall

Dynamic IP pool end address: 192.168.1.190

⊟ Debug options

☑ Log AVP debugging information
☑ Log network debugging information
☐ Log state debugging information
☐ Log tunnel debugging information
☐ Enable ppp debugging

Save and restart

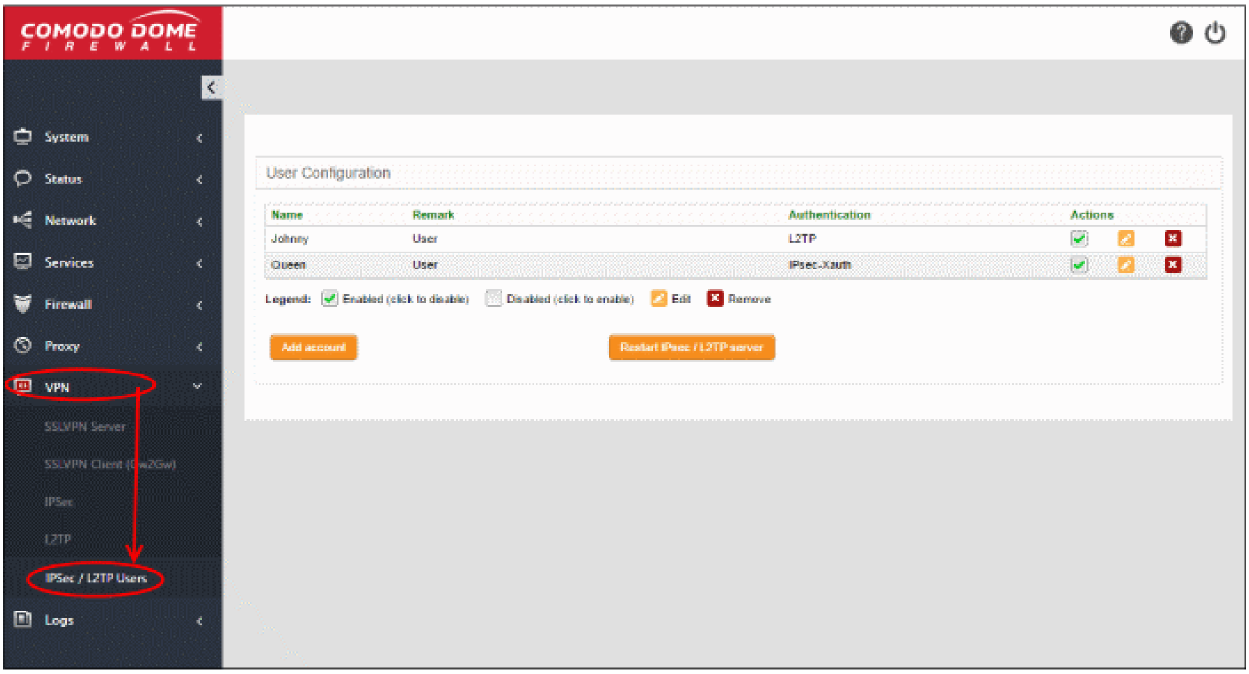
- Click 'Save and restart'. The VPN server needs to be restarted for your configuration to take effect.

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 allows you to 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
Johnny	User	L2TP	☑ ✎ ☒
Queen	User	IPsec-Xauth	☑ ✎ ☒

