



Comodo One

Software Version 3.8

Dome Cloud Firewall Quick Start Guide

Guide Version 1.1.021220

Comodo Dome Cloud Firewall – Quick Start

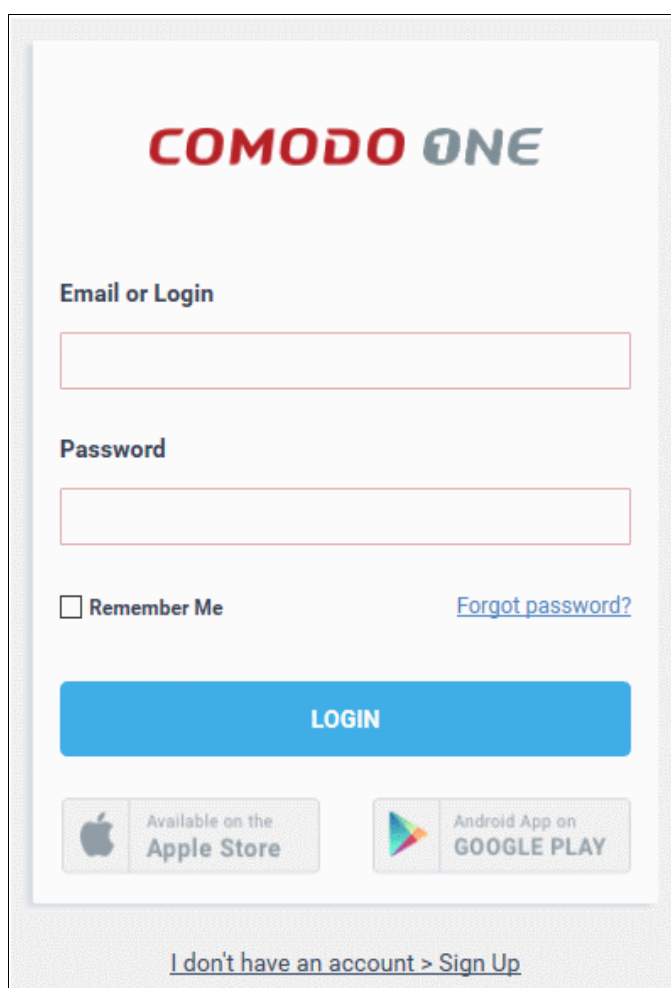
This tutorial explains how to setup Comodo Dome Cloud Firewall (DCF) then add users, connect clients and networks, and create firewall and VPN policies.

The guide will take you through the following processes:

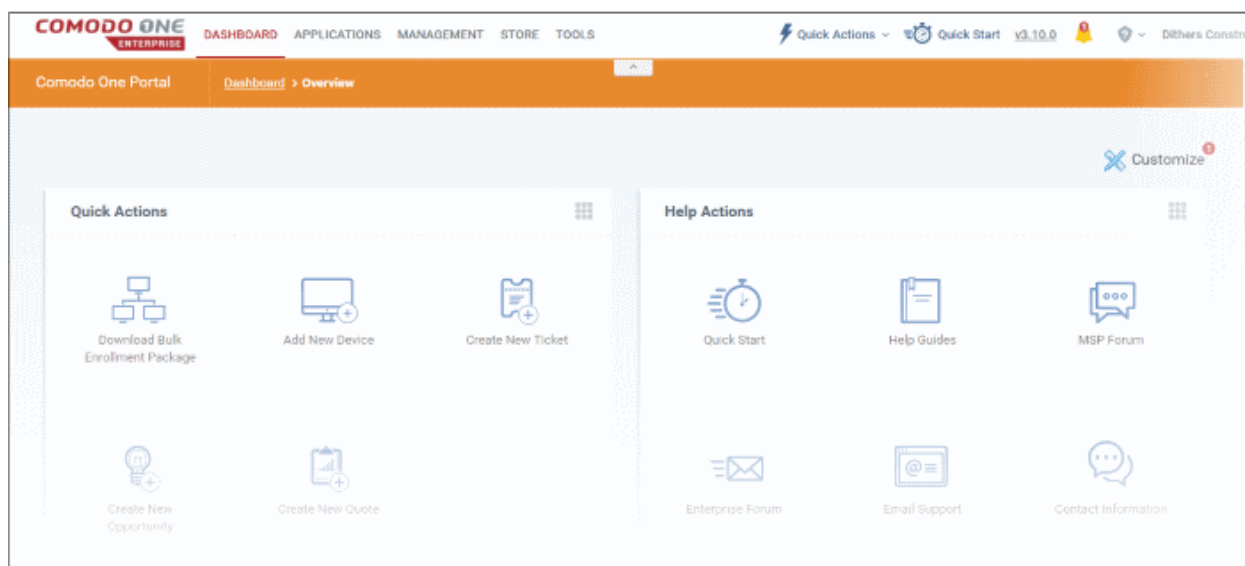
- **Step 1 – Login to Dome Cloud Firewall Module**
- **Step 2 – Configure the Network Interfaces**
- **Step 3 – Configure your Network / Clients to Connect to Dome Cloud Firewall**
- **Step 4 – Configure Firewall Policy**
- **Step 5 – Configure VPN Policy**
- **Step 6 – View Logs**

Step 1 – Login to Dome Cloud Firewall

To access the Dome Cloud Firewall module, first login to C1 at <https://one.comodo.com/app/login>.

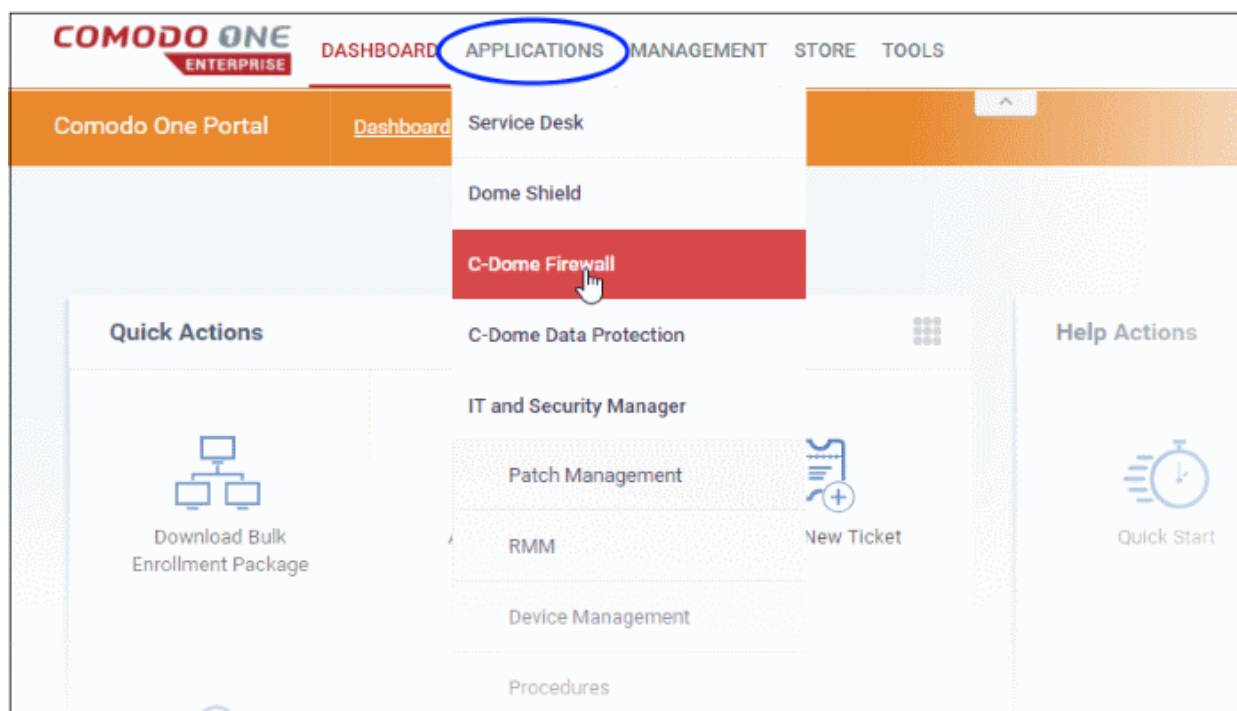


The C1 dashboard will be displayed.



