SOPHOS

Cybersecurity made simple.

XG Firewall

CLI guide

Contents

1 Preface

Welcome to Sophos XG Firewall Command Line Console guide. This guide describes commands that you can use from the command line interface (CLI) to configure and manage your firewall.

The default account to access the CLI is admin. We recommend that you change the default password for this account immediately after you have finished deployment.

2 Accessing Command Line Console

You can access CLI in three ways:

- **Locally with console cable** - Connect your computer directly to the console port of your firewall. For further details see knowledge base article 130693
- **Remotely through network** - Connect your computer through any network interface attached to one of the ports on your firewall.

  If you want to connect using an SSH client, the network interface must have SSH administrative access turned on.

  If you want to connect by accessing the CLI Console in the web admin console, the network interface must have HTTPS administrative access turned on. The CLI console can be accessed from the upper-right hand corner of the screen.

Note
XG Firewall closes idle SSH sessions after 15 minutes.

Navigating the menu

On successful login, the main menu screen is displayed with the following options:

```
       Main Menu

         1. Network Configuration
         2. System Configuration
         3. Route Configuration
         4. Device Console
         5. Device Management
         6. VPN Management
         7. Shutdown/Reboot Device
         0. Exit

         Select Menu Number [0-7]:
```

To access any of the menu items, type the number corresponding to the menu item.

Example: To access **Network Configuration**, press 1.

Related information
Connect to the CLI using a local serial console connection

3 Network configuration

Use this menu for the following settings;

- Configuring and managing interfaces
- Configuring and managing DNS

3.1 Interface configuration

Use this screen to configure interface settings.

Interface menu screens

The following screen displays the current network settings like IPv4 Address/Netmask and/or IPv6 Address/Prefix for all the Ports. In addition, it displays IPv4 Address/Netmask and/or IPv6 Address/Prefix of Aliases, if configured.

```
            Network Settings
                Interface Name      : PortA (Physical)
                Zone Name           : LAN

                IPV4/Netmask        : 172.16.16.16/255.255.255.0 (Static)
                IPV4 Gateway        : N.A.

                Ipv6/Prefix         : Not Configured
                IPV6 Gateway        : N.A.

                Configured Aliases

                No Alias Configured

            Press Enter to continue ......
```

```
            Network Settings
                Interface Name      : PortB (Physical)
                Zone Name           : WAN

                IPV4/Netmask        : 10.10.10.1/255.255.192.0 (Static)
                IPV4 Gateway        : 10.10.10.254 (OK)

                Ipv6/Prefix         : Not Configured
                IPV6 Gateway        : N.A.

                Configured Aliases

                No Alias Configured

            Press Enter to continue ......
```

```
            Network Settings
                Interface Name      : PortC (Physical)
                Zone Name           : DMZ
```

```
               IPV4/Netmask        : 172.16.16.17/255.255.255.255 (Static)
               IPV4 Gateway        : N.A.

               Ipv6/Prefix         : Not Configured
               IPV6 Gateway        : N.A.

               Configured Aliases

               No Alias Configured

            Press Enter to continue ......
```

Note
VLAN and WLAN interfaces are not displayed here.

Set Interface IP Address

This section allows setting or modifying the Interface Configuration for any port. Following screen allows setting or modifying the IPv4 Address for any port. Type y and press Enter to set IP Address.

```
Set IPv4 Address (y/n)  :   No  (Enter) >
```

Displays the IP Address, Netmask and Zone and prompts for the new IP Address and Netmask for each Port.

Press Enter if you do not want to change any details. For example, we are skipping changing the network schema for Port A and B while updating the IP Address and Netmask for Port C, as shown in the image below:

```
               Network configuration of Ethernet PortC

                   Current IP address  :   172.16.16.17
                   New IP address      :   10.10.1.5
                   Current Netmask     :   255.255.255.255
                   New Netmask         :   255.255.255.0
                   Zone                :   DMZ (DMZ)

               Changing IP Address of the device ...... Done.
```

Note

- The network configuration settings described above are applicable to Gateway mode deployment.
- Aliases such as, VLAN, DHCP, PPPoE, WLAN and WWAN settings cannot be configured through the CLI.
- The steps described above are for setting or modifying IPv4 addresses only. The screen elements differ slightly for IPv6 configuration.

3.2 DNS Configuration

Configure and manage DNS

The following screen displays a list of all the IPv4 and IPv6 DNS servers configured in the device:

```
                DNS Configuration

                    Current Ipv4 DNS configuration  :   Static

                        DNS 1 : 10.201.4.51
                        DNS 2 : 10.201.4.59
                        DNS 3 : 4.4.4.4

                    Current Ipv6 DNS Configuration  :   Static

                        DNS 1 : N.A.
                        DNS 2 : N.A.
                        DNS 3 : N.A.

                    Press Enter to continue ......
```

Set DNS IP Address

This section allows setting or modifying the existing DNS configuration. The following screen allows you to set or modify the DNS configuration. Type y and press Enter to set the DNS server IP Address. Press Enter again to skip changing the current DNS configuration.

```
Set IPv4 DNS (y/n)  :   No (Enter) >
```

Press Enter to return to the Main menu.

4 System settings

Use this menu to configure and manage various system settings.

```
            System Settings

                1. Set Password for user Admin
                2. Set System Date
                3. Set Email ID for system notification
                4. Reset Default Web Admin Certificate
                0. Exit

                Select Menu Number [0-4]:
```

4.1 Set password for administrator

Use to change the password of the admin user.

Type the new password, retype for confirmation, and press Enter.

```
            Enter new password:
            Re-Enter new password:
            Password Changed.
```

Displays successful completion message.

Press Enter to return to the System Settings Menu.

4.2 Set system date

Use to change time zone and system date.

Type y to set new time and press Enter.

```
            Current Date:Mon Aug 24 20:33:49 GMT 2019

            Set Date (y/n) : No (Enter) >
```

If an NTP server is configured for synchronizing date and time, a screen with the warning message as shown below will be displayed. If you the set date manually, the NTP server settings is disabled automatically.

```
            Current Date :Mon Aug 24 20:33:49 GMT 2019

            WARNING: NTP is configured. Settings date manually will disable
NTP.

            Set Date (y/n) : No (Enter) >
```

Type: Month, Day, Year, Hour, Minute

```
            Setting New Date :
                Enter Month (01,02....12): 03 (Enter) > 03
                Enter Daye  (01,02....31): 25 (Enter) > 25
                Enter Year  (2000,2001..): 2019 (Enter) > 2019
                Enter Hour  (00,01....23): 17 (Enter) > 18
                Enter Minute  (00,01..59): 59 (Enter) > 00

            New Date : Mon Mar 25 18:00:12 GMT 2019

            Press Enter to continue ......
```

Press Enter to return to the System Settings menu.

4.3 Set email address for system notification

Use to set the Email ID for system notifications. Sophos XG Firewall sends system alert mails on the specified Email ID.

Type the email address you wish to receive system notifications to and press Enter. The new email ID is displayed.

```
            Device will send System Alerts on this email address: >

            Want to change Email Address (y/n : No (Enter) > y

            Enter Administrator Email ID: > john.smith@sophos.com

            Administrator Email ID is changed to: > John.smith@sophos.com
```

Press Enter to return to the System Settings Menu.

4.4 Reset Web admin certificate

Use to reset the web admin certificate back to default.

Sophos XG Firewall is shipped with a default CA certificate which is used to provide secure access (HTTPS) for the web admin console and when block or warning pages are displayed by the web proxy. You can only change the default certificate from the web admin console but can reset it to the default certificate from both web admin console and CLI.

Type y to reset the web admin certificate back to default.

```
            This will reset the web admin console certificate to default
device certificate. Are you sure you
            want to continue? (Y/N): y

            Web admin certificate reset successfully.
```

4.5 Reset secure storage master key

The secure storage master key provides extra protection for the account details stored on XG Firewall. The key encrypts sensitive information, such as passwords, secrets, and keys, preventing unauthorized access.

Once the secure storage master key has been configured, you can reset it using this option on the CLI.

Note
You can't restore backups taken using the old secure storage master key with the new master key.

The secure storage master key can only be reset using the default super administrator account.

To reset the secure storage master key, do as follows:

1. Enter the default admin account password.
2. Enter a new secure storage key.
3. Reenter the new key to confirm.
4. The secure storage master key is reset.

The following image shows the secure storage master key reset process.

```
System Settings


    1.  Set Password for User Admin
    2.  Set System Date
    3.  Set Email ID for system notification
    4.  Reset Default Web Admin Certificate
    5.  Reset secure storage master key
    0.  Exit

Select Menu Number [0-5]: 5
Enter the default admin account password:
****
Enter a new key that satisfies the following requirements:
    -   Minimum 12 characters
    -   An uppercase letter
    -   A lowercase letter
```

```
        -   A number (0-9)
        -   A special character (!#$%&()*+,-./:;<=>?@[]^_`{|}~)
    New secure storage key:
    ************
    To confirm, reenter the new key:
    ************
    Secure storage master key has been reset.
```

5 Route configuration

Use this menu to configure the following routing options:

- Static Routes
- RIP
- OSPF
- Enable/Disable multicast forwarding

Sophos XG Firewall adheres to Cisco terminology for routing configuration and provides a Cisco compliant CLI to configure static routes and dynamic routing protocols.

Traditionally, IP packets are transmitted in one of two ways –Unicast (1 sender – 1 receiver) or Broadcast (1 sender – all devices on the network). Multicast delivers IP packets simultaneously to a specified group of devices on the network.

```
Router Management

    1. Configure Unicast Routing
    2. Configure Multicast Routing
    0. Exit

    Select Menu Number [0-2]:
```

5.1 Configure Unicast Routing

Use this page for configuring RIP, OSPF, and BGP.

```
Unicast Routing Configuration

    1. Configure RIP
    2. Configure OSPF
    3. Configure BGP
    0. Exit

    Select Menu number:
```

Note
The options: Configure RIP, Configure OSPF and Configure BGP are not available when Sophos XG Firewall is deployed in Transparent mode.

5.2 RIP configuration

This option to configure RIP is available only when Sophos XG Firewall is deployed in Gateway mode.

Routing Information Protocol (RIP) is a widely used routing protocol that uses hop count to determine the best route to a destination.

Routing Information Protocol (RIP) is a distance-vector routing protocol intended for small, relatively homogeneous networks. It uses hop count as its routing metric. Each network is usually counted as one hop. The network diameter is limited to 15 hops. Hence, when the hop count becomes 16 network is considered as unreachable and at infinite distance.

Firewall uses RIP protocol to send routing update messages at regular intervals to the next router. Next router updates its routing table and increases the metric value for the path by 1 once it receives changes. The sender of the message is considered as the next hop. Firewall maintains only the route which has the least metric value to a destination.

Firewall implementation of RIP supports:

- RIP version 1 (see RFC 1058)
- RIP version 2 (see RFC 2453)
- Plain text and Message Digest 5 (MD5) authentication

Removing routes

To remove route configuration, execute the no network command followed by the IP address in the command prompt as shown below. Be sure to replace the IP address with the appropriate address for your network.

```
rip(config)#no network 10.10.0.1
```

To exit this screen and return to the menu type exit.

```
rip(config)#exit
```

Disabling RIP

To disable RIP routing configuration, execute the no router command from the command prompt as below:

```
rip(config)#no router rip
```

To exit this screen and return to the menu type exit.

```
rip(config)#exit
```

RIP configuration task list

RIP must be enabled before carrying out any of the RIP commands.