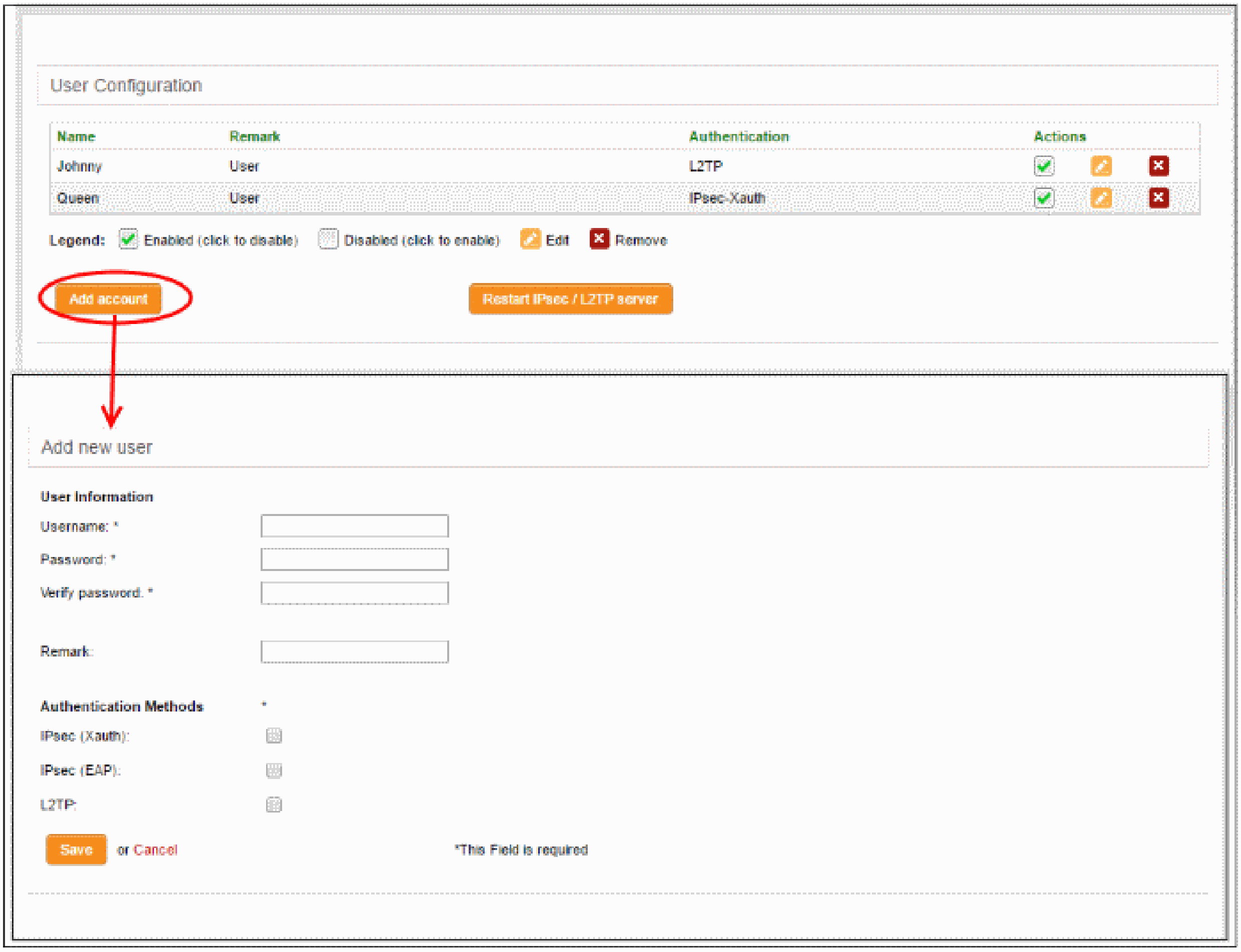
Legend: ☑ Enabled (click to disable) □ Disabled (click to enable) ✎ Edit ☒ Remove

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	The name of the user.
Remark	A short description of the 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
Johnny	User	L2TP	☑ ✎ ☒
Queen	User	IPsec-Xauth	☑ ✎ ☒

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

Add new user

User Information

Username: *

Password: *

Verify password: *

Remark:

Authentication Methods *

IPsec (Xauth): □

IPsec (EAP): □

L2TP: □

*This Field is required

User Information

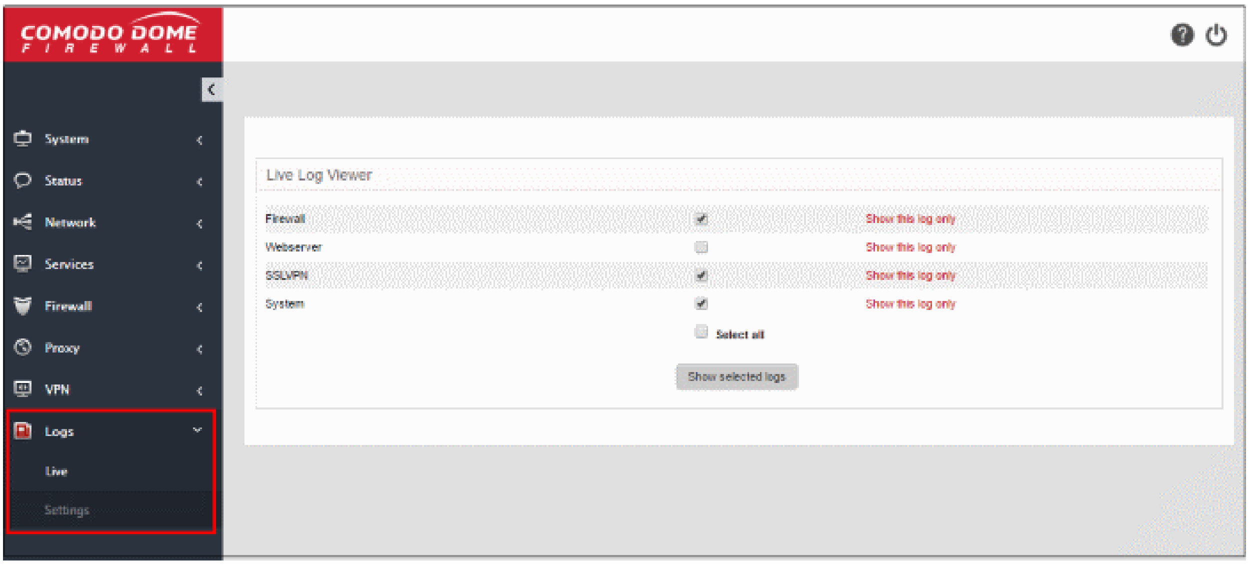
- Username - Enter the name of the user
- Password - Enter the password for the user to connect to the VPN and re-enter the password for confirmation in the 'Verify password' field
- Remark- A short description of the user account

Authentication Methods

- Select the type(s) of authentication used by the user by selecting the respective checkboxe(s).
- 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 ' in the 'User Configuration' screen to enable the user.

11 Viewing 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
System	☑	Show this log only

□ Select all

Show selected logs

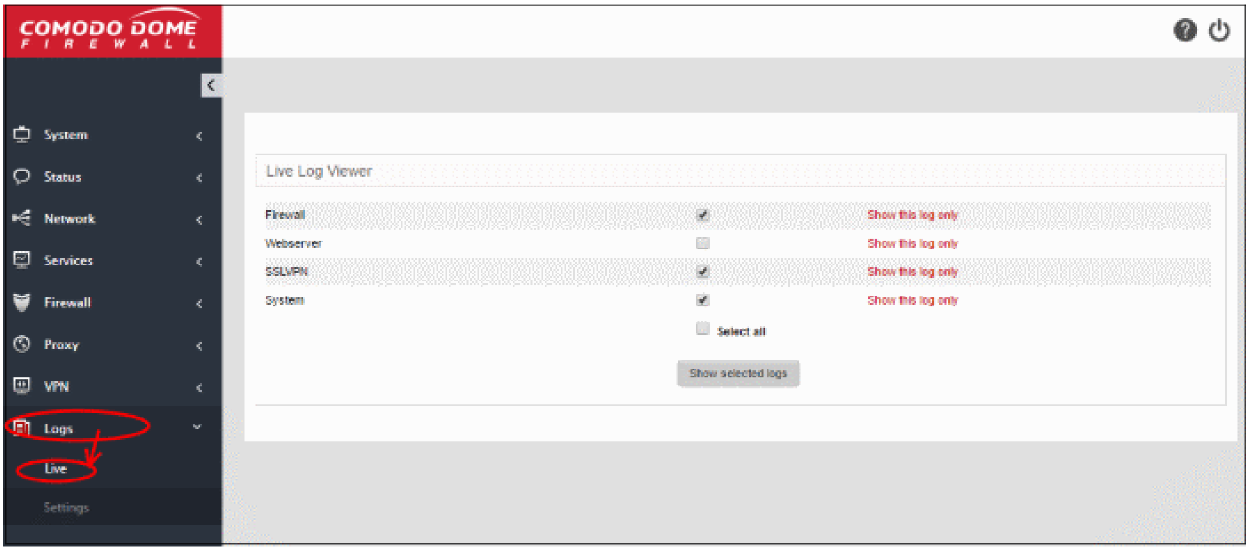
The following sections provide more information on the logs area:

- **Realtime Logs** - Viewing realtime logs of selected features.
- **Configuring Log Settings** - Configure log settings such as view options, remote syslog server, life cycle of log summaries and so on.

11.1 Realtime Logs

Comodo Dome Cloud Firewall can keep realtime logs of events from selected modules. The 'Live Logs' interface displays a list of modules and their current events. Events pertaining to selected modules are displayed in a scrolling window which is updated in real time. The window also allows you to filter logs to view events matching 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
System	☑	Show this log only

□ Select all

Show selected logs

Realtime logs of the following modules are available:

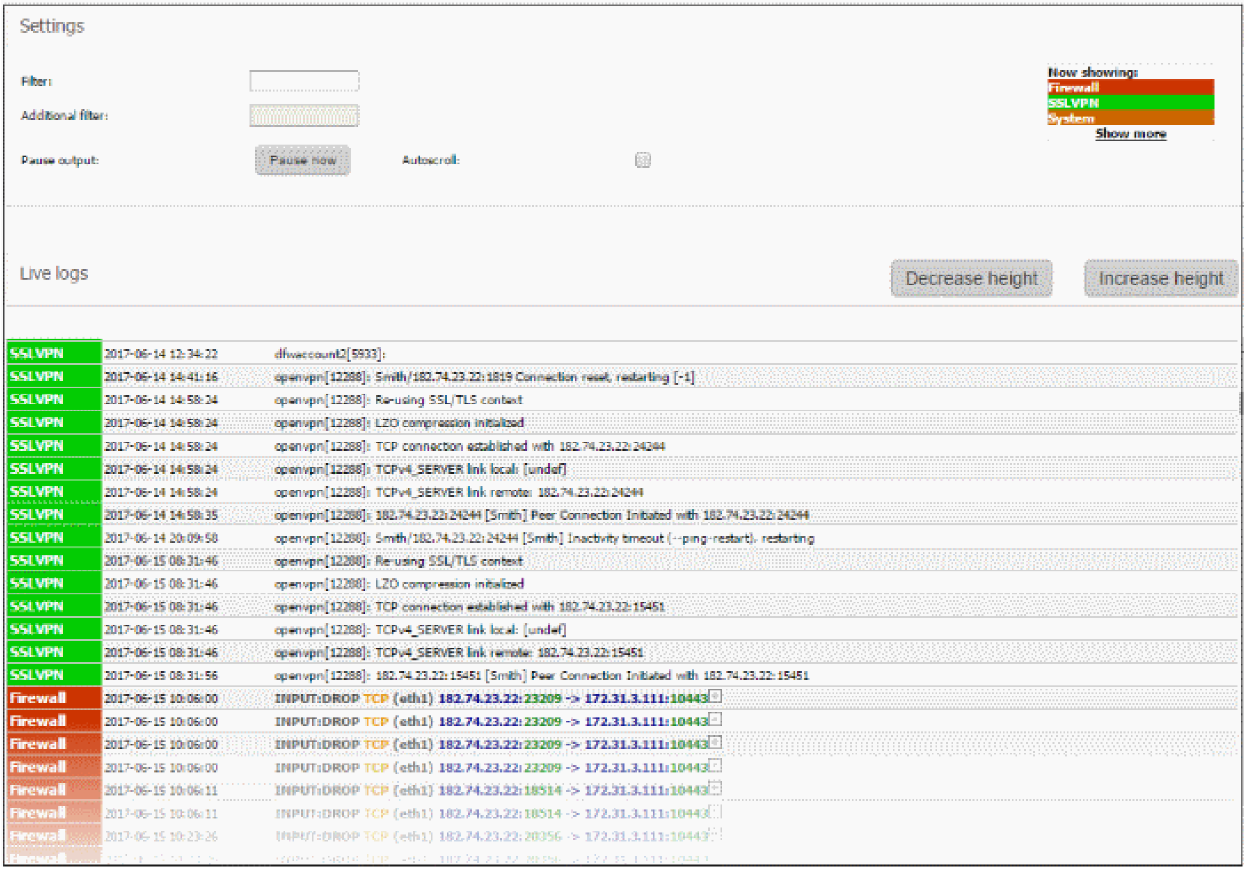
- **Firewall** - Log of connection attempts that were allowed or blocked by the Firewall. Click the '+' button to view details such as IP / Port / MAC address of the source and destination, the connection protocol and more.
- **SSLVPN** - Displays events relevant to SSL VPN connections.
- **System** - Displays events concerning changes in DCF system settings and network configuration.