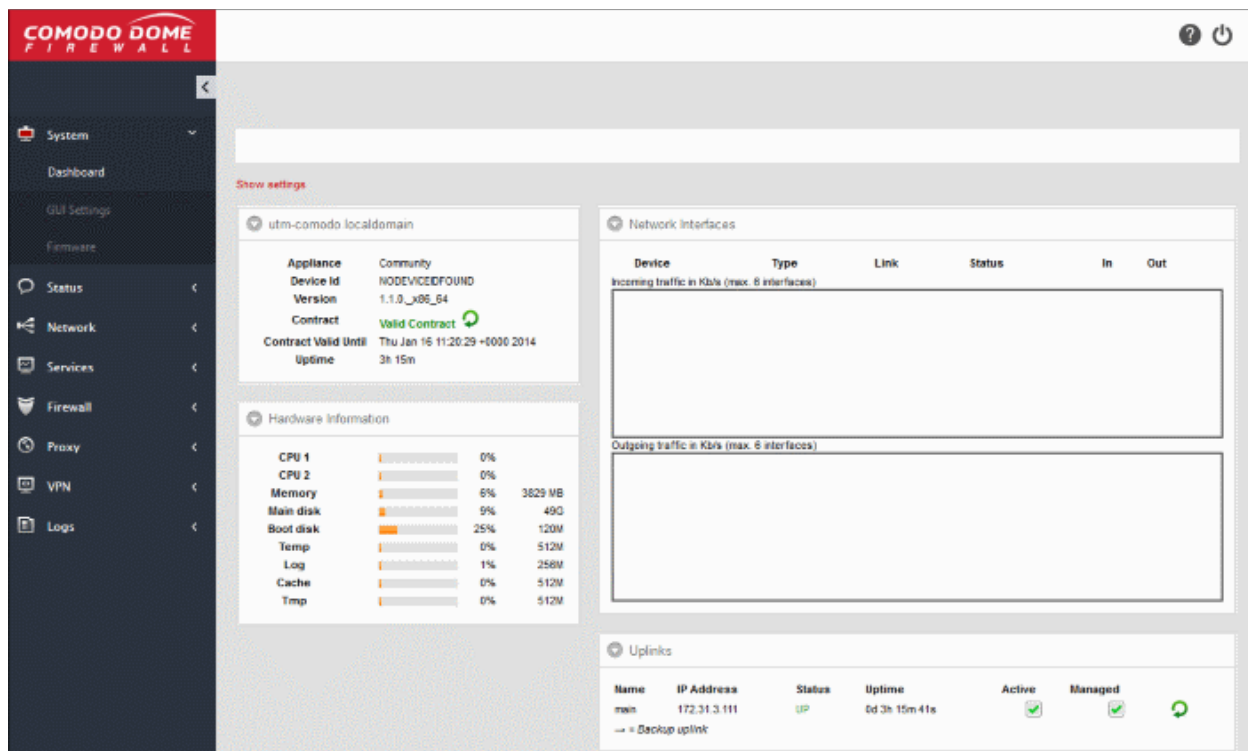
Open the Dome Cloud Firewall module

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

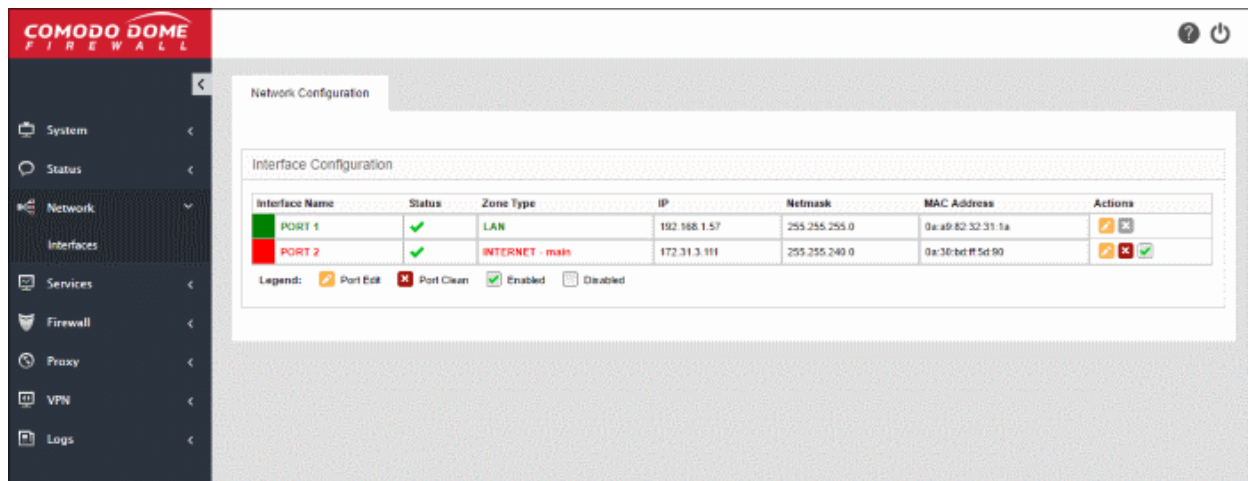


Step 2 – Configure the Network Interfaces

The network interfaces (LAN and Internet) used to connect endpoints to internal and external networks are pre-configured by Comodo.

To configure the network interfaces

- Click 'Network' on the left then 'Interfaces':




You may update the configuration of these interfaces if required. See the following links for more details:

- [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 DNS and advanced settings only.

To update the external network zone

- Click the edit icon  in the row of the interface you wish to update

- 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

Save or Cancel * 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.

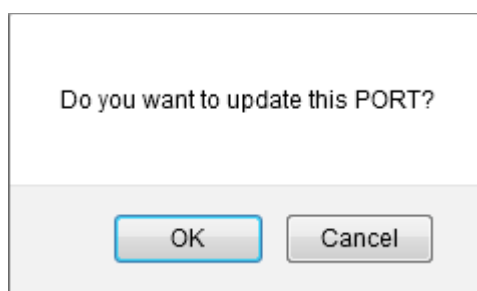
- Select the 'Active' checkbox beside the uplink in the Uplinks box from the Dashboard.
- Start uplink on boot - The uplink will start automatically on every restart of DCF. Deselect this checkbox if you want to manually start the uplink only when required.
- Uplink is managed - The uplink will be managed 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.