To configure RIP, see RIP configuration steps (page 11)

5.2.1 RIP configuration steps

The steps below describe how to configure RIP in Sophos XG Firewall.

To configure RIP, do as follows:

1. Select **Option 3 (route Configuration) > Option 1 (Configure unicast Routing) > option 1 (Configure RIP)**. You then see the following prompt:

```
rip>
```

2. Type `enable`.

   Enables RIP routing process and places you in Global Configuration mode.

3. Specify a list of networks for the RIP routing process. This requires a series of commands:

   Note
   During initial setup these commands will need to be entered sequentially.

Option	Description
`configure terminal`	Enables RIP configuration mode which places you in the router configuration mode and allows you to configure RIP from the terminal.
`router rip`	Allows you to configure and start the RIP routing process.
`network` ip-address/subnet mask	Specify IP address and subnet information For example, if the network for 10.0.0.0/24 is RIP enabled, this results in all the addresses from 10.0.0.0 to 10.0.0.255 being enabled for RIP. Enables RIP interfaces between specified network address. RIP routing updates are sent and received only through interfaces on this network. Also, if the network of an interface is not specified, the interface isn't advertised in any RIP update. The interfaces which have addresses matching with network are enabled.
`end`	Exits from the Router Configuration mode and places you into the Enable mode.

4. To configure authentication, do as follows:

   Note
   During initial setup these commands will need to be entered sequentially.

Option	Description
`rip#configure terminal`	Enables RIP configuration mode which places you in router configuration mode and allows you to configure from the terminal.
`rip(config)#interface ifname`	Select the interface on which you wish to configure authentication.

Option	Description

`rip(config-if)#ip rip authentication mode{text[ string]}`	To set authentication mode as text and set the authentication string. Defines authentication mode for each interface. By default, authentication is enabled for all interfaces. If authentication is not required for any of the interfaces, you should disable it.
	RIP Version 1 doesn't support authentication. RIP Version 2 supports Clear Text (simple password) or Keyed Message Digest 5 (MD5) authentication.
	To enable authentication for RIP Version 2 packets and to specify the set of keys that can be used on an interface, use the IP RIP authentication key-chain command in interface configuration mode. If authentication isn't required for any of the interfaces, use the no form of this command.
	Example:
	`rip(config)#interface A`
	`rip(config-if)#ip rip authentication modetext`
	`rip(config-if)#ip rip authentication stringteststring`

`rip(config)#interface ifname`	See description above.

`rip(config-if)#ip rip authentication mode {md5[Key-chain name of key-chain]}`	To set authentication mode as MD5 and set the authentication string.
	Example:
	`rip(config)#interface A`
	`rip(config-if)#ip rip authentication modemd5key-chain testkeychain`

`rip(config)#interface ifname`	See description above.

`rip(config-if)#no ip rip authentication mode`	Disables authentication
	Example:
	`rip(config)#interface A`
	`rip(config-if)#no ip rip authentication mode`

`rip(config-if)#end`	Exits from router configuration mode and places you into enable mode.

5. Exit to the router management menu.

```
rip(config-if)#exit
```

5.3 OSPF configuration

The option to configure OSPF is available only when Sophos XG Firewall is deployed in Gateway mode.

OSPF (Open Shortest Path First) is one of the IGPs (Interior Gateway Protocols). Compared with RIP (Routing Information Protocol), OSPF can serve many more networks and the period of convergence is very short. OSPF is widely used in large networks such as ISP backbone and enterprise networks.

The Sophos XG Firewall implementation of OSPF supports:

- OSPF version 2 (as described in RFC 2328)
- Plain text and Message Digest 5 (MD5) authentication

How OSPF works

OSPF keeps track of a complete topological database of all connections in the local network. It is typically divided into logical areas linked by area border routers. An area comprises a group of contiguous networks. An area border router links one or more areas to the OSPF network backbone.

Sophos XG Firewall participates in OSPF communications, when it has an interface in the same area. Sophos XG Firewall uses the OSPF Hello protocol to acquire neighbors in an area. A neighbor is any router that has an interface to the same area as the Sophos XG Firewall. After initial contact, the Sophos XG Firewall exchanges Hello packets with its OSPF neighbors at regular intervals to confirm that the neighbors can be reached.

OSPF-enabled routers generate link-state advertisements and send them to their neighbors whenever the status of a neighbor changes or a new neighbor comes online. If the OSPF the network is stable, link-state advertisements between OSPF neighbors do not occur. A Link-State Advertisement (LSA) identifies the interfaces of all OSPF-enabled routers in an area, and provides information that enables OSPF-enabled routers to select the shortest path to a destination. All LSA exchanges between OSPF-enabled routers are authenticated. The Sophos XG Firewall maintains a database of link-state information based on the advertisements that it receives from OSPF-enabled routers. To calculate the shortest path to a destination, the Sophos XG Firewall applies the Shortest Path First (SPF) algorithm to the accumulated link-state information.

The Sophos XG Firewall updates its routing table dynamically based on the results of the SPF calculation to ensure that an OSPF packet will be routed using the shortest path to its destination.

Removing routes

To remove route configuration, execute the `no network` command from the command prompt as shown below:

```
ospf(config-router)#no network ip address area area-id
```

Turning off OSPF

To turn off OSPF routing configuration, execute the `no router` command from the command prompt as shown below:

```
ospf(config)#no router ospf
```

OSPF configuration task list

OSPF must be turned on before you carry out any of the OSPF commands.

To configure OSPF, see OSPF configuration steps (page 15)

5.3.1 OSPF configuration steps

The steps below describe how to configure OSPF in Sophos XG Firewall

To configure OSPF, do as follows:

1. Select **Option 3 (Route Configuration) > Option 1 (Configure Unicast Routing) > Option 2 (Configure OSPF)**. You then see the following prompt:

   ```
   OSPF>
   ```
2. Type `enable`.

   This enables OSPF routing process and places you in Global Configuration mode.
3. Specify a list of networks for the OSPF routing process

Option	Description
`ospf#configure terminal`	Enables OSPF configuration mode which places you in router configuration mode and allows you to configure OSPF from the terminal.
`ospf(config)#router ospf`	Allows you to configure and start the OSPF routing process.
`ospf(config-router)#network ip-addressareaarea-id`	Specify ip-address with the subnet information Assigns an interface to an area. The area ID is the area number the interface should be in. The area ID can be an integer from 0 to 4294967295 or can take a form similar to an IP address A.B.C.D. Interfaces that are part of the network are advertised in OSPF link state advertisements.
`ospf(config - router)# show running - config`	View the current OSPF configuration.
`ospf(config-router)#end`	Exits from router configuration mode and places you into enable mode.

Option	Description
`ospf(config - if)#exit`	Exits to the router management menu.

5.4 BGP configuration

The option to configure BGP is only available when Sophos XG Firewall is deployed in Gateway mode.

Border Gateway Protocol (BGP) is a path vector protocol that is used to carry routing information between routers that are in different administrative domains (Autonomous Systems). Example: BGP is typically used by ISPs to exchange routing information between different ISP networks.

The Sophos XG Firewall implementation of BGP supports:

- Version 4 (RFC 1771)
- Communities Attribute (RFC 1997)
- Route Reflection (RFC 2796)
- Multiprotocol extensions (RFC 2858)
- Capabilities Advertisement (RFC 2842)

Additionally, a firewall rule needs to be configured for the zone for which the BGP traffic is to be allowed. Example: LAN to LOCAL or WAN to LOCAL.

How BGP works

When BGP is enabled, the Sophos XG Firewall advertises routing table updates to neighboring autonomous systems whenever any part of the Sophos XG Firewall routing table changes. Each AS, including the local AS of which the Sophos XG Firewall device is a member, is associated with an AS number. The AS number references a specific destination network.

BGP updates advertise the best path to a destination network. When the XG Firewall unit receives a BGP update, the XG Firewall examines potential routes to determine the best path to a destination network and records the path in the XG Firewall routing table.

Removing routes

To remove route configuration, execute the `no network` command from the command prompt as shown below:

```
bgp(config-router)#no network ipaddress
```

Turning off BGP

To turn off BGP routing configuration, execute the `no router` command from the command prompt as shown below:

```
bgp(config)#no router bgpAS number
```

BGP configuration task list

BGP must be turned on before carrying out any of the BGP commands.

To configure BGP please see BGP configuration steps (page 17)

5.4.1 BGP configuration steps

BGP configuration steps in Sophos XG Firewall

To configure BGP, do as follows:

1. Select **Option 3 (Route Configuration) > Option 1 (Configure Unicast Routing) > Option 3 (Configure BGP)**

   You see the following prompt:

   ```
   bgp>
   ```

2. Type `enable`

   This turns on the BGP routing process and places you in Global Configuration mode.

3. Specify a list of networks for the BGP routing process.

Option	Description
`bgp#configure terminal`	Enables the BGP configuration mode which places you in the Router Configuration mode and allows you to configure from the terminal.
`bgp(config)#router bgp AS number`	Allows you to configure and start BGP routing process. AS (Autonomous System) number is the number of the local AS that Sophos XG Firewall unit is a member of.
`bgp(config-router)#network ip-address`	Specify the `ip-address` with the subnet information of the network to be advertised. IP Addresses and network masks or prefixes of networks to advertise to BGP peers. Sophos XG Firewall may have a physical or VLAN interface connected to those networks.
`bgp(config - router)#show running - config`	Shows the configuration. By default, the router ID is the IP address of the XG Firewall. The router ID is used to identify the XG Firewall to other BGP routers. The router ID can be an integer or can take a form similar to an IP address A.B.C.D.
`bgp(config-router)#end`	Exits from the router configuration mode and places you into the enable mode.
`bgp#exit`	Exits to the router management menu.

5.5 Multicast routing

This page provides details about multicast routing.

This section covers the following topics:

- Enable/Disable multicast forwarding
- Configure static multicast routes
- Viewing routes
- Removing Routes

To reach the configuration menu from the main menu select: **Option 3 (Route Configuration) > Option 2 (Configure Multicast Routing)**

You will then be presented with the below screen:

```
Multicast Routing Configuration

                    1. Enable/Disable Multicast forwarding
                    2. Configure static-routes
                    3. Exit

                    Select Menu Number:
```

IP Multicast

Internet Protocol (IP) multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of recipients and homes. IP multicast delivers source traffic to multiple receivers without adding any additional burden on the source or the receivers.

Applications like videoconferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news use IP multicasting.

If IP multicast is not used, a source is required to send more than one copy of a packet or an individual copy to each receiver. In such case, high-bandwidth applications like Video or Stock where data is sent more frequently and simultaneously, use a large portion of the available bandwidth. In these applications, the only efficient way of sending information to more than one receiver simultaneously is by using IP multicast.

Multicast Group

Multicast is based on the concept of a group. An arbitrary group of receivers express an interest in receiving a specific data stream. This group does not have any physical or geographical boundaries. The hosts can be located anywhere on the Internet. Hosts that are interested in receiving data flow to a specific group must join the group. Hosts must be a member of the group to receive the data stream.

IP Multicast Addresses

Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to this group.

IP Class D Addresses

The Internet Assigned Numbers Authority (IANA) controls the assignment of IP multicast addresses. Multicast addresses fall in Class D address space ranging from 224.0.0.0 to 239.255.255.255.