To view the live logs

- Click 'Logs' > 'Live' on the left-hand menu
- Select the module(s) whose events you want to view.
- Click 'Show selected logs'

Tip: You can add or remove modules in the live log viewer too.

The 'Live Log Viewer' will open in a new browser window.



```
SSLVPN    2017-06-14 12:34:22    dfwaccount2[5933]:
SSLVPN    2017-06-14 14:41:16    openvpn[12288]: Smith/182.74.23.22:1819 Connection reset, restarting [-1]
SSLVPN    2017-06-14 14:58:24    openvpn[12288]: Re-using SSL/TLS context
SSLVPN    2017-06-14 14:58:24    openvpn[12288]: LZO compression initialized
SSLVPN    2017-06-14 14:58:24    openvpn[12288]: TCP connection established with 182.74.23.22:24244
SSLVPN    2017-06-14 14:58:24    openvpn[12288]: TCPv4_SERVER link local: [undef]
SSLVPN    2017-06-14 14:58:24    openvpn[12288]: TCPv4_SERVER link remote: 182.74.23.22:24244
SSLVPN    2017-06-14 14:58:35    openvpn[12288]: 182.74.23.22:24244 [Smith] Peer Connection Initiated with 182.74.23.22:24244
SSLVPN    2017-06-14 20:09:58    openvpn[12288]: Smith/182.74.23.22:24244 [Smith] Inactivity timeout (--ping-restart), restarting
SSLVPN    2017-06-15 08:31:46    openvpn[12288]: Re-using SSL/TLS context
SSLVPN    2017-06-15 08:31:46    openvpn[12288]: LZO compression initialized
SSLVPN    2017-06-15 08:31:46    openvpn[12288]: TCP connection established with 182.74.23.22:15451
SSLVPN    2017-06-15 08:31:46    openvpn[12288]: TCPv4_SERVER link local: [undef]
SSLVPN    2017-06-15 08:31:46    openvpn[12288]: TCPv4_SERVER link remote: 182.74.23.22:15451
SSLVPN    2017-06-15 08:31:56    openvpn[12288]: 182.74.23.22:15451 [Smith] Peer Connection Initiated with 182.74.23.22:15451
Firewall  2017-06-15 10:06:00    INPUT:DROP TCP (eth1) 182.74.23.22:23209 -> 172.31.3.111:10443 +
Firewall  2017-06-15 10:06:00    INPUT:DROP TCP (eth1) 182.74.23.22:23209 -> 172.31.3.111:10443 +
Firewall  2017-06-15 10:06:00    INPUT:DROP TCP (eth1) 182.74.23.22:23209 -> 172.31.3.111:10443 +
Firewall  2017-06-15 10:06:00    INPUT:DROP TCP (eth1) 182.74.23.22:23209 -> 172.31.3.111:10443 +
Firewall  2017-06-15 10:06:11    INPUT:DROP TCP (eth1) 182.74.23.22:18514 -> 172.31.3.111:10443 +
Firewall  2017-06-15 10:06:11    INPUT:DROP TCP (eth1) 182.74.23.22:18514 -> 172.31.3.111:10443 +
Firewall  2017-06-15 10:23:26    INPUT:DROP TCP (eth1) 182.74.23.22:20356 -> 172.31.3.111:10443 +
```

- Click the '+' button at the right end of a log entry to view its details.