- 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 the edit icon  in the row of the interface you wish to update

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: * ulm-comodo Domainname: * localdomain

Save or Cancel * 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:c:a:05:b3:10:5a
 PORT 2	✓	INTERNET			

- 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?


OK Cancel

- 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.

Step 3 – Configure your Network / Clients to Connect to Dome Cloud Firewall

The next 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:

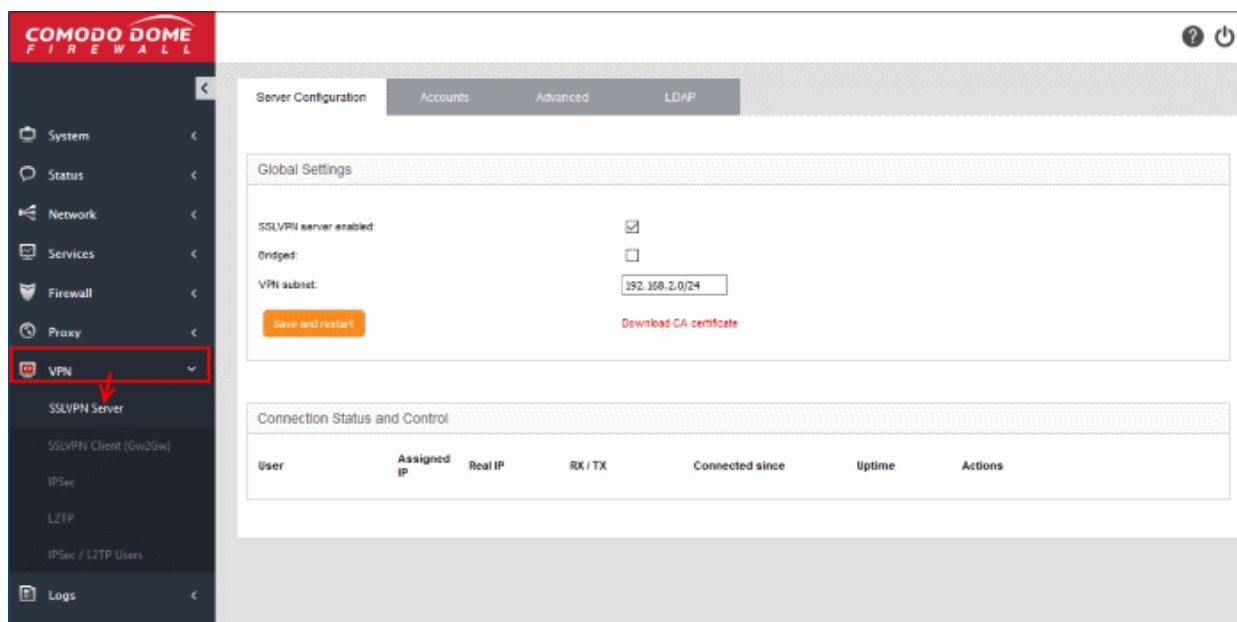
- **Client to Site VPN**
- **Site to Site VPN**

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'



Specify the following information in the server configuration screen:

- **SSLVPN server enabled** - Select to enable SSLVPN server functionality.
- **Bridged** - Select if you wish to run the server in bridged mode.
- **Bridge to** - Choose the local network zone to which the server should be bridged. This option will appear only if you elected to run the server in bridged mode in the previous option.
- **Dynamic IP pool start/end addresses** - Enter the first and last addresses of the IP pool from which addresses are to be dynamically assigned to clients. All traffic from these IP addresses will pass through the VPN firewall, if it is enabled.
- Click 'Save and Restart'. The SSL VPN server service will be restarted to implement your settings.
- 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:



To add a new user account

- Click the 'Add account' button. The 'Add new user' pane will open:

The screenshot shows the 'Add new user' form. It has several sections: 'Account information' with fields for 'Username', 'Password', and 'Verify password'; 'Client routing' with checkboxes for 'Direct all client traffic through the VPN server' and 'Push only global options to this client', and a text area for 'Networks behind client'; 'Push only these networks' with a text area and a note; 'Custom push configuration' with a text area for 'Static IP addresses', checkboxes for 'Push these remote servers' and 'Push domain', and a text area for 'Push domain'. At the bottom left are 'Save' and 'Cancel' buttons. At the bottom right is a note: '*This field is required.'.

Account information

Specify the username and password for the user account. These credentials are to be entered into the client to authenticate 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

Note: You can also add users via an external LDAP server after configuring and synchronizing it with DCF. See '**Configuring LDAP Server Settings**' for more details.

Client routing

Configure the routing traffic for the client

- Direct all client traffic through the VPN server - All incoming and outgoing traffic pertaining to the

client will pass through the VPN server.

- Push only global options to this client - The server will push only those network routes, name servers and domains which are specified in 'Global Push Options' under the 'Advanced' settings.
- Networks behind client - Enter the network subnet address of the VPN gateway server for the client to connect to VPN.
- Push only these networks - Push only the routes of specific networks to the client. Enter the network/subnet addresses of the networks you wish to push. Leave this blank if you wish to push all available networks.

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.

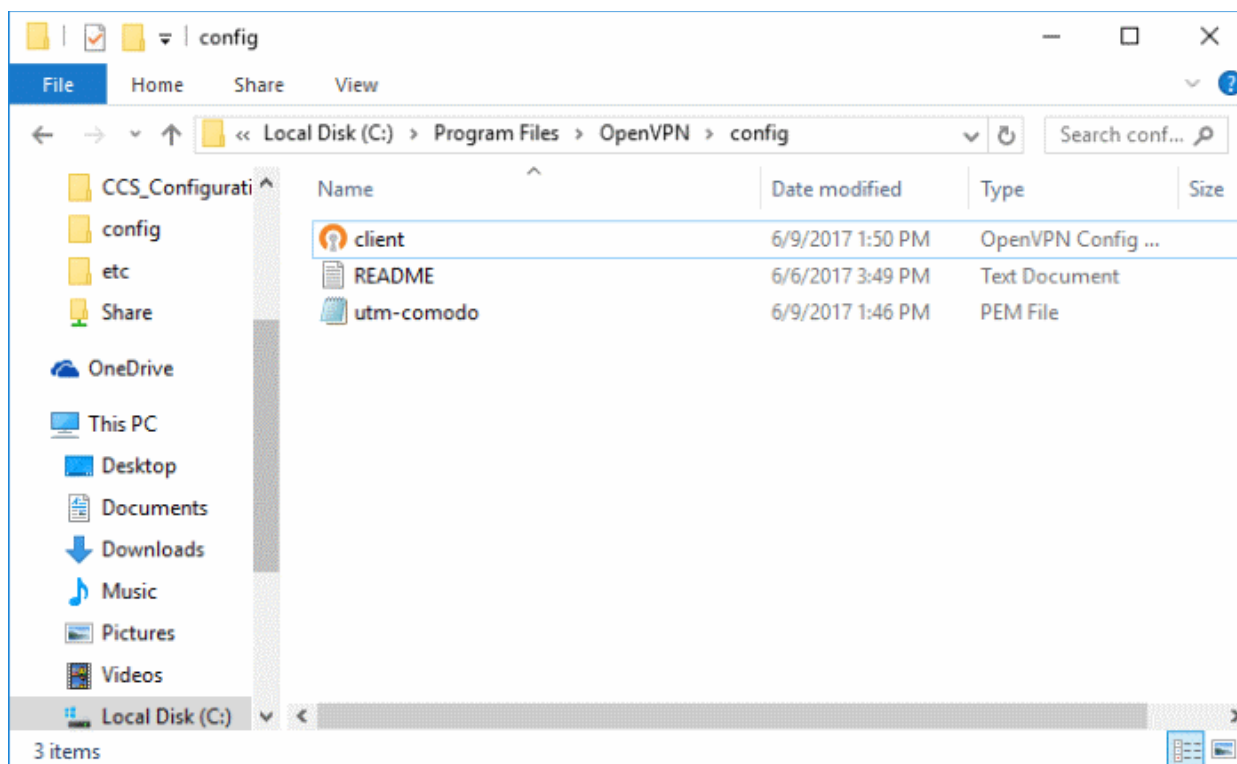
- Click the 'Download CA certificate' link to download the server certificate.
- Click the 'Download Client Configuration' link to download the SSL VPN client configuration file in .ovpn format.