This address range is only for the group address or destination address of IP multicast traffic. The source address for multicast datagrams is always the unicast source address.

Multicast Forwarding

In multicast routing, the source is sending traffic to a group of hosts represented by a multicast group address. The multicast router must determine which direction is upstream (towards the source) and which direction (or directions) is downstream. If there are multiple downstream paths, the router replicates the packet and forwards the traffic down the appropriate downstream paths. This is not necessarily all paths.

Turn on or turn off Multicast forwarding

With multicast forwarding, a router forwards multicast traffic to networks where other multicast devices are listening. Multicast forwarding prevents the forwarding of multicast traffic to networks where there are no nodes listening.

For multicast forwarding to work across inter-networks, nodes and routers must be multicast capable.

A multicast capable node must be able to:

- Send and receive multicast packets.
- Register the multicast addresses being listened to by the node with local routers, so that multicast packets can be forwarded to the network of the node.

IP multicasting applications that send multicast traffic must construct IP packets with the appropriate IP multicast address as the destination IP Address. IP multicasting applications that receive multicast traffic must inform the TCP/ IP protocol that they are listening for all traffic to a specified IP multicast address.

Setting up IP Multicast forwarding

Configuring multicast forwarding is two-step process:

- Enable multicast forwarding (both the modes)
- Configure multicast routes (only in Gateway mode)

To enable multicast forwarding, select: **Option 3 (Route Configuration) > option 2 (Configure Multicast Routing) > option 1 (enable/Disable Multicast Forwarding)**

and execute the following command:

```
enable multicast-forwarding
```

5.5.1 Configure Multicast Routing

This page provides details about configuration of multicast routing.

Use the steps below to configure multicast routing.

Multicast routes can't be added before enabling multicast forwarding.

Configure static multicast routes

1. Select: **option 3 (Route configuration) > option 2 (Configure Multicast Routing) > option 2 (Configure Static-routes)** and execute the following command

   ```
   console> mroute add input-interface port portnumber source-ip
   sourceipaddress dest-ip destinationipaddress output-interface port
   portnumber
   ```

   The parameters and their meanings are shown in the table.

Option	Description
`input-interface`	Interface from which multicast traffic is supposed to arrive (interface that leads to the source of multicast traffic). This is the port through which traffic arrives.
`source-ip`	Unicast IP address of source transmitting multicast traffic.
`destination-ip`	Class D IP address (224.0.0.0 to 239.255.255.255).
`output-interface`	Interface on which you want to forward the multicast traffic (interface that leads to the destination of multicast traffic). This is the port through which traffic exits the XG Firewall.

   Example:

   ```
   console> mroute add input-interface PortA source-ip 1.1.1.1 dest-ip
    230.1.1.2 output-interface PortB
   ```

   Sophos XG Firewall forwards multicast traffic received on interface PortA from IP address 1.1.1.1 to 230.1.1.2 through interface PortB.

   If you want to inject multicast traffic to more than one interface, you have to add routes for each destination interface.

   Example:

   ```
   console> mroute add input-interface PortA source-ip 1.1.1.1 dest-ip
    230.1.1.2 output-interface PortB
   ```

   ```
   console> mroute add input-interface PortA source-ip 1.1.1.1 dest-ip
    230.1.1.2 output-interface PortC
   ```

Viewing routes

2. Select **Option 3 (Route Configuration) > Option 2 (Configure Multicast Routing) > Option 2 (Configure Static-routes)** and execute the following command:

```
console> mroute show
```

Removing routes

3. Select **Option 3 (Route configuration) > Option 2 (Configure Multicast Routing) > Option 2 (Configure Static-routes)** and execute the following command:

```
console> mroute del input-interface source-ipaddress destination-ip
 output-interface
```

Example:

```
console> mroute del eth0 1.1.1.1 230.1.1.1 eth2
Multicast route deleted successfully
```

Note

- Source and destination interfaces can't be the same for multicast routes.
- Multicast destination interfaces can't be defined. Route manipulation per interface is required to add or delete multicast routes.
- Non-Ethernet interfaces such as IPsec0 aren't supported.

Multicast routes over IPsec VPN tunnel

Sophos XG Firewall supports secure transport of multicast traffic over untrusted networks using an IPsec VPN connection.

It is possible to send and receive both unicast and multicast traffic between two or more VPN sites connected through the public internet. This removes the dependency of multicast-aware routers between the sites connecting via IPsec VPN.

Any unicast host wanting to access a multicast needs to be configured as an explicit host (with netmask /32) in the VPN configuration.

4. Select **Option 3 (Route Configuration) > Option 2 (Configure Multicast Routing) > Option 2 (Configure Static-routes)** and use the below commands to configure multicast routing over IPsec:

Option	Description
`mroute add input-interface Port portnumber source-ip ipaddress destip ipaddress output-interface Port portnumber`	To forward multicast traffic coming from a given interface to another interface. Example: `console>mroute add input-interface PortA source-ip192.168.1.2 dest-ip239.0.0.55 outputinterface PortB`
`mroute add input-interface Port portnumber source-ip ipaddress destip ipaddress output-tunnel gre name gretunnelname`	To forward multicast traffic coming from a specific interface to a specific GRE tunnel. Example: `console>mroute add input-interface PortA source-ip192.168.1.2 dest-ip 239.0.0.55 output-tunnel gre name Elitecore`

Option	Description
`mroute add input-interface Port portnumber source-ip ipaddress destip ipaddress output-tunnel IPsec`	To forward multicast traffic coming from a specific interface to IPsec tunnels.Sophos XG Firewall automatically selects the appropriate tunnel to be used depending upon the local and remote network configurations. Example: `console>mroute add input-interface PortA source-ip 192.168.1.2 dest-ip 239.0.0.55 outputtunnel IPsec`
`mroute add input-tunnel IPsec name IPsecconnectionname sourceip ipaddress dest-ip ipaddress output-interface Port portnumber`	Forwards multicast traffic coming from an IPsec connection to a specific interface. Example: `console>mroute add input-tunnel IPsec ~Net2Net source-ip 192.168.1.2 dest-ip 239.0.0.55 output-interface PortB`
`mroute add input-tunnel IPsec name IPsecconnectionname sourceip ipaddress dest-ip ipaddress output-tunnel IPsec`	Forwards multicast traffic coming from a specific IPsec tunnel to other IPsec tunnels. Sophos XG Firewall automatically selects the appropriate tunnel to be used based upon the local and remote network configurations. Example: `console>mroute add input-tunnel IPsec name Net2Net source-ip 192.168.1.2 destip 239.0.0.55 output-tunnel IPsec`
`mroute add input-tunnel IPsec name port number source-ip ipaddress dest-ip ipaddress output-tunnel gre name gretunnelname`	Forwards multicast traffic coming from a specific IPsec tunnel to another specific GRE tunnel Example: `console>mroute add input-tunnel IPsec name Net2Net source-ip 192.168.1.2 destip 239.0.0.55 output-tunnel gre name Elitecore`
`mroute add input-tunnel gre name gretunnelname source-ip ipaddress dest-ip ipaddress output-interface Port portnumber`	Forwards multicast traffic coming a specific GRE tunnel to a specific interface. Example: `console>mroute add input-tunnel gre name Elitecore source-ip 192.168.1.2 destip 239.0.0.55 output-interface PortB`

Option	Description
`mroute add input-tunnel gre name gretunnelname source-ip ipaddress dest-ip ipaddress output-tunnel gre name gretunnelname`	Forwards multicast traffic from a specific GRE tunnel to another specific GRE tunnel. Example: `console>mroute add input-tunnel gre name Elitecore source-ip 192.168.1.2 destip 239.0.0.55 output-tunnel gre name Terminal1`
`mroute add input-tunnel gre name gretunnelname source-ip ipaddress dest-ip ipaddress output-tunnel IPsec`	Forwards multicast traffic coming a specific GRE tunnel to IPsec tunnels.Sophos XG Firewall automatically selects the appropriate tunnel to be used depending on the local and remote network configurations. Example: `console>mroute add input-tunnel gre name Elitecore source-ip 192.168.1.2 dest-ip 239.0.0.55 output-tunnel IPsec`
`mroute del source-ip ipaddress dest-ip ipaddress`	Deletes a multicast route. Example: `console>mroute del source-ip 192.168.1.2 dest-ip 239.0.0.55` **Note** The CLI only shows static interfaces as input and output interfaces whereas the web admin console shows both static and dynamic interfaces (PPPoE, DHCP etc).

6 Device console

This page describes the CLI console and the various commands available in the base console.

The device console is used to perform various checks on the system and to view logs files for troubleshooting.

When using the command line, the CLI console requires that you use valid syntax and conform to expected input constraints. It will reject invalid commands.

Sophos XG Firewall has inbuilt help at the command prompt itself to help users with the syntax without the need to exit from the CLI.

To view the list of available commands go to **Option 4 (Device Console)** and press Tab. The following is displayed:

```
console>
clear               ping            telnet
disableremote       ping6           telnet6
dnslookup           set             traceroute
dnslookup6          show            traceroute6
drop-packet-capture system
enableremote        tcpdump
console>
```

Once you start typing a command you can press Tab again to view the list of arguments that are supported or required. Example: When you type ping and press Tab, you are presented with the list of parameters that are required or allowed as shown below:

```
console>ping
<ipaddress>    count       quiet       sourceip
<string>       interface   size        timeout
console>
```

Type the command and then press ? to view the list of arguments supported with descriptions. Example: when you type ping and press ?, all parameters are shown with descriptions.

```
console>ping
quiet          display the summary at startup and end
count          Stop after sending count packets
size           Number of data bytes to be sent
timeout        timeout 'in seconds' before ping exits
interface      Bind interface
sourceip       Bind source ipaddress
<ipaddress>    A.B.C.D (0 <= A,B,C,D < 256)
<string>       Alpha-Numeric TEXT with/without quotes
```

To return the main menu type `exit`.

Below you will find a list of CLI commands and descriptions of their functions.

set

Use `set` to configure various system parameters. For further information on the available parameters see set (page 33).

system

Use `system` to configure various settings. For further information on the available options see system (page 46).

clear

Clears the screen.

disableremote

Disables remote connectivity over SSH, if enabled. By default it is not enabled. The appliance will no longer listen on port 22 for new connections, and existing ones will be terminated. Refer to `enableremote` to allow remote SSH connections.

dnslookup

Query internet domain name servers to resolve hostnames.

Parameter list & description

Syntax	Description
`Host` *`ipaddress`* `Host` *`url`*	Host to be searched.
`Server` *`ipaddress`* `[host]`	Internet name or address of the name server.

dnslookup6

Query internet domain name servers to resolve IPv6 hostnames.

Parameter list and description

Syntax	Description
`Host` *`ipaddress`* `Host` *`url`*	Host to be searched.
`Server` *`ipaddress`* `[host]`	Internet name or address of the name server.

drop-packet-capture

Displays the packets dropped by firewall rules. It will provide connection details and details of the packets processed by the device. This will help administrators to troubleshoot firewall rules. You can also filter the dropped packets.

Syntax	Description
text	BPF (Berkeley Packet Filter) Compatible Packet Filter Expression.
interface *port*	Listen on this interface.
snaplen *20-68835*	Number of bytes to capture.