The 'Settings' pane of the live log viewer contains the filtering options and controls. The 'Live Logs' pane displays the list of the current events relevant to the selected modules in forward or reverse chronological order and is continuously updated realtime.

Settings

The Settings area contains the options and controls for the following:

- **Selecting Modules for viewing Logs**
- **Filtering the Log Entries**

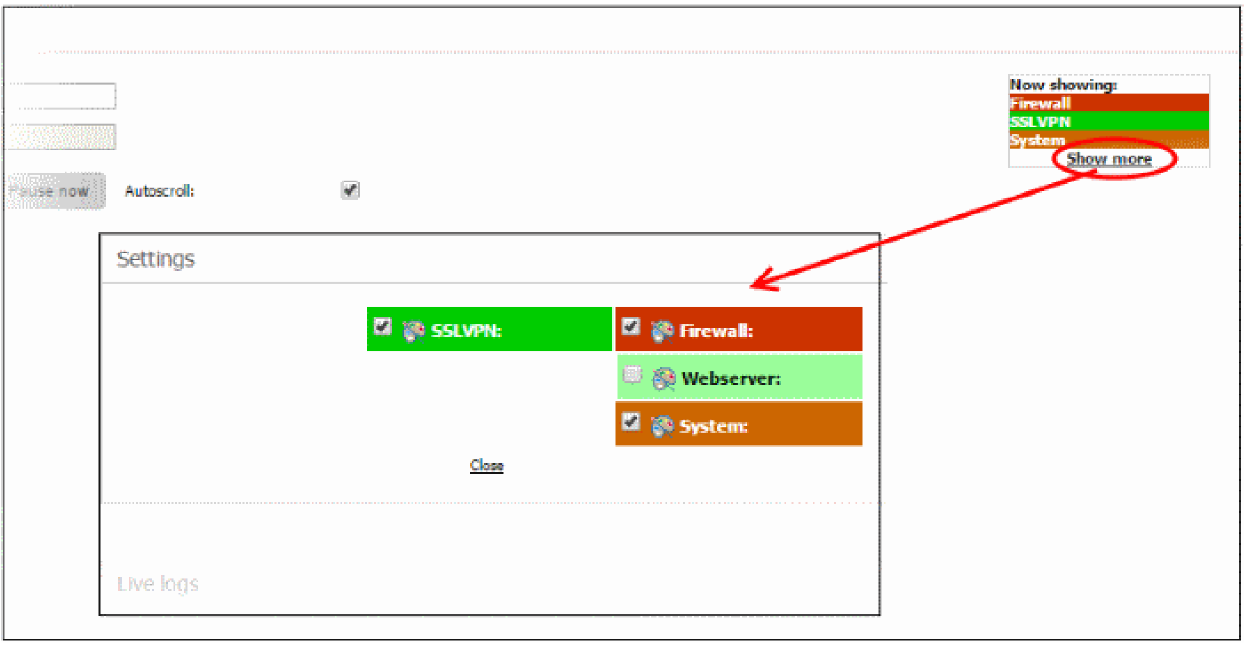
- Pausing and Resuming the log updates
- Autoscrolling the Live Log Viewer

Selecting Modules for viewing Logs

The modules for which the live loges are displayed, are listed at the top right of the settings pane. Each module name is highlighted by a color that indicate the log type. The log entries in the 'Live Logs' pane are highlighted with the respective color of the log type.

To add or remove modules to view the logs

- Click the 'Show More' link at the top right. A list of available modules will be displayed.



- 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.

Filtering the Log Entries

The log entries displayed at the lower pane can be filtered by entering the filter criteria keywords.

To filter the log entries

- Enter the keyword for primary filter in the 'Filter' text field
- Enter the keyword for filtering the results from the primary filter, in the 'Additional filter' text field

The realtime log entries will be filtered and displayed based on the entered filter criteria.