Note: The 'Advanced' section allows you to configure more settings such as port, protocol, authentication and more. See '**Configuring Advanced SSL VPN Server Settings**' for more details.

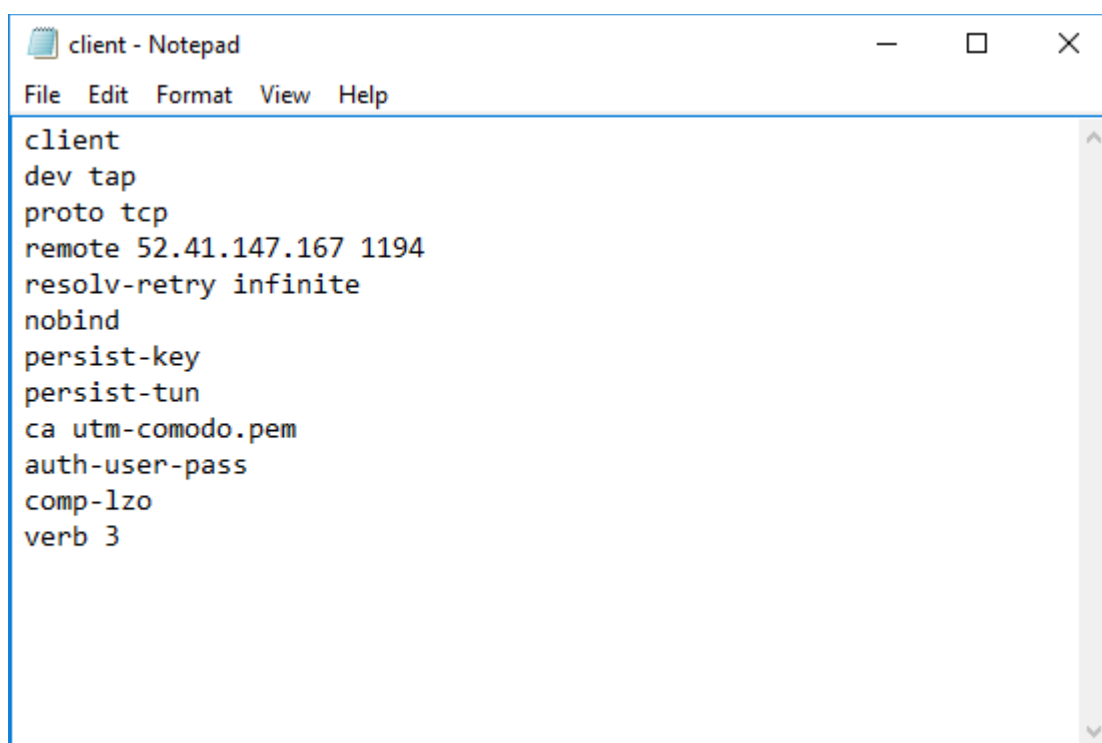
Next, transfer the certificate and the configuration file to the client. In order to connect for the client to connect to Dome Cloud Firewall, download and install openvpn client. You can download the client from

<https://openvpn.net/index.php/open-source/downloads.html>

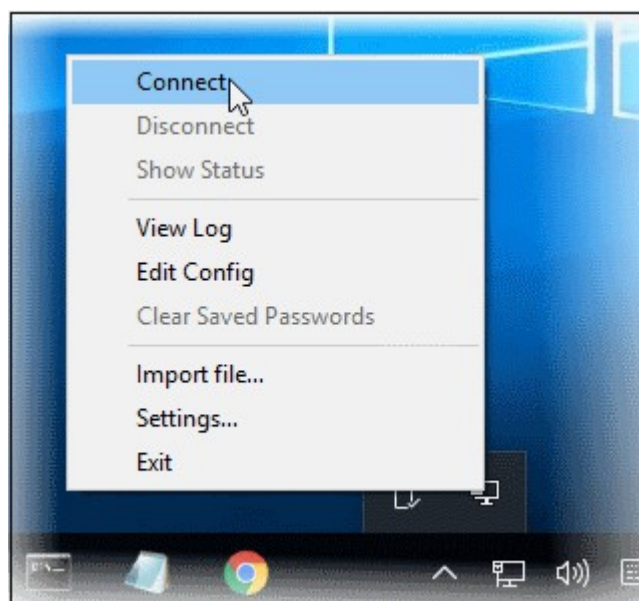
- After installing the OpenVPN GUI client, you need to paste the downloaded CA certificate and configuration file into the OPVN config file. The configuration file will be available in Program Files > OpenVPN > config.



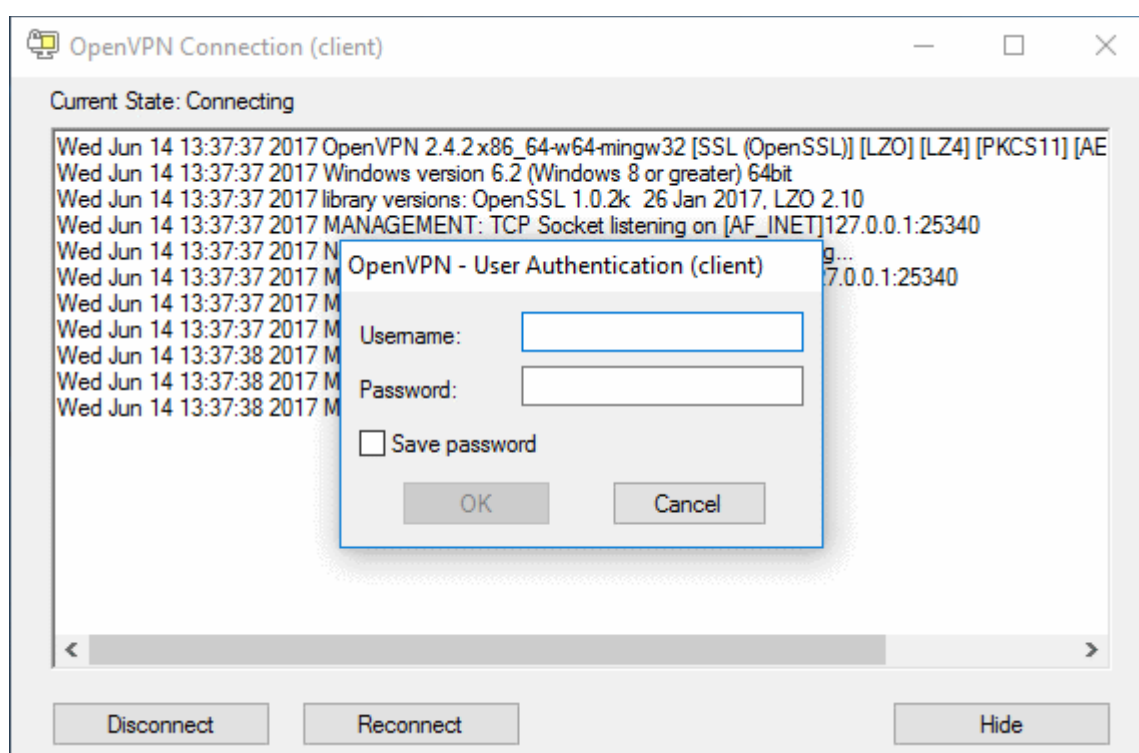
- Open the configuration file and make sure the parameters are as shown below:



- 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.