How to check packets of the	Example
Specific host	host 10.10.10.1
Specific source host	src host 10.10.10.1
Specific destination host	dst host 10.10.10.1
Specific network	net 10.10.10.0
Specific source network	src net 10.10.10.0
Specific destination network	dst net 10.10.10.0
Specific port	port 20
Two specific ports	port 20 or port 21
Specific source port	src port 21
Specific destination port	dst port 21
Specific host for a specific port	host 10.10.10.1 and port 21
Specific host for all ports except SSH	host 10.10.10.1 and port not 22
Specific protocol	proto ICMP, proto UDP, proto TCP

enableremote

Allows remote SSH connections to Sophos XG Firewall. The appliance will listen for SSH connections on the specified port and will allow connections from the specified addresses.

Syntax	Description
port *number*	Ethernet port on the appliance through which a remote SSH can be established.
serverip *ipaddress*	Host IP address from which SSH connections to the appliance will be allowed.

ping

Sends ICMP ECHO_REQUEST packets to IPv4 network hosts and listens for the corresponding ECHO_REPLY.

Syntax	Description
ipaddress	IP Address to be pinged.
string	Domain to be pinged.
count *number*	Send a specific number of packets. Ping will stop after the count number is reached.
interface *interfaceid*	Set the interface on XG Firewall to send packets from.
quiet	Display a summary only at start and end of the ping sequence.
size *number*	Specifies the length, in bytes of the data field in the echo request messages sent. The default is 32. The maximum size is 65,527.
sourceip *ipaddress*	Specifies the source IP address packets will be sent from.
timeout *number*	Stop sending packets and exit from ping after specified time is reached.

ping6

Send ICMPv6 ECHO_REQUEST packets to IPv6 network hosts and listens for the corresponding ECHO_REPLY.

Syntax	Description
ipaddress6	IPv6 address to be pinged.
count *number*	Send a specific number of packets. Ping will stop after count number is reached.
interface *interfaceid*	Set the interface on XG Firewall to send packets from.
quiet	Display a summary only at start and end of the ping sequence.

Syntax	Description
`size` *number*	Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.

tcpdump

Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.

Syntax	Description
text	Packet filter expression. Based on the specified filter, packets are dumped. If no expression is given, all packets are dumped otherwise only packets for which the expression is `true' are dumped. The expression consists of one or more primitives. Primitives usually consist of an id (name or number) proceeded by one or more qualifiers. Refer to the below example table on writing filtering expressions.
`count` *number*	Exit tcpdump after receiving specified number of packets.
`filedump`	Tcpdump output can be generated based on criteria required. The output file can be found under `/tmp`.
`hex`	Print each packet (minus its link level header) in hexadecimal notation.
`interface` *interfaceid*	Specifies the interface to listen on.
`llh`	View packet contents with ethernet or other layer 2 header information.
`no_time`	Do not print a timestamp for each dump line.
`quite`	Print less protocol information so that output lines are shorter.
`verbose`	Verbose output. For example, the time to live, identification, total length and options in an IP packet are printed. Also enables additional packet integrity checks such as verifying the IP and ICMP header checksum.

Below you will find some examples of how to use the tcpdump command to view different information.

Note
Expressions can be combined using logical operators AND, OR and NOT. Make sure when using different combinations to encapsulate the full query within single quotes.

How to view traffic of	tcpdump command	Example
Specific host	tcpdump 'host <ipaddress>'	tcpdump 'host 10.10.10.1'
Specific network	tcpdump 'net <network address>'	tcpdump 'net 10.10.10.0'
Specific source network	tcpdump 'src net <network address>'	tcpdump 'src net 10.10.10.0'
Specific destination network	tcpdump 'dst net <network address>'	tcpdump 'dst net 10.10.10.0'
Specific port	tcpdump 'port <portnumber>'	tcpdump 'port 21'
Specific source port	tcpdump 'src port <port number>'	tcpdump 'src port 21'
Specific destination port	tcpdump 'dst port <port number>'	tcpdump 'dst port 21'
Specific host and specific port	tcpdump 'host <ipaddress> and port <port number>'	tcpdump 'host 10.10.10.1 and port 21'
Specific host and all ports except SSH	tcpdump 'host <ipaddress> and port not <port number>'	tcpdump 'host 10.10.10.1 and port not 22'
Specific protocol	tcpdump 'proto <protocol name>'	tcpdump 'proto ICMP' tcpdump 'proto UDP'
Specific interface	tcpdump interface <interfaceid>	tcpdump interface port2
Specific port on a specific interface	tcpdump interface <interfaceid> 'port <port number >'	tcpdump interface port2 'port 21'

telnet

Use telnet to connect to another remote computer. Can be used to check if a system is accepting connections on a specific port. Telnet data is sent in clear text so for admin tasks it is advised to use SSH when possible.

Syntax	Description
`ipaddress` *`port number`*	FQDN, alias or IP address of a remote host followed by the port number to connect to. If no port information is specified then the default telnet port (23) is used.

telnet6

Use telnet6 to connect via telnet to an IPv6 addressed system

Syntax	Description
`ipv6address` *`port number`*	FQDN, alias or IPv6 address of a remote host followed by the port number to connect to. If no port information is specified then the default telnet port (23) is used.

traceroute

Traceroute tracks the route packets take from an IPv4 network on their way to a specific host. It utilizes the IP protocol's time to live (TTL) field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to the host.

Syntax	Description
<ipaddress>	Specifies the destination IP address to trace the route to.
<string>	Specifies the domain to trace the route to.
`first-ttl`	Sets the initial time to live used in the first outgoing packet.
`icmp`	Use ICMP ECHO instead of UDP datagrams.
`max-ttl`	Specifies the maximum time to live of packets.
`no-frag`	Sets the don't fragment bit in the sent packets.
`probes`	Probes are sent at each ttl. Default value is 3.
`source`	Sets the specified IP address as the source address of sent packets.
`timeout`	Sets the timeout in seconds for a response to a probe. Default is 5.
`tos`	For IPv4, set the Type of Service (TOS) and Precedence value. Useful values are 16 (low delay) and 8 (high throughput).

traceroute6

Traceroute tracks the route packets take from an IPv6 network on their way to a specific host. It utilizes the IP protocol's time to live (TTL) field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to the host.

Syntax	Description
<ipv6address>	Specifies the destination IPv6 address to trace the route to.
<string>	Specifies the domain to trace the route to.
`first-ttl`	Sets the initial time to live used in the first outgoing packet.
`icmp`	Use ICMP ECHO instead of UDP datagrams.
`max-ttl`	Specifies the maximum time to live of packets.
`no-frag`	Sets the don't fragment bit in the sent packets.
`probes`	Probes are sent at each ttl. Default value is 3.
`source`	Sets the specified IP address as the source address of sent packets.
`timeout`	Sets the timeout in seconds for a response to a probe. Default is 5.
`tos`	Sets the type of service. For IPv6, this is referred to as the Traffic Control value.

show

Displays configured parameters of the following firewall settings.

Syntax	Description
`advanced-firewall`	Displays the currently configured advanced firewall parameters. For a full explanation of parameters please refer to set (page 33)
`arp-flux`	Shows if arp-flux is currently turned on or off.

`country-host`
`ip2country` *ipaddress*
`list`
	Use the **ip2address > ipaddress** option to find the country that hosts a specific IP address. Use the list parameter to list the stored IP addresses and the country that hosts them.

Syntax	Description
`fqdn-host`	Displays the configured parameters for: • cache-ttl • idle-timeout • learn-subdomains • IP eviction
`http_proxy`	Displays to following configured parameters for the HTTP proxy. • add_via_header • core_dump • relay_invalid_http_traffic • connect_timeout • tunnel_timeout • client_timeout • response_timeout • proxy_tlsv_0 • captive_portal_tlsv1_0 • captive_portal_x_frame_options
`ips-settings`	Displays the currently configured IPS settings and running instances.

`ip-signature`
`alert`
`disable`
`drop`
	Lists the IPS signatures, by numeric ID, currently configured.
	Alert will show signatures configured to alert when triggered.
	Disable will show the signatures currently disabled.
	Drop will show the signatures currently configured to drop traffic when triggered.

`ips_conf`	Shows the current IPS configuration.
`lanbypass`	Shows the current lanbypass configuration. In this mode, one or two pairs of interfaces are bridged, allowing uninterrupted traffic flow without scanning when there is power failure or hardware malfunction.

`nat-policy`
`application-server`
`failover`
`mail-notification`
	Displays the nat policy settings, enabled or disabled, for the protected application servers.

Syntax	Description
`network`	Displays various configured network parameters according to the filters used.
`interface-speed`*`interfaceid`*	Shows the current network speed over the specified interface.
`interfaces`	Shows details of interfaces on the appliance including logical interfaces.
`lag-interface`*`interfaceid`*	Shows details of the specified LAG interface.
`macaddr`*`interfaceid`*	Displays the MAC address of the specified interface.
`mtu-mss`*`interfaceid`*	Shows the current configured MTU of the specified interface, default MTU 1500 MSS 1460.
`static-route`	Displays all current IPv4 static routes.
`static-route6`	Displays all current IPv6 static routes.

6.1 set

Details of the system components that are configurable via the `set` command.

Use the set command to define settings and parameters for various system components.

For example after typing `set` press tab to view list of configurable components. These options and their parameters are described below.

advanced-firewall

The advanced-firewall option allows configuration of various firewall related parameters and settings such as the traffic to be inspected, protocol timeout values and traffic fragmentation. The full list of parameters available for configuration is shown in the table below.

Syntax	Description
`bypass-stateful-firewall-config [`*`add`*`] [`*`del`*`] [ `*`dest_host`*`] [`*`dest_network`*`] [`*`source_host`*`] [`*`source_network`*`]`	Add a host or network where the outbound and return traffic does not always traverse through Sophos XG Firewall. You can add or delete either single hosts or entire networks.
`icmp-error-message [`*`allow`*`] [`*`deny`*`]`	Allow or deny ICMP error packets describing problems such as network/host/port unreachable, destination network/host unknown.

Syntax	Description
`strict-icmp-tracking [on] [off]`	Allow or drop ICMP reply packets. Setting this option **On** drops all ICMP reply packets.
`tcp-appropriate-byte-count [on] [off]`	Controls Appropriate Byte Count (ABC) settings. ABC is a way of increasing congestion window (cwnd) more slowly in response to partial acknowledgments. for more information see RFC3465
`tcp-selective-acknowledgement [on] [off]`	tcp-selective-acknowledgement Off: Disables selective acknowledgment. Using selective acknowledgments, the data receiver can inform the sender about all segments that have arrived successfully, so the sender need retransmit only the segments that have actually been lost.
`tcp-window-scaling [on] [off]`	tcp-window-scaling Off: Disables window scaling. The TCP window scaling increase the TCP receiving window size above its maximum value of 65,535 bytes. For more information see RFC1232
`fragmented-traffic [allow] [deny]`	Allow or deny fragmented traffic. IP Fragmentation is the process of breaking down an IP datagram into smaller packets before transmitting and reassembling them at the receiving end. For more information see RFC4459 Section 3.1
`ipv6-unknown-extension-header [allow] [deny]`	Allow or drop IPv6 packets with unknown extension headers.
`strict-policy [on] [off]`	When strict policy is applied, the device drops specific traffic and IP based attacks against the firewall. By default, strict policy is always on. When strict policy is off, strict firewall policy is disabled.
`tcp-est-idle-timeout [2700-432000]`	Sets the idle timeout value in seconds for established TCP connections. Available values are 2700-432000.