Pausing and Resuming the log updates

By default, the 'Live Logs' viewer is dynamically updated with the current events that are pertinent to the selected modules. The administrator can temporarily stop the updates, for deeper analysis of certain events.

- To pause the updates click the 'Pause now' button.
- To resume updating, click 'Continue' button.

Autoscrolling the Live Log Viewer

The dynamically updated live logs viewer automatically scrolls 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 logs 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

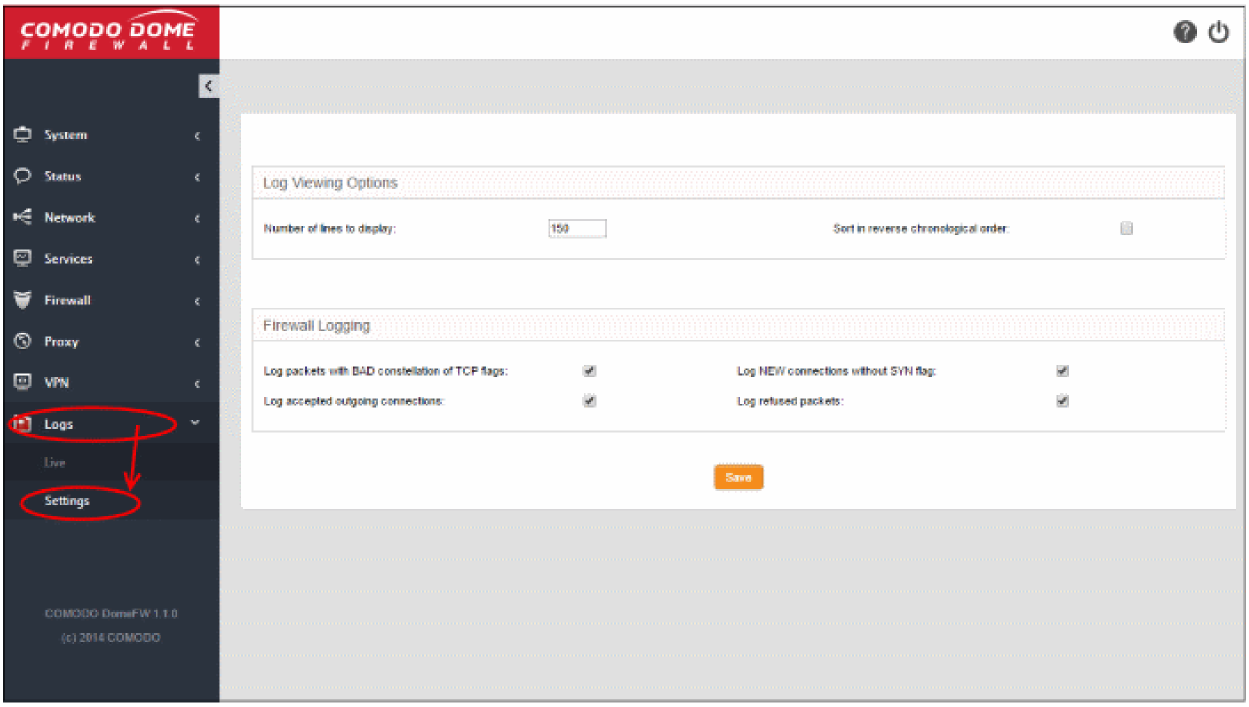
The 'Live Logs' area displays the list of events pertaining to the selected modules and services. Each entry contains the log type, the precise date and time of the event and the message describing the event. The administrator can increase or decrease the height of the live log viewer.

- To view more number of log entries at once, click 'Increase height' repeatedly. The height is increased by two entries for a single click.
- To view less number of log entries, 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: ☐

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 two areas:

- **Log Viewing Options**
- **Firewall Logging**

Log Viewing Options

The 'Log Viewing Options' area allows the administrator to customize the log viewer screens of different DCF 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.

Firewall Logging

The 'Firewall Logging' area allows the administrator to specify 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 Firewall to include packets with all flags set, in the log.
  - Log NEW connections without SYN flag - Instructs 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.

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.

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.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: EnterpriseSolutions@Comodo.com