- 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

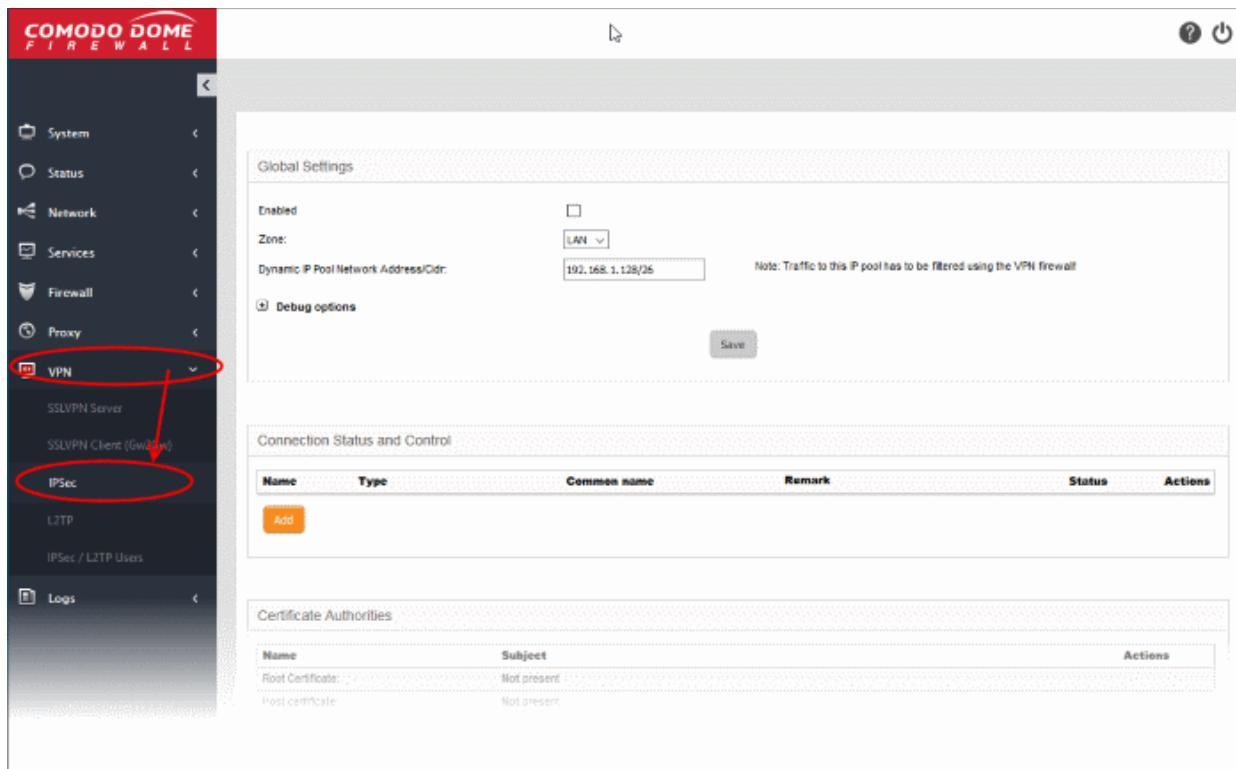
In this method, a network is configured to connect to Dome Cloud Firewall. Once done, all the clients behind the network will be routed via Dome Cloud Firewall but one disadvantage here is any client (roaming device) leaving the office network will not be routed via Dome Cloud Firewall. These roaming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

To configure a network to connect to Dome Cloud Firewall

Enable VPN tunnel at Dome Cloud Firewall

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



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 FW 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 FW 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'

- Click 'Add'

The 'Connection Configuration' interface will be displayed:

- 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 FW.

- 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 FW.

Enable VPN tunnel at your site

In order for the connection to be established between your network and Dome FW, 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 FW
- Configure the authentication method that you selected in Dome FW. 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 techsupport@comodo.com

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

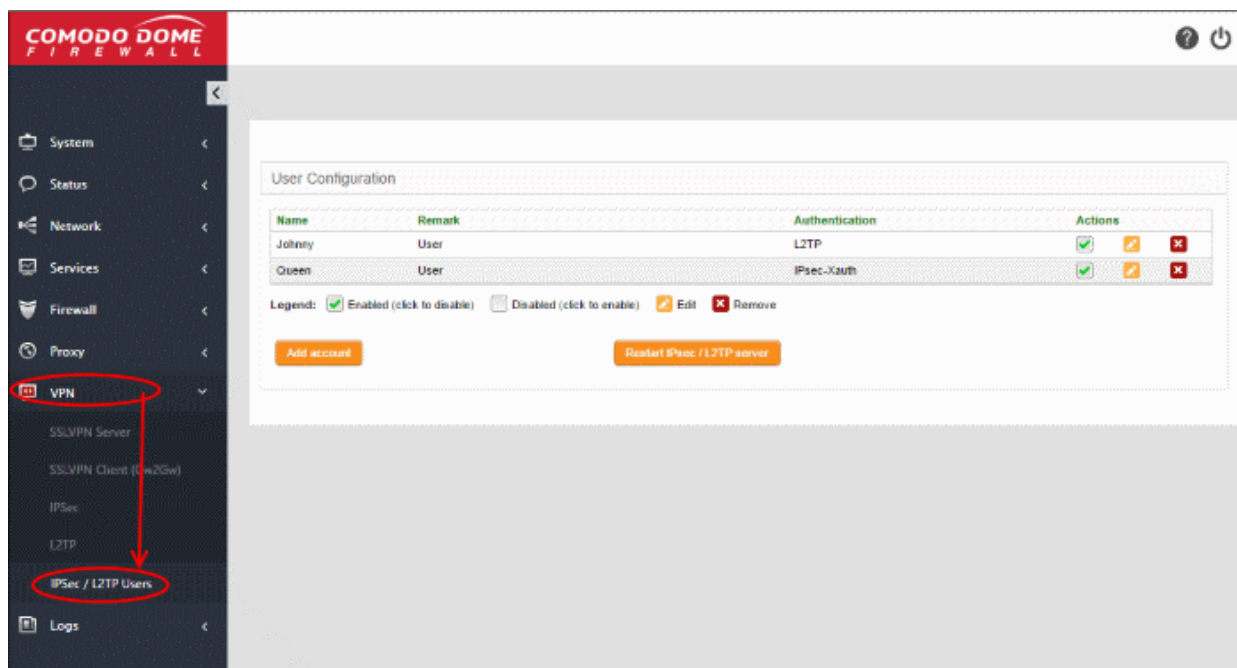
L2TP Service Configuration (optional)

- Once IPSec VPN is configured, you can also allow 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. See '**L2TP Server Configuration**' for more details.