Syntax	Description
`tcp-seq-checking [on] [off]`	Every TCP packet contains a Sequence Number (SYN) and an Acknowledgment Number (ACK). Sophos XG Firewall monitors SYN and ACK numbers within a certain window to ensure that the packet is indeed part of the session. However, certain application and third party vendors use non-RFC methods to verify a packet's validity or for some other reason a server may send packets with invalid sequence numbers and expect an acknowledgment. For this reason, XG Firewall offers the ability to disable this feature.
`udp-timeout [30-3600]`	Set the timeout value in seconds for UDP connections that have not yet been established. Available values are 30-3600.
`ftpbounce-prevention [control] [data]`	Prevent FTP bounce attacks on FTP control and data connections. Traffic is considered as an FTP bounce attack when an attacker sends a PORT command with a third party IP address to an FTP server instead of its own IP address.
`midstream-connection-pickup [on] [off]`	Configure midstream connection pickup settings. Enabling midstream pickup of TCP connections will help while plugging in the Sophos XG Firewall as a bridge in a live network without any loss of service. It can also be used for handling network behavior due to peculiar network design and configuration. E.g. atypical routing configurations leading to ICMP redirect messages. By default, XG Firewall is configured to drop all untracked (mid-stream session) TCP connections in both deployment modes.
`sys-traffic-nat [add] delete] [destination] [interface] [netmask] [snatip]`	Administrators can NAT the traffic generated by the firewall so that the IP Addresses of its interfaces are not exposed or to change the NAT'd IP for traffic going to a set destination. for more information please see KB 122999
`tcp-frto [on] [off]`	Enable or disable forward RTO-Recovery (F-RTO). F-RTO is an enhanced recovery algorithm for TCP retransmission timeouts and it is particularly beneficial in wireless environments where packet loss is typically due to random radio interference rather than intermediate router congestion. F-RTO is sender-side only modification. Therefore it does not require any support from the peer.

Syntax	Description
`tcp-timestamp [on] [off]`	Enable or disable tcp timestamps. Timestamp is a TCP option used to calculate the round trip measurement in a better way than the retransmission timeout method.
`udp-timeout-stream [30-3600]`	Set up UDP timeout value in seconds for established UDP connections. Available values are from 30-3600.

arp-flux

ARP flux occurs when multiple ethernet adapters, often on a single machine, respond to an ARP query. Due to this, problem with the link layer address to IP address mapping can occur. Sophos XG Firewall may respond to ARP requests from both Ethernet interfaces. On the machine creating the ARP request, these multiple answers can cause confusion. ARP flux affects only when Sophos XG Firewall has multiple physical connections to the same medium or broadcast domain.

Syntax	Description
`on`	Sophos XG Firewall may respond to ARP requests from both ethernet interfaces when Sophos XG Firewall has multiple physical connections to the same medium or broadcast domain.
`off`	Sophos XG Firewall responds to ARP requests from respective ethernet interfaces when Sophos XG Firewall has multiple physical connections to the same medium or broadcast domain.

fqdn-host

Sophos XG Firewall supports FQDN Hosts that define an entry by the Fully Qualified Domain Name which resolve to the IP address as found by DNS requests. This allows for dynamically assigned IP addresses to be used as host definitions, there is limit of 16,000 for the number of hosts that can be created. This can also be configured from the GUI, for further information about GUI configuration see KB 123035

Syntax	Description
`cache-ttl [60-86400] [ dns-reply-ttl]`	Set cache-ttl value for FQDN Host. The cache-ttl value represents the time in seconds after which the cached FQDN host to IP address binding will be updated. Range: 1 – 86400 seconds Default: 3600 seconds dns-reply-ttl: use the ttl value in DNS reply packet as cache-ttl
`eviction [enable] [ disable] [interval] [ 60-86400]`	Duration in seconds after which IP addresses for subdomains of wildcard FQDNs are evicted. The available range is 60-86400.
`idle-timeout [60-86400] [default]`	The idle-timeout value represents the time in seconds after which the cached FQDN host to IP address binding is removed. Range: 60 – 86400 seconds Default: 3600 seconds
`learn-subdomains [enable] [disable]`	Learn the IP address of subdomains for FQDN using wildcard. Enable if you want to know ip address of subdomains of local traffic and that is passing through XG Firewall, that is, traffic that is not destined for or originated by the XG Firewall.

http_proxy

Sets various parameters for the HTTP proxy, these are described in the tble below.

Syntax	Description
`add_via_header [on] [off]`	Either add or remove the via header to traffic that passes through the proxy. The via header is used for tracking message forwards, avoiding request loops, and identifying the protocol capabilities of senders along the request/ response chain.
`captive_portal_tlsv1_0 [on] [off]`	Allow or deny connections using TLSv1 to the captive portal. TLSv1 has been superseded and is no longer considered secure, therefore this should only be enabled if required for a certain business need.

Syntax	Description
`captive_portal_x_frame_options [on] [off]`	Enable or disable the addition of the x frame options header for captive portal traffic. The x-frame-options (XFO), is an HTTP response header, also referred to as an HTTP security header, which has been around since 2008. In 2013 it was officially published as RFC 7034, but is not an internet standard. This header tells the browser how to behave when handling a site's content. The main reason for its inception was to provide clickjacking protection by not allowing rendering of a page in a frame. for further information please see RFC 7034
`client_timeout [1-2147483647] [default]`	Sets the timeout in seconds for clients with established connections via the proxy. The available values are 1-2147483647, default is 60.
`connect_timeout [1-2147483647] [default]`	Sets the timeout value in seconds for connections attempting to be made via the proxy. Available values are 1-2147483647, default is 60.
`core_dump [on] [off]`	Determines whether a coredump file will be created in the event the proxy encounters an error and crashes. Coredump files can help with troubleshooting issues and will be useful to support in the event that issues are encountered.
`proxy_tlsv1_0 [on] [off]`	Allow or deny connections using TLSv1 through the proxy. TLSv1 is a deprecated encryption protocol that has been superseded by TLSv1.3. Therefore care should be taken when allowing TLSv1 connections.
`relay_invalid_http_traffic [on] [off]`	Determines whether non HTTP traffic sent over HTTP ports should be relayed or dropped by the proxy. Some applications will send traffic over ports normally used by HTTP, 80 and 443, in these instances the proxy may not be able to handle the traffic which can cause issues. If this is the case then it is often advisable to bypass the proxy all together for this traffic.
`response_timeout [1-2147483647] [default]`	Sets the timeout in seconds that the proxy will wait for a response to be received for a new connection before that connection is terminated. Available values are 1-2147483647, default is 60.

Syntax	Description
`tunnel_timeout [1-2147483647] [default]`	Sets the timeout value in seconds that the proxy will wait for a response whilst trying to set up an HTTPS connection. Available values are 1-2147483647, default is 300.
`disable_tls_url_categories [on] [off]`	Allows you to turn on or turn off category lookup for SSL/TLS Inspection Rules. If disable_tls_url_categories is on, traffic isn't categorized. This affects which SSL/TLS inspection rule will be chosen. For SSL/TLS inspection rules it will only match those with **ANY** specified for **Categories and websites** and nothing else. For example, if there is no SSL/TLS rule with value **ANY** for **Categories and websites**, no rule will be matched if disable_tls_url_categories is on, the default behavior applies. These settings also affect any web policy applied to the traffic. The traffic will be uncategorized when a web policy is applied to it during the TLS handshake. The disable_tls_url_categories setting does not affect categorization of URLs for HTTP or decrypted HTTPS traffic as the full packet contents can be seen in these scenarios.

ips

Allows configuration of settings for the Intrusion Prevention System, IPS. The configurable parameters are described below. IPS consists of a signature engine with a predefined set of signatures. Signatures are the patterns that are known to be harmful. IPS compares traffic to these signatures and responds at a high rate of speed if it finds a match. Signatures included within the device are not editable.

Syntax	Description
`enable_appsignatures [on] [off]`	Turns app based signatures on or off for IPS. App signatures determine the application that is using a specific data stream to help determine if traffic is malicious or should be allowed. By default app based signatures are enabled.
`failclose [apply] [off] [on] [timeout] [tcp] [udp] [1-43200]`	Determines if a connection should be closed in the event of a failure and the timeout in seconds for both tcp and udp connections that pass through IPS. The available timeout values for both UDP and TCP traffic are 1-43200.

Syntax	Description
`http_response_scan_limit [0-262144]`	Sets the scan limit for HTTP response packets. Available values are 0-262144, for full scanning this should be set to 0.
`inspect [all-content] [untrusted-content]`	Specifies IPS inspection for all or untrusted content. *untrusted-content*: Inspects untrusted content only. Doesn't inspect content trusted by Sophos Labs. Provides best performance. *all-content*: Inspects all content. Provides best security. Default: Inspects untrusted content only.
`ips-instance [apply] [clear] [add] [IPS] [cpu] [0-1]`	Creates a new IPS cpu instances, clears the IPS instance or applies a new IPS configuration.
`ips_mmap [on] [off]`	Enabling mmap optimizes RAM usage, especially in low-end devices. By default mmap is on.
`lowmem-settings [on] [off]`	Enables or disables low memory settings for IPS. These settings will only be applied in the event that the appliance encounters memory issues.
`maxpkts [numeric value above 8] [all] [default]`	Sets the number of packets to be sent for application classification. By default this is set to 8 but can be changed to send all packets or any number of packets above 8.
`maxsesbytes-settings [update] [ numeric value]`	The maxsesbytes-settings allows you to set the maximum allowed file size to be scanned by IPS. Any file larger the configured size is bypassed and is not scanned. This value is applied per session.

Syntax	Description
`packet-streaming [on] [off]`	Determines whether packet streaming is to be allowed or not. Packet streaming is used to restrict the streaming of packets in situations where the system is experiencing memory issues. If stream is set to on, which is the default setting, the IPS engine builds an internal table during a session and deletes them at the end of each session. It also reassembles all incoming packets and checks the data for any known signatures. If stream is set to off, then protocols such as Telnet, POP3, SMTP, and HTTP are vulnerable as reassembly of packets or segments can no longer occur. Data is sometimes broken up into chunks of packets and must be reassembled to check for signatures, these protocols are now vulnerable to malicious files that are hidden by splitting.
`search-method [ac-bnfa] [ac-q] [hyperscan]`	Set the search method to be used for IPS signature pattern matching. ac-bnfa (low memory usage, high performance) ac-q (high memory usage, best performance) hyperscan (low memory usage, best-performance)
`sip_ignore_call_channel [enable] [disable]`	Set whether the audio and video data channels should be ignored. Enable this option to ignore such channels. Enabled by default.
`sip_preproc [enable] [disable]`	Set whether SIP preprocessor should be enabled or not. Enabling this will scan all the SIP sessions to prevent any network attacks.

ips_conf

Allows the administartor to add, delete or edit an existing IPS configuration entry.

Syntax	Description
`add [key] [text] [value] [text]`	Add a new IPS configuration.
`del [key] [text] [value] [text]`	Delete and existing IPS configuration.
`update [key] [text] [value] [text]`	Update and exiting IPS configuration.

lanbypass

In this mode, one or two pairs of interfaces are bridged, allowing uninterrupted traffic flow without scanning when there is a power failure or hardware malfunction. When enabled, traffic is bypassed for all modules - onboard and external modules. When power is restored, XG Firewall automatically resumes normal functionality. For example, in XG750, if 7 modules (14 LAN bypass pairs) are connected, bypass is enabled for all 14 pairs.