Add IPSec / L2TP Users

The next step is to add IPSec VPN users. 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:



A list of existing user accounts will be displayed.

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	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>
Queen	User	IPsec-Xauth	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>

Legend: ☒ Enabled (click to disable) ☐ Disabled (click to enable)

Add account **Restart IPsec / L2TP server**

Add new user

User Information

Username: *

Password: *

Verify password: *

Remark:

Authentication Methods *

IPsec (Xauth): ☐

IPsec (EAP): ☐

L2TP: ☐

Save or **Cancel** *This Field is required

User Information

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

Authentication Methods

- Select the type(s) of authentication used by the user by selecting the respective checkbox(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.

See '**IPsec / L2TP Users Configuration**' for more details.

Step 4 – Configure Firewall Policy

Before creating a firewall policy, you must first configure firewall objects. Once done, objects can be used in a firewall policy, source network address translation (SNAT), system access rules and a VPN policy. You will be able to **create a new firewall policy** after configuring the following objects:

- **Firewall Addresses**
- **Firewall Groups (optional)**
- **Schedule (optional)**
- **Active Directory (optional)**

Firewall Addresses

The firewall address object can be created in two ways:

- From the 'Add an Address' pane. Define a name for the object and the IP address, IP range or subnet of the host(s) to be included in the object. See [section below](#) for more details.
- By importing users from Active Directory. See '[Active Directory](#)' for more information.

To create a new firewall address object

- Click 'Firewall' > 'Objects' on the left menu and click the 'Firewall Addresses' tab.
- Click 'Add an address' at top left

The screenshot displays the 'Firewall Addresses' management interface. At the top, there are tabs for 'Firewall Addresses', 'Firewall Groups', 'Schedule', and 'Active Directory'. Below the tabs, there is a table of existing addresses. A red circle and arrow highlight the 'Add an address' button in the top left corner. Below the table, there is a form to add a new address. The form includes fields for 'Name', 'Comment', and 'Type'. The 'Type' field has four radio button options: 'Subnet', 'IP Address', 'IP Range', and 'FQDN'. The 'Name' field is marked with an asterisk, indicating it is required. The 'Add' button is orange, and the 'Cancel' button is green. A legend at the bottom shows icons for 'Edit' and 'Remove'.

Name	Address	Type	Comment	Actions
AD_Admin	127.0.0.1	ipaddr	Active Directory Admin	[Edit] [Remove]
HR_Manager	192.168.112.10	ipaddr	HR Manager System	[Edit] [Remove]

Firewall Addresses

Name: *

Comment:

Type: *

Subnet ☐ IP Address ☐ IP Range ☐ FQDN ☐

Add or Cancel

* This field is required.

Legend: [Edit] [Remove]

- Enter the parameters for the new object as shown below:
 - **Name** - 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 category of addresses which will be protected by the object. The 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 as a source or destination address when creating a firewall rule. Simply type the first few letters of the object name to locate it.

Policy Firewall Rule Editor

Incoming Interface: INTERNET +

Source Address: INTERNET +

Outgoing Interface: ma +

Destination Address: HR_Manager Marketing_dept +

Schedule: +

Create

See '[Managing Firewall Address Objects](#)' if you need more help with this.

Firewall Groups (optional)

The firewall object group can be created in two ways:

- From the 'Add a Group' pane. Define a name for the group and the individual objects which will be included in the group. See [section below](#) for more details.
- By importing users from Active Directory. See '[Active Directory](#)' for more information.

To create a new object group

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

Firewall Groups

+ Add a Group

Name	Addresses	Comment	Actions
Home_group	John_external, James_external	Home users	+ -

Firewall Groups

Name: *

Comment:

Addresses: * +

Add or Cancel

* This Field is required.

Legend: + Edit - Remove

- 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 which will be in the group. Separate each name with a comma. Type the first few letters of an object name to view and select matching objects.

Firewall Addresses | Firewall Groups | Schedule | Active Directory

Name: * HR_Mark
Comment: Computers in hr and marketing

Addresses: *
Add or Cancel

Legend: Add Edit Remove

* This Field is required.

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

The group will be available for selection as a source or destination address when creating a firewall rule. Simply type the first few letters of the group name to locate it.

Policy Firewall Rule Editor

Incoming Interface: INTERNET

Source Address: [dropdown]

Outgoing Interface: [dropdown]

Destination Address: [dropdown] (Search: hr, Results: HR_Manager, HR_Mark)

Schedule: [dropdown]

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

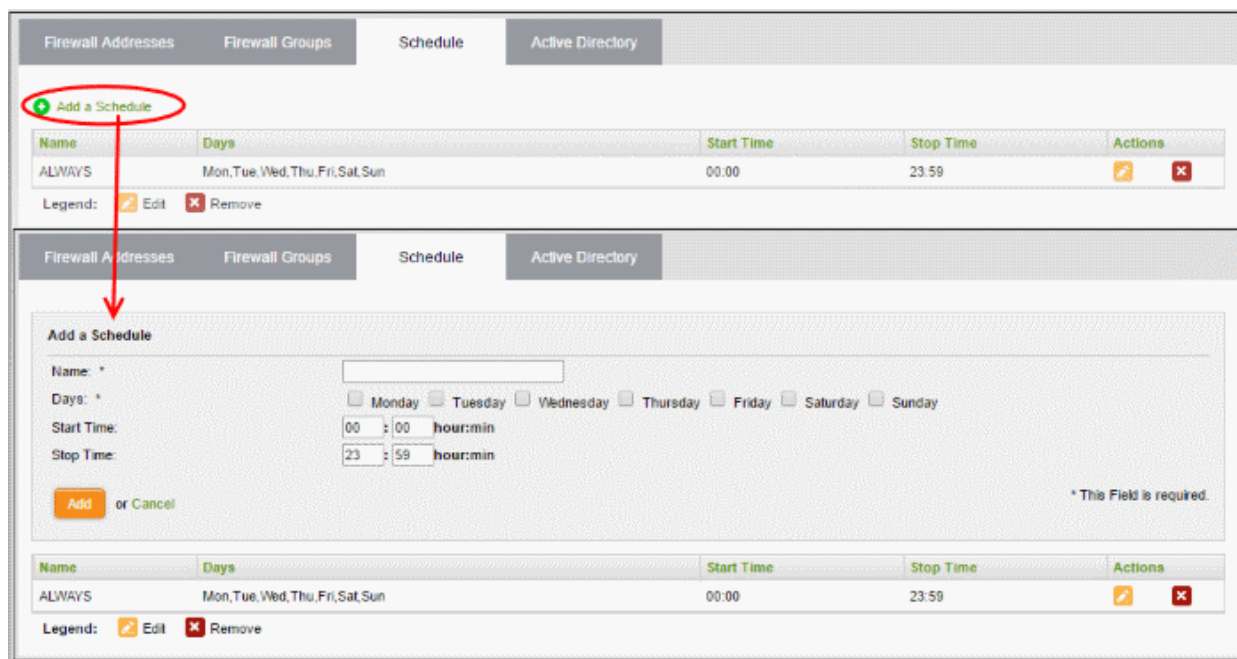
See '[Managing Firewall Object Groups](#)' if you need more help with this.