Syntax	Description
`off`	Turns Lan bypass off. This is the default setting.
`on`	Turns Lan bypass on.

network

Allows you to configure various network parameters including routes, interface speeds, MTU, MAC address and ports.

Syntax	Description
`interface-speed [PortID] [speed] [1000fd] [100fd] [100hd] [10fd] [10hd] [auto]`	Allows to configure the interface speed. Values are given in Mbps and either full or half duplex. Auto allows the interface to automatically negotiate speed with the connected neighbor device.
`macaddr [PortID] [default] [override] [string value]`	Allows you to set the MAC address of the interface. Default will keep the existing MAC, if using the override parameter then you will need to define the required MAC address string manually.
`mtu-mss [PortID] [mtu ] [number value] [default] [mss] [number value] [default]`	Allows you to define the required MTU and MSS for interfaces. Default values are, MTU 1500 and MSS 1460.

on-box-reports

Allows you to determine if reports are generated on Sophos XG Firewall or not.

Syntax	Description
`on`	Turn on box reports on.
`off`	Turns on box reports off.

port-affinity

Configures port affinity settings. Administrators can manually assign/unassign a CPU Core to a specific interface. Once configured, all the network traffic for that interfaces is handled by the assigned CPU Cores.

Note
CPU cores can only be assigned to interfaces that have already been configured.

Port-affinity is not supported with legacy network adaptors, for example, when a virtual appliance is deployed in Microsoft Hyper-V.

Syntax	Description
`add [port] [PortID] [bind-with] [start-with] [cpu] [cpu number]`	Allows you to add port affinity settings to the desired interface.
`defsetup`	Applies the default port affinity configuration.
`del [port] [PortID]`	Deletes current port affinity settings for the selected port.
`fwonlysetup`	This is the legacy default port affinity setup and only handles plain firewall traffic which doesn't include any proxy or IPS traffic.

proxy-arp

Allows to define how the proxy will respond to arp requests.

Syntax	Description
`add [interface] [PortID] [dest_ip] [ dst_iprange]`	Applies proxy arp settings to the defined interface.
`del [interface] [PortID] [dest_ip] [ dst_iprange]`	Deletes proxy arp settings from the defined interface

report-disk-usage

Sets a watermark in percentage for the report disk usage. The watermark represents the percentage up to which data can be written to the report disk.

Syntax	Description
`watermark [default] [numerical value]`	Sets the watermark level, allowed values are from 60 to 85. Default: 80.

routing

Allows configuration of routing parameters for multicast group limits,source base route for aliases and wan load balancing.

Syntax	Description
`multicast-group-limit [numerical value]`	Applies the multicast group limit.
`source-base-route-for-alias [enable] [disable]`	Applies or removes source based routes for alias addresses.
`wan-load-balancing [session-persistant] [weighted-round-robin] [connection-based] [destination-only ] [source-and-destination] [source-only ] [ip-family ] [all] [ipv4] [ipv6]`	Configures WAN load balancing to balance traffic between multiple WAN interfaces. Session persistence will send traffic for the same session over a specific interface. Weighted round robin will pass traffic over different interfaces depending on the load that each interface is experiencing. When using session persistence to balance traffic this can be defined in four ways. Connection based send all traffic related to the same connection over the same interface. Destination only send all traffic to a specific source over the same interface. Source and destination sends all traffic between the same source and destination over the same interface. Source only sends all traffic from a specific source over the same interface. Furthermore you can choose to balance just IPv4, IPv6 or all traffic.

service-param

By default XG Firewall inspects all HTTP, HTTPS, FTP, SMTP/S, POP and IMAP traffic on the standard ports. Use service-param to enable inspection of traffic sent over non-standard ports.

Syntax	Description

`FTP [add] [delete] [port] [port number]`
`HTTP [add] [delete] [port] [port number]`
`IMAP [add] [delete] [port] [port number]`
`IM_MSN [add] [delete] [port] [port number]`
`IM_YAHOO [add] [delete] [port] [port number]`
`POP [add] [delete] [port] [port number]`
`HTTPS [add] [delete] [port] [port number] [deny_unknown_proto] [on] [off] [invalid-certificate] [allow] [block]`
`SMTP [add] [delete] [port] [port number] [failure_notification] [on] [off] [fast-isp-mode] [on] [off] [notification-port] [add] [port] [port number] [strict-protocol-check] [on] [off]`
`SMTPS [add] [delete] [port] [port number] [invalid-certificate] [allow] [block]`
	To allow inspection of traffic on non-standard ports for a specific protocol use the add port commands, this works for all services available within the service-param command list.
	HTTPS, SMTP and SMTPS have further options available.

network

Allows you set various network parameters for interfaces such as speed, MAC address, MTU-MSS and LAG details.

Syntax	Description
`interface-speed [Port] [speed] [speed value]`	Available speed values are: 1000fd, 100fd, 100hd, 10fd, 10hd or auto. The fd and hd denote half or full duplex.
`macaddr [Port] [default] [override] [string]`	Allows to set the MAC address of an interface. Here string would be the new MAC address you want to use.
`mtu-mss [Port] [default] [number]`	Sets the MTU-MSS value foe the interface. Default is 1500.

Syntax	Description
`lag-interface [interface_name] [lag-mgt] [active-backup] [auto] [Port] [lacp] [lacp-rate] [fast] [slow] [static-mode] [enable] [disable] [xmit-hash-policy] [layer2] [layer2+3] [layer3+4] [link-mgt] [down-delay] [value] [garp-count] [value] [monitor-interval] [value] [up-delay] [value]`	Allows you to set various parameters for any configured lag interfaces. Where the variable is stated as value, the available values are shown below. down-delay available values 0-10000 milliseconds garp-count values 0-255 monitor-interface values 0-10000 milliseconds up-delay values 0-10000 milliseconds

VPN

Allows you to set various parameters for VPN connections including failover settings, authentication settings and MTU.

Syntax	Description
`conn-remove-on-failover [all] [non-tcp] [conn-remove-tunnel-up] [disable] [enable] [l2tp] [authentication] [ANY] [CHAP] [MS_CHAPv2] [PAP] [mtu] [number] [pptp] [authentication] [ANY] [CHAP] [MS_CHAPv2] [PAP]`	Authentication parameters can be set for L2TP and PPTP vpns aswell as global failover and failback parameters for all traffic or just non tcp traffic. MTU can be set for L2TP, the available values are 576 – 1460, default is 1410.

6.2 system

The `system` command allows configuration of a range of system parameters.

The components and their parameters configurable via `system` are described in the sections below:

airgap

Allows you to view airgap status and turn airgap functionality on and off.

Syntax	Description
`[enable]`	Use to enable airgap functionality.
`[disable]`	Use to disable airgap functionality.
`[show]`	Displays the current airgap configuration.

appliance_access

Allows you to override or bypass the configured device access settings and allow access to all the XG Firewall services.

Syntax	Description
`[disable]`	Disables appliance access. Disable is the default setting.
`[enable]`	Enables appliance access.
`[show]`	Displays the current appliance access status.

application_classification

Once application classification is enabled, traffic is categorized on the basis of application, and is displayed on the Admin Console. Once application classification is enabled, you can enable microapp discovery, which identifies and classifies microapps used within web browsers. If application classification is disabled, traffic categorization is based on port numbers.

Syntax	Description
`[off] [on] [show] microapp-discovery [off] [on] [show]`	If application classification is enabled, traffic is categorized on the basis of application. Once application classification is enabled, you can enable microapp discovery, which identifies and classifies microapps used within web browsers. If application classification is disabled then traffic is classified based on port number. Default: on

auth

Sets authentication parameters for use with STAS, terminal services, thin client, and maximum live user settings.

Syntax	Description
`cta [add] [delete] [IP-Address]`	CTA is used in the configuration of STAS authentication. When entering commands where IP-Address is specified you need to type the IP address.

Syntax	Description
`max-live-users [set] [numerical value] [show]`	For max live users the available values are 8192-32768. Using the command show will display the currently configured values.
`thin-client [add] [delete] [citrix-ip] [IP-Address] [show]`	Thin client is used for authentication within a Citrix environment.

auto-reboot-on-hang

Auto reboot on hang determines how the system behaves if the kernel goes into a hung state.

Syntax	Description
`[disable] [enable] [show]`	Default: enabled.

bridge

Allows setting of various parameters for bridged interfaces.

Syntax	Description
`bypass-firewall-policy [unknown-network-traffic] [allow] [drop] [show] [dynamic] [static]`	Use the bypass-firewall-policy command to configure a policy for non-routable traffic for which no security policy is applied.
`static-entry [add] [delete] [show] [interface] [bridge name] [Port] [macaddr] [MAC Address] [priority] [dynamic] [static]`	Use the static-entry command for configuring static MAC addresses in bridge mode. The bridge forwarding table stores all the MAC addresses learned by the bridge and is used to determine where to forward packets.
`max_bridge_members [reset] [set] [limit] [numerical value] [show]`	Use the max_bridge_members command to set the maximum number of interfaces allowed for a bridged interface. Available values are, 2-256.

captcha_authentication_global

Allows you to enable or disable CAPTCHA for administrators signing in to the web admin console and for local and guest users signing in to the user portal using the WAN or VPN interfaces.

If you use this command to disable the CAPTCHA, it will override the VPN-specific setting. We recommend having this setting enabled, and only disabling the CAPTCHA for VPN users using the VPN specific command, captcha_authentication_VPN.

Signing in from a LAN interface doesn't require a CAPTCHA.

Syntax	Description
`[disable] [enable] [show] for [webadminconsole] [userportal]`	Default: Enabled

captcha_authentication_VPN

Allows you to enable or disable CAPTCHA for administrators signing in to the web admin console and for local and guest users signing in to the user portal.

Administrators signing in to the web admin console, and local and guest users signing in to the user portal from the WAN or VPN zones must enter a CAPTCHA. Local users are registered on XG Firewall and not on an external authentication server, such as an AD server.

The CAPTCHA doesn't show on XG 85, XG 85w devices, and on Cyberoam devices upgraded to XG Firewall.

Syntax	Description
`[disable] [enable] [show] for [webadminconsole] [userportal]`	Default: Disabled

If you configured a site-to-site IPsec connection with remote subnet set to **Any**, the CAPTCHA applies to all these tunnels. To make sure the CAPTCHA doesn't apply to specific remote hosts or networks, add these to an IPsec route. For `<mytunnel>`, select from the names of the original IPsec connections shown on the command-line interface.

Examples of commands to add a remote host or network are as follows:

Remote host: `console> system ipsec_route add host <50.50.50.1> tunnelname <mytunnel>`

Remote network: `console> system ipsec_route add net <10.10.10.0/255.255.255.0> tunnelname <mytunnel>`

cellular_wan

Allows you to enable or disable the cellular WAN and view any Wi-Fi modem information if connected. The cellular WAN menu will be available in web admin console once cellular WAN has been enabled from CLI.

Syntax	Description
`[disable] [enable] query [serialport] [serial port number] [ATcommand] [command string] set [disconnect-on-systemdown] [off] [on] modem-setup-delay [numerical value]`	When using the modem-setup-delay command, the numerical value is the number of seconds that you wish to delay the modem coming online. When using AT commands all valid AT commands are accepted.

custom-feature

Allows you to add top users to generated PDF reports.

Syntax	Description
`[disable] [enable] [show]`	You can enable or disable this feature and show the current setting.

dhcp

XG Firewall supports configuration of DHCP options, as defined in RFC 2132. DHCP options allow you to specify additional DHCP parameters in the form of pre-defined, vendor-specific information that is stored in the options field of a DHCP message. When the DHCP message is sent to clients on the network, it provides vendor-specific configuration and service information. Appendix A provides a list of DHCP options by RFC-assigned option number.

Syntax	Description
`conf-generation-method [new] [old] [show]`	Use conf-generation-method to assign the method of generating configuration messages. Default: old.
`dhcp-relay-refresh-interval [set] [seconds] [numerical value] [show]`	Use dhcp-relay-refresh-interval to set the time in seconds for refresh packets to be sent. Available options, 10-1000. Default, 10
`dhcp-options [add] [optioncode] [numerical value] [delete] [optionname] [binding] [add] [delete] [dhcpname] [show]`	Use dhcp-options to assign properties from the DHCP server to the clients. Example: Set a DNS server address.
`lease-over-IPSec [disable] [enable] [show]`	Use lease-over-IPSec to specific how DHCP leases should be handled for IPsec connections. Default: disable.
`one-lease-per-client [disable] [enable] [show]`	Default: disable
`send-dhcp-nak [disable] [enable] [show]`	Default: enable
`static-entry-scope [disable] [enable] [show]`	Default: network

dhcpv6

XG Firewall supports configuration of DHCPv6 options, as defined in RFC 3315. DHCPv6 options allow you to specify additional DHCPv6 parameters in the form of pre-defined, vendor-specific information that is stored in the options field of a DHCPv6 message. When the DHCPv6 message

is sent to clients on the network, it provides vendor-specific configuration and service information. Appendix B provides a list of DHCPv6 options by RFC-assigned option number.

Syntax	Description
`dhcpv6-options [add] [optioncode] [numerical value] [delete] [optionname] [list] [binding] [add] [delete] [dhcpname] [show]`	Available values for optioncode: 1-65535.

discover-mode

Use this command to configure discover mode on one or more interfaces.

Syntax	Description
`tap [add] [delete] [Port] [show]`	Add and delete discover mode for the specified ports or show current ports that have discover mode configured.

diagnostics

Diagnostics allows you to view and set various system parameters for troubleshooting purposes.

Syntax	Description
`ctr-log-lines [numerical value] [traceroute] [traceroute6]`	Set number of lines to display in Consolidated Troubleshooting Report (CTR) log file. ctr-log-lines available options 250-10000. Default, 1000.
`purge-old-log`	Use purge-old-log to purge all rotated log files
`subsystems [Access-Server] [Bwm] [CSC] [IM] [IPSEngine] [LoggingDaemon] [Msyncd] [POPIMAPDaemon] [Pktcapd] [SMTPD] [SSLVPN] [SSLVPN-RPD] [WebProxy] [Wifiauthd]`	When using subsystems: Configure each subsystem individually. Configuration options include: debug, purge-logs and purge-oldlogs
`show [cpu] [interrupts] [syslog] [version-info] [ctr-log-lines] [memory] [sysmsg] [disk] [subsystem-info] [uptime]`	Use diagnostics to view the current status of various systems such as cpu and memory usage.
`utilities [arp] [bandwidthmonitor] [connections] [dnslookup] [dnslookup6] [drop-packet-capture] [netconf] [netconf6] [ping] [ping6] [process-monitor] [route] [route6] [traceroute] [traceroute6]`	Utilities provides a number of systems to help with troubleshooting.

dos-config

Use dos-config to configure denial of service (DoS) policies and rules. You can enable flood protection for ICMP/TCP/UDP/IP packet types by configuring the maximum packets per second to be allowed per source, destination or globally. If the traffic exceeds the limit then the device considers it an attack.

DOS policy configuration:

Syntax	Description
`add [dos-policy] [policy_name] [string] [ICMP-Flood] [IP-Flood] [SYN-Flood] [UDP-Flood] [numerical value] [pps] [global] [per-dst] [per-src]`	Value options 1-10000 packets per second. Using per-src: Configures packets per second (pps) allowed from a single source, above which the device will drop the packets. The limit is applicable to individual source requests per user/IP address. Using per-dest: Configures packets per second (pps) allowed to a single destination. The limit is applicable to individual destination requests per user/IP address. Using global: Apply the limit on the entire network traffic regardless of source/destination requests. With per-src option configured, if the source rate is 2500 packets/second and the network consists of 100 users then each user is allowed a packet rate of 2500 packets per second. With global option selected, if limit configured is 2500 packets/second and the network consists of 100 users then only 2500 packets/second are allowed to the entire traffic coming from all the users.

DOS rule configuration:

Syntax	Description
`add [dos-rule] [rule_name] [rule_name] [srcip] [ipaddress] [dstip] [ipaddress] [netmask] [netmask value] [protocol] [icmp] [ip] [tcp] [udp] [rule-position] [position number] [src-interface] [interfacename] [src-zone] [DMZ] [LAN] [WAN] [VPN] [WiFi] [custom zone] [dos-policy] [policy name]`	You can create a DOS rule to apply to all packet types or specific packet types within one command.

To delete a DOS rule or policy:

Syntax	Description
`delete [dos-policy] [dos-rule] [dos-policy] [rule-name] [policy-name] [string]`	When specifying the string this should be the name of your dos rule or policy.

To flush or view DOS rules and policies the following options are available:

Syntax	Description
`flush [dos-rules] show [dos-rules] [dos-policies] [rule-name] [policy-name] [string]`	When specifying a string this should be your policy or rule name.

filesystem

The filesystem command enables you to enforce disk write permissions for the report partition.

Syntax	Description
`enforce-disk-write [partition-name] [report] [enable] [disable] [show]`	Enable or disable disk write permissions or show the current status. Default: enabled.

firewall-acceleration

Use firewall-acceleration to enable the uses advanced data-path architecture allowing faster processing of data packets for known traffic.

Syntax	Description
`[disable] [enable] [show]`	Enable or disable firewall acceleration or show the current configuration. Default: enabled.

fsck-on-nextboot

Check file system integrity of all the partitions. Turning this option on forcefully checks the file system integrity on next device restart. If the device goes into failsafe mode then this check is automatically turned on. The device can go into failsafe mode for the following reasons;

- Unable to start config, report or signature database.
- Unable to apply migration.
- Unable to find the deployment mode.

Syntax	Description
`[off] [on] [show]`	Turn integrity checking on or off for the next restart or show the current configuration. Default: off.

gre

Using gre you can configure, delete, set TTL and status for gre tunnels. You can also view route details like tunnel name, local gateway network and netmask and remote gateway network and netmask.

Syntax	Description

`route [add] [del] [ipaddress] [network/netmask] [tunnelname][local-gw] [WAN Address] [remote-gw] [remote WAN ipaddress] [local-ip] [ipaddress] [remote-ip] [ipaddress] [show]`
 	
`tunnel [add] [name] [tunnelname] [local-gw] [port] [remote-gw] [ipaddress/netmask] [local-ip] [ipaddress] [remote-ip] [ipaddress] [del] [ALL] [name] [local-gw] [Port] [remote-gw] [network/ netmask]`
	When usinf route and adding or deleting a host ipaddress type the IP address. Example, 192.168.0.1
	
	When adding or deleting a network type both the network and subnet mask. Example, 192.168.0.0/255.255.255.0
	
	For name, type the tunnel name.
	
	When using tunnel to add or delete a new tunnel, tunnelname should be the name you want to give to the tunnel.

ha

Allows configuration of certain HA parameters.

Syntax	Description
`auxiliary_system_traffic_through_dedicated_link [all] [none] [only_dynamic_interface] [show]` `load-balancing [on] [off] [show]`	Use auxiliary_system_traffic_through_dedicated_link to configure routing for system traffic sent by the auxillary. Default: pass all traffic over the dedicated link Load balancing can be turned on or off and will balance traffic between the appliances. Show will display the current HA configuration.

ipsec_route

Provides options for configuring IPsec routing.

Syntax	Description
`add [host] [ipaddress] [tunnelname] [string]` `del [net] [ipaddress/netmask] [tunnelname] [ipaddress/netmask] [tunnelname] [string] [show]`	Add or delete IPsec routes by host or network or show the current routes configured.

link_failover

You can configure a vpn as a backup link. When configured, whenever the primary link fails, traffic will be sent through the vpn connection.

Syntax	Description
`add [primarylink] [portname] [backuplink] [vpn] [gre] [tunnel] [tunnelname] [monitor PING host] [monitor TCP host] [ipaddress] [portnumber]`	Failover can be configured to use a vpn or gre tunnel. When using TCP host monitoring you will also need to specify the TCP port to be monitored. The monitoring port is not required if using ping monitoring..

restart

Restart XG Firewall.

Syntax	Description
`[all]`	Restarts XG Firewall. If configured in HA this will cause a failover.

route_precedence

Sets routing precedence. By default route lookup precedence is;

1. Policy
2. VPN
3. Static

Syntax	Description
`set [sdwan_policyroute] [static] [vpn] [show]`	When setting route precedence the first choice take highest priority when entering more than one option. Use show to display the current configuration.

shutdown

Shut down XG Firewall. There are no further options to use with this command.

system_modules

Load or unload the following system modules;

- dns
- h323
- irc
- pptp
- sip
- tftp

By default system modules are loaded.

Syntax	Description
`dns [load] [unload]`	DNS: The dns module learns the subdomains of non-local DNS traffic.
`h323 [load] [unload]`	H323: The H.323 standard provides a foundation for audio, video, and data communications across IP-based networks, including the internet.
`pptp [load] [unload]`	PPTP: Point to Point Tunneling Protocol is a network protocol that enables secure transfer of data from a remote client to a private server, creating a point to point VPN tunnel using a TCP/IP based network.
`irc [load] [unload] [port] [portname] [default]`	IRC: Internet Relay Chat is a multi-user, multi-channel chatting system based on a client-server model. A single server links with many other servers to make up an IRC network, which transports messages from one user (client) to another. In this manner, people from all over the world can talk to each other live and simultaneously. DoS attacks are very common as it is an open network and with no control on file sharing, performance is affected.

Syntax	Description
`sip [load] [unload] [portname] [default]`	SIP: Session Initiation Protocol is a signaling protocol which enables the controlling of media communications such as VoIP. The protocol is generally used for maintaining unicast and multicast sessions consisting of several media systems. SIP is a text based and TCP/IP supported application layer protocol.
`tftp [load] [unload] [portname] [default] [show]`	TFTP: Trivial File Transfer Protocol is a simple form of the file transfer protocol (FTP). TFTP uses the user datagram protocol (UDP) and provides no security features.

usb-setup-delay

Manage the waiting period for detecting the readiness of the USB drive.

Use this option when you're using firewall provisioning or zero touch configuration to set up the firewall.

Syntax	Description
`set [number] [show]`	Set the value in seconds that you wish to wait before USB devices are detected. Available values are: 1-15. The default is 3.

vlan-tag

Set VLAN tags for VLAN traffic passing through XG Firewall.