Schedule (optional)

Scheduling allows you to specify the days and times when a firewall rule should be active. Schedule objects can be added to a rule like other objects.

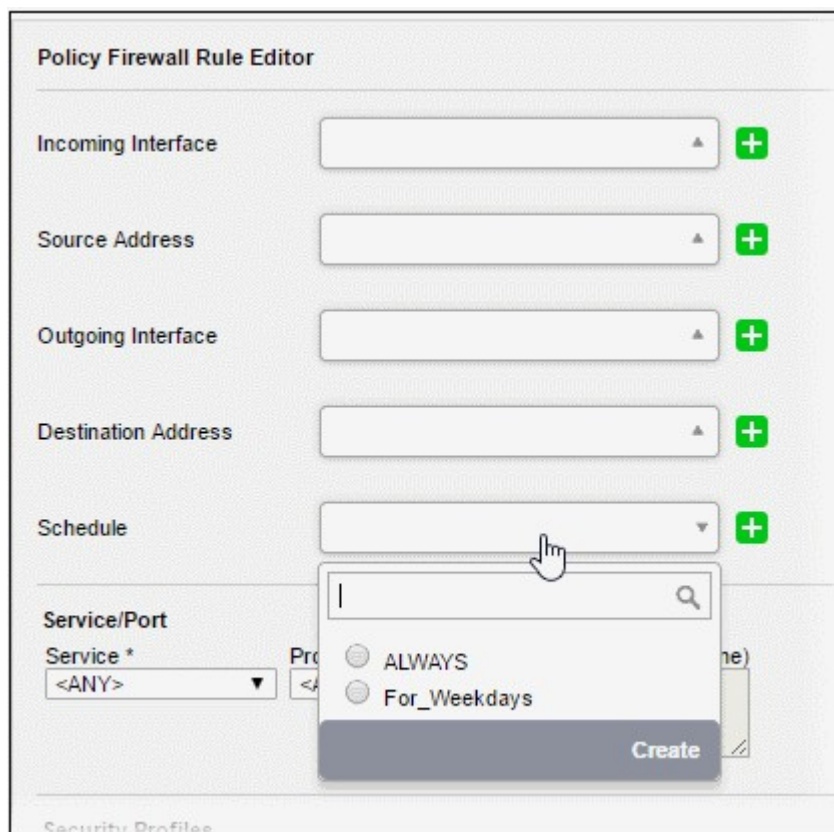
To create a new schedule

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



- 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 firewall rules from the 'Policy Firewall' interface.



See '[Managing Firewall Schedules](#)' if you need more help with this.

Active Directory (optional)

Integrating your Active Directory (AD) server with Dome Cloud Firewall 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.

See '[Active Directory Integration](#)' for details about importing AD to DCF.

Once the AD has been successfully imported into DCF, the LDAP table in the Active Directory interface displays the domains. 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 addresses objects and user groups to firewall object groups from the 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 Addresses'.

Firewall Addresses

Firewall Groups

Schedule

Active Directory

+ Add an address

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'.

Firewall Addresses

Firewall Groups

Schedule

Active Directory

Add a group

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

Once the firewall objects configuration is completed, you can create a firewall policy.

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.

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 can create a new object from this interface too by clicking 'Create' from the drop-down.

- **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 can create a new object from this interface too by clicking 'Create' from the drop-down.

- **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, you can create a new object from this interface too by clicking 'Create' from the drop-down.

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.

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

Configuring the Policy Firewall Settings

The lower 'Policy Firewall Settings' pane allows you to enable/disable the Policy firewall rules and to opt for logging the packets that pass the rule and analysis of HTTPS sites.

- 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.
- 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.

See '[Managing Firewall Configuration](#)' if you need more help with this.

Other firewall rules that can be configured from the firewall section include:

- Source Network Address Translation (SNAT) rules. See '[Source Network Address Translation](#)' for more details.
- Virtual IP rules – See '[Configuring Virtual IP for Destination Network Address Translation](#)' for more details.
- System Access rules – See '[Configuring System Access](#)' for more details.

Step 5 – Configure VPN Policy

VPN firewall rules allow you to set traffic limits for users and hosts who are connected through SSL VPN and IPsec tunnels. The added firewall objects, explained in step 3, will be available for selection while creating a VPN rule.

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.

The screenshot shows the 'VPN Firewall Rule Editor' interface. A red circle highlights the '+ Add a new VPN firewall rule' button in the 'Current Rules' section of the top panel. A red arrow points from this button to the 'VPN firewall rule editor' section in the bottom panel. The editor section contains fields for Incoming Interface, Source Address, Outgoing Interface, Destination Address, and Schedule, each with a green '+' icon. Below these is the 'Service/Port' section with dropdowns for Service and Protocol, and a text area for Destination port. The 'Security Profiles' section includes Action (ALLOW), Remark, Position (First), and checkboxes for Enabled and Log all accepted packets. At the bottom are 'Create Rule' and 'Cancel' buttons, and a legend for rule status.

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 by clicking 'Create' from the drop-down.

- **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 can create a new object from this interface too by clicking 'Create' from the drop-down.

- **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, you can create a new object from this interface too by clicking 'Create' from the drop-down.

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.

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

Configuring the VPN Firewall Settings

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

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

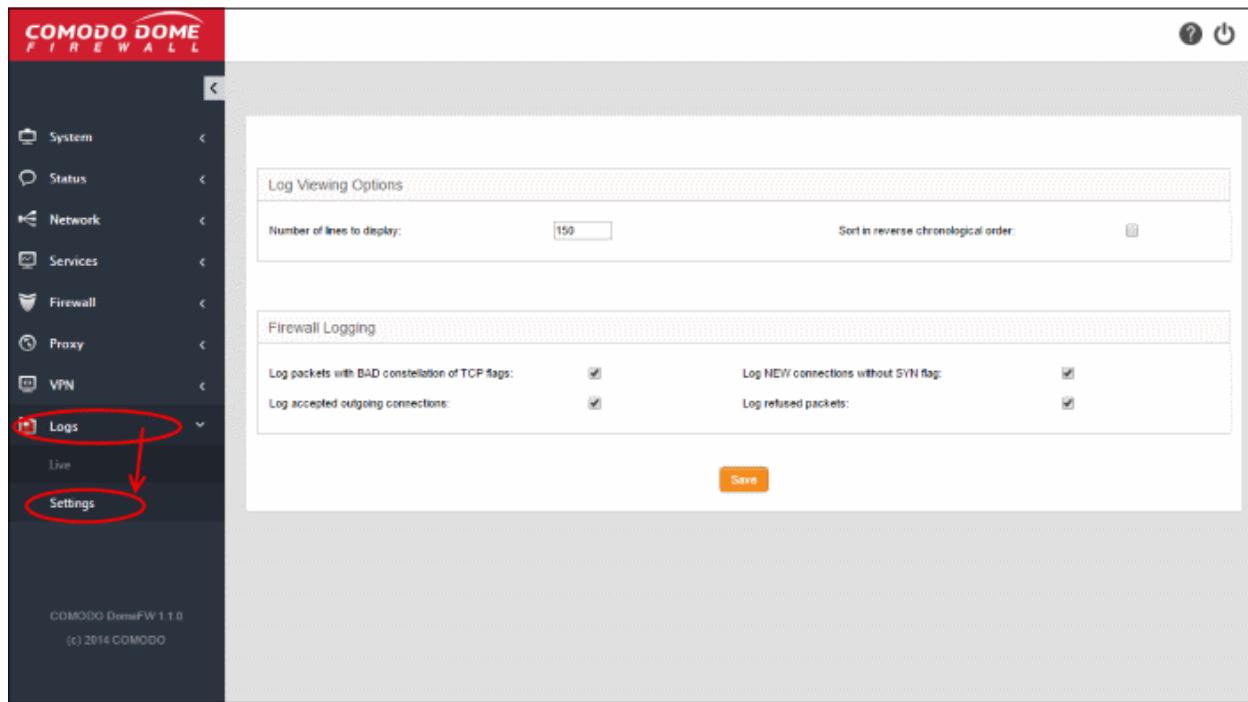
See '[Managing VPN Firewall Rules](#)' for more details.