Syntax	Description
`set [interface] [interfacename] [vlanid] [number]` `reset [interface] [interfacename] [reset]`	Use these commands to set and reset VLAN IDs for an interface or to show the current configuration. Available VLAN IDs: 0-4094.

Note
From SFOS 18.0 you can configure all VLAN tagging, including for bridge interfaces, from the web admin console. If you have previously configured VLAN tags for a bridge interface from the CLI, we recommend you delete the configuration and set the tags in the web admin console instead.

wireless-controller

The wireless-controller settings let you configure parameters for attached access points including enabling troubleshooting features.

Syntax	Description

`ap_localdebuglevel [get] [set] [number]`
 	
`global [ap_autoaccept] [value] [ap_debuglevel] [number] [log_level] [number] [radius_accounting_start_delay] [number] [show] [stay_online] [number] [store_bss_stats] [number] [tunnel_id_offset] [number]`
	Use the ap_localdebuglevel and ap_debuglevel commands to configure the debugging level the device will use when logging.
	
	The level parameter must be from 0 (lowest) to 15 (highest).
	
	You can view the current debug level using the get parameter.
	
	The log_level parameter configures the logging level the device will use. When an event is logged, it is printed into the corresponding log if the log level of the message is equal or higher than the configured log level. The level parameter must be from 0 (lowest) to 7 (highest).
	
	The radius_accounting_start_delay parameter sets the delay to start the 802.1x accounting for the Wi-Fi client. You can set the delay depending on the DHCP response time. You can set a value from 0 to 60 seconds. This allows the Wi-Fi client to receive the IP address first and then start the accounting. The Wi-Fi SSO uses the framed IP address from the accounting start message and allows the user to sign in to XG Firewall.
	
	Available values for ap_autoaccept, stay_online and store_bss_stats are, 0 (off) or 1 (on).
	
	The tunnel_id_offset parameter value must be from 0 (lowest) to 65535 (highest).

`remote_pktcap [disable] [enable] [show] [AP serial number]`	The remote_pktcap command captures packets on access points when a packet capture is running. To start packet capturing, the value of the ap_debuglevel parameter must be equal to or greater than 4.
`set_channel_width [Wi-Fi interface name] [band] [Wi-Fi band] [channel_width] [number]`	You can choose Wi-Fi band 2.5GHz or 5GHz. Available channel widths are: 20 and 40 for 2.5GHz, and 20, 40, or 80 for 5GHz.

7 Device Management

Device management allows you to reset the firewall configuration to factory default, check the firmware versions currently installed, access the advanced shell, and flush reports stored on the appliance.

Device management is accessed from the main menu under Option 5 **Device Management**. The available options under Device Management are as follows:

Menu Item	Description
Reset the factory defaults	Selecting this resets the appliance to the same state in which it left the factory. All custom configurations created since deployment will be lost, including network configurations, passwords, users, groups, policies, VPN configurations and so on.
Show Firmware	List the currently installed firmware, and the previous version of firmware still available to install. Sophos XG Firewall keeps the previous firmware available on the appliance to allow for easy rollback without the need to reimage the appliance.
Advanced Shell	The advanced shell can be used to display more detailed information than the device console. It is a full Linux shell and provides full access to system internals such as databases and system services. The advanced shell should be used with caution.
Flush Device Reports	This option deletes the reports stored on the device. The appliance will restart and will be unreachable over the network for approximately 10 minutes. When flushing reports, you need to consider the time it will take, as current internet gateway connectivity will be lost until the device is back online.

8 VPN Management

VPN Management allows you to regenerate RSA keys and restart VPN services. RSA keys are used for authenticating IPsec VPN connections for both user and site-to-site connections.

The VPN Management menu allows you to restart the VPN service daemon and regenerate the RSA public/private key pair used to authenticate IPsec connections.

Menu Item	Description
Regenerate RSA Key	Use this option to regenerate the RSA public/private key pair used to authenticate IPsec connections. For endpoint connections the user needs to download the new VPN configuration from the user portal. For site-to-site connections the key at the remote location will need to be updated to use the new key pair.
Restart VPN Service	This restarts the VPN service daemon and causes all VPN tunnels to drop. If you want to restart a single VPN connection, use the GUI.

9 Reset to factory settings

Reset allows you to reset your XG Firewall to factory default settings. Resetting to factory default settings does not affect registration.

Connect to XG Firewall using an SSH client. At the prompt, enter **RESET**.

- To delete all custom configurations and reset to the default configuration, choose option 1.
- To delete all custom configuration and signatures and reset to the default configuration, choose option 2.
- To delete all custom configuration, signatures, and reports, and reset to the default configuration, choose option 3.
- To reset the administrator password to the default password, choose option 4. This option is useful when administrator has forgotten password. If XG firewall is part of HA cluster then the password of only this device will be reset.

10 Appendix A – DHCP Options (RFC 2132)

A DHCP server can provide optional configurations to the client. Sophos XG Firewall provides support to configure following DHCP Options as defined in RFC 2132.

To set the options, refer to DHCP Management section.

Option Number	Name	Description	Data Type
2	Time offset	Time offset in seconds from UTC	Four-byte numeric value
4	Time servers	N/4 time server addresses	Array of IP addresses
5	Name servers	N/4 IEN-116 server addresses	Array of IP addresses
7	Log servers	N/4 logging server addresses	Array of IP addresses
8	Cookie servers	N/4 quote server addresses	Array of IP addresses
9	LPR servers	N/4 printer server addresses	Array of IP addresses
10	Impress servers	N/4 impress server addresses	Array of IP addresses
11	RLP servers	N/4 RLP server addresses	Array of IP addresses
12	Host name	Hostname string	String
13	Boot file size	Size of boot file in 512 byte chunks	Two-byte numeric Value
14	Merit dump file	Client to dump and name of file to dump to	String
16	Swap server	Swap server addresses	IP address
17	Root path	Path name for root disk	String
18	Extension file	Patch name for more BOOTP info	String

Option Number	Name	Description	Data Type
19	IP layer forwarding	Enable or disable IP forwarding	Boolean
20	Src route enabler	Enable or disable source routing	Boolean
22	Maximum DG reassembly size	Maximum datagram reassembly size	Two-byte numeric value
23	Default IP TTL	Default IP time-to-live	One-byte numeric value
24	Path MTU aging timeout	Path MTU aging timeout	Four-byte numeric value
25	MTU plateau	Path MTU plateau table	Array of two-byte numeric values
26	Interface MTU Size	Interface MTU size	Two-byte numeric value
27	All subnets are local	All subnets are local	Boolean
28	Broadcast address	Broadcast address	IP address
29	Perform mask discovery	Perform mask discovery	Boolean
30	Provide mask to others	Provide mask to others	Boolean
31	Perform router discovery	Perform router discovery	Boolean
32	Router solicitation address	Router solicitation address	IP address
34	Trailer encapsulation	Trailer encapsulation	Boolean
35	ARP cache timeout	ARP cache timeout	Four-byte numeric value
36	Ethernet encapsulation	Ethernet encapsulation	Boolean
37	Default TCP TTL	Default TCP TTL	One-byte numeric value
38	TCP keepalive interval	TCP keepalive interval	Four-byte numeric value

Option Number	Name	Description	Data Type
39	TCP keepalive garbage	TCP keepalive garbage	Boolean
40	NIS domain name	NIS domain name	String
41	NIS server addresses	NIS server addresses	Array of IP addresses
42	NTP servers addresses	NTP servers addresses	Array of IP addresses
43	Vendor specific information	Vendor specific information	String
45	NetBIOS datagram distribution	NetBIOS datagram distribution	Array of IP addresses
46	NetBIOS node type	NetBIOS node type	One-byte numeric Value
47	NetBIOS scope	NetBIOS scope	String
48	X window font server	X window font server	Array of IP addresses
49	X window display manager	X window display manager	Array of IP addresses
50	Requested IP address	Requested IP address	IP addresses
51	IP address lease time	IP address lease time	Four-byte numeric value
52	Option overload	Overload “sname” or “file”	One-byte numeric value
53	DHCP message type	DHCP message type	One-byte numeric value
55	Parameter Request List	Parameter request list	Array of one-byte numeric values
56	Message	DHCP error message	String
57	DHCP maximum message size	DHCP maximum message size	Two-byte numeric value
58	Renew time value	DHCP renewal (T1) time	Four-byte numeric value
59	Rebinding time value	DHCP rebinding (T2) time	Four-byte numeric value
60	Client identifier	Client identifier	String

Option Number	Name	Description	Data Type
61	Client identifier	Client identifier	String
62	Netware/IP domain name	Netware/IP domain name	String
64	NIS+ V3 client domain name	NIS+ V3 client domain name	String
65	NIS+ V3 server address	NIS+ V3 server address	Array of IP addresses
66	TFTP server name	TFTP server name	String
67	Boot file name	Boot file name	String
68	Home agent addresses	Home agent addresses	Array of IP addresses
69	Simple mail server addresses	Simple mail server addresses	Array of IP addresses
70	Post office server addresses	Post office server addresses	Array of IP addresses
71	Network news server addresses	Network news server addresses	Array of IP addresses
72	WWW server addresses	WWW server addresses	Array of IP addresses
73	Finger server addresses	Finger server addresses	Array of IP addresses
74	Chat server addresses	Chat server addresses	Array of IP addresses
75	StreetTalk server addresses	StreetTalk server addresses	Array of IP addresses
76	StreetTalk directory assistance addresses	StreetTalk directory assistance addresses	Array of IP addresses
120	SIP server	The SIP server DHCP option carries a 32-bit (binary) IPv4 address used by the SIP client to locate a SIP server.	Array of IP addresses

11 Appendix B – DHCPv6 Options (RFC 3315)

A DHCP server can provide optional configurations to the client. Sophos XG Firewall provides support to configure following DHCPv6 Options as defined in RFC 3315. To set the options, refer to DHCPv6 Management section.

Option Number	Name	Description	Data Type
21	SIP servers names	The domain names of the SIP outbound proxy servers for the client to use	Alphanumeric text with/ without quotes
22	SIP servers addresses	Specifies a list of IPv6 addresses indicating SIP outbound proxy servers available to the client	Alphanumeric text with/ without quotes
24	Domain search	Specifies the domain search list the client is to use when resolving hostnames with DNS	Alphanumeric text with/ without quotes
27	NIS servers	Provides a list of one or more IPv6 addresses of NIS servers available to the client	Alphanumeric text with/ without quotes
28	NISP servers	Provides a list of one or more IPv6 addresses of NIS+ servers available to the client	Alphanumeric text with/ without quotes
29	NIS domain name	Used by the server to convey client's NIS Domain Name info to the client	Alphanumeric text with/ without quotes
30	NISP domain name	Used by the server to convey client's NIS+ Domain Name info to the client	Alphanumeric text with/ without quotes
31	SNTP servers	Provides a list of one or more IPv6 addresses of SNTP servers available to the client for synchronization	Alphanumeric text with/ without quotes

Option Number	Name	Description	Data Type
32	INFO refresh time	Specifies an upper bound for how long a client should wait before refreshing information retrieved from DHCPv6	Alphanumeric text with/ without quotes
33	BCMS server D	Broadcast and Multicast service controller domain name list option for DHCPv6	Alphanumeric text with/ without quotes
34	BCM server A	Broadcast and Multicast service controller IPv6 address option for DHCPv6	Alphanumeric text with/ without quotes