Step 6 – View Logs

You can view events that are currently taking place across firewall module, SSLVPN module and system to stay informed in real time and troubleshoot problems if any.

First, specify the type of events that should be logged in the log settings interface.

- To open the 'Log Settings' interface, click 'Logs' > 'Settings' on the left menu:



The interface contains two areas:

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

Log Viewing Options

The 'Log Viewing Options' area allows you 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.

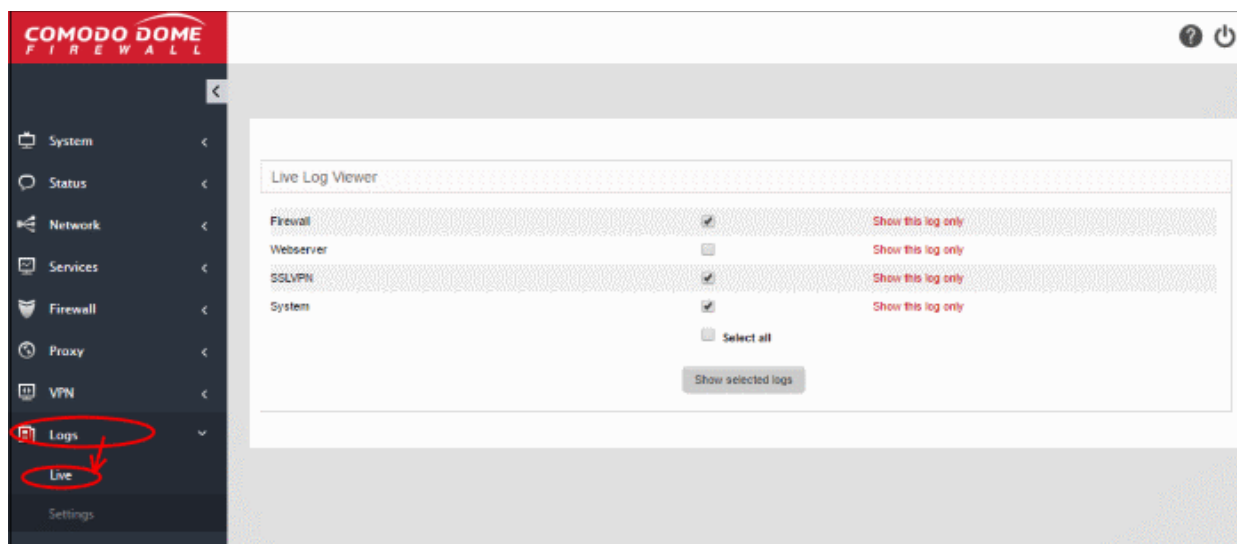
Firewall Logging

The 'Firewall Logging' area allows you 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.

The realtime logs are displayed according to the settings.

- Click 'Logs' > 'Live' to open the 'Live Logs' interface:



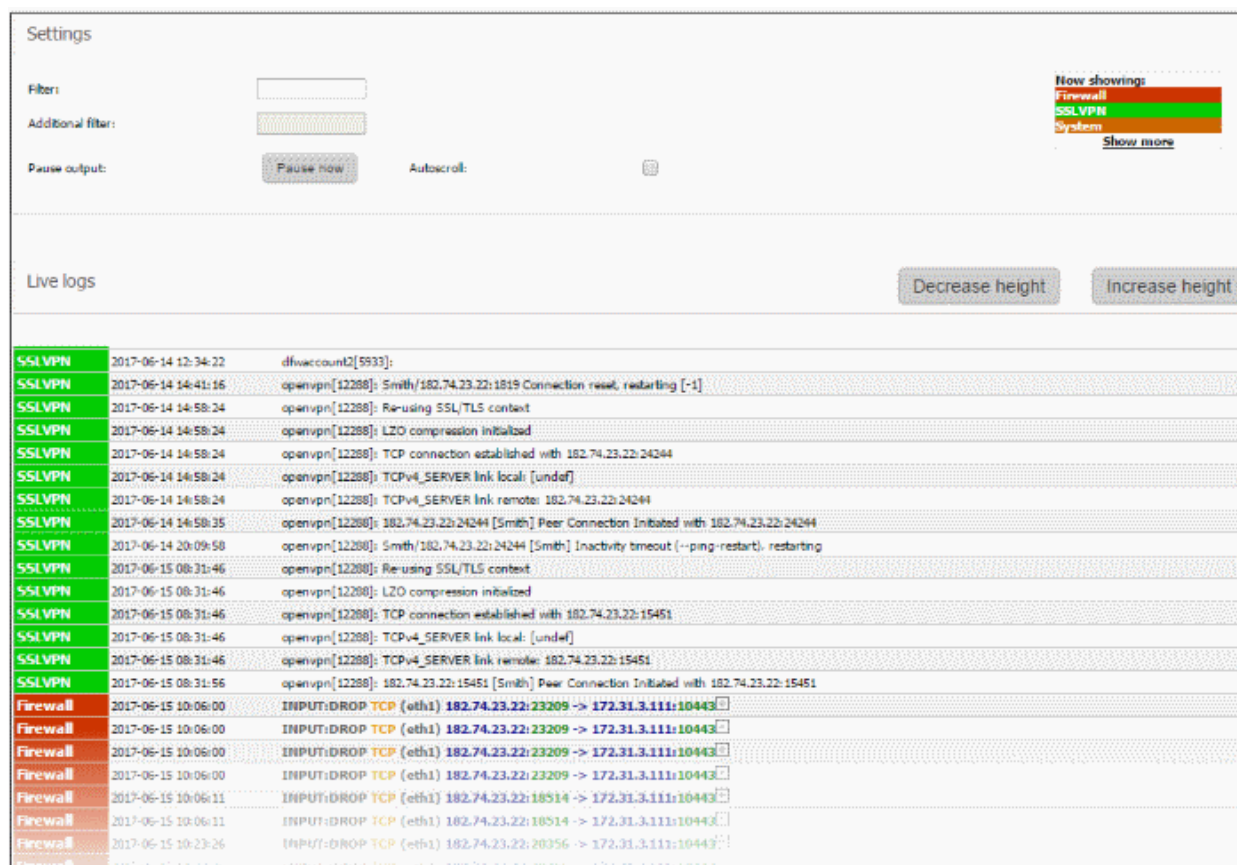
Realtime logs of the following modules are available:

- **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

- Select the module(s) whose events you want to view.
- Click 'Show selected logs'

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



- 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.

See '**Viewing Logs**' for more details.

Click [here](#) to refer to the full Dome Cloud Firewall administrator guide.

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](https://www.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