SOPHOS
Security made simple.

Sophos XG Firewall Command Reference Guide v16.5

For Sophos Customers

Document Date: April 2017

Copyright Notice

Contents

Preface

Welcome to Sophos Firewall OS Command Line Console (CLI) guide. This guide helps you configure and manage your Sophos XG Firewall command line interface. It also provides list of CLI commands that you can use from the command line interface.

The default password to access the Command Line Console is **admin**. It is recommended to change the default password immediately post deployment.

Guide Audience

This Guide describes CLI commands used to configure and manage a Sophos XG Firewall device from the Command Line Console (CLI). The Guide is written to serve as a technical reference and describes features that are specific to the Command Line Console.

This guide is primary intended for the Network Administrators and Support personnel who perform the following tasks:

- Configure System & Network
- Manage and maintain Network
- Manage various services
- Troubleshooting

This guide is intended for reference purpose and readers are expected to possess basic-to-advanced knowledge of systems networking.

Note: The Corporate and individual names, data and images in this guide are for demonstration purpose only and do not reflect the real data.

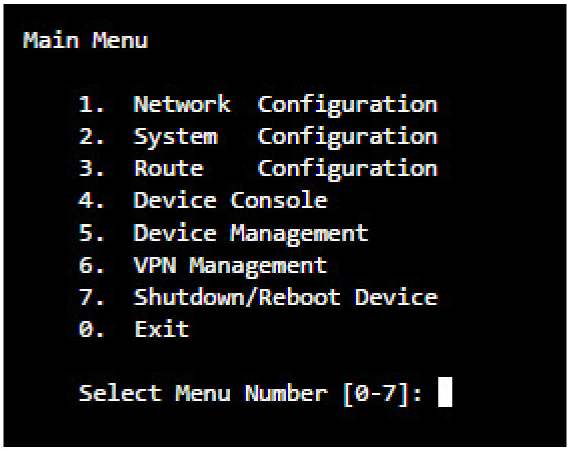
Accessing Command Line Console

There are two ways to access Sophos XG Firewall CLI:

- **Connection over Serial Console** - Physically connecting one end of a serial cable -RJ45 connector to the Console port of the device and the other end to a PC’s serial port.

  For more information, refer to the KB article titled “Setup Serial Console Connection using PuTTY".
- **Remote connection using SSH or TELNET** - Access Sophos XG Firewall CLI using a SSH client, e.g. PuTTY. IP Address of the Sophos XG Firewall is required. Start SSH client and create new connection with the following parameters:
  - **Hostname** - <Sophos XG Firewall IP Address>
  - **Username** – admin
  - **Password** – admin

On successful login, following **Main Menu** screen is displayed:



```
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 against **Select Menu Number** and press **Enter** key.

For Example, to access **Network Configuration** – press 1; to access **Device Management** – press 5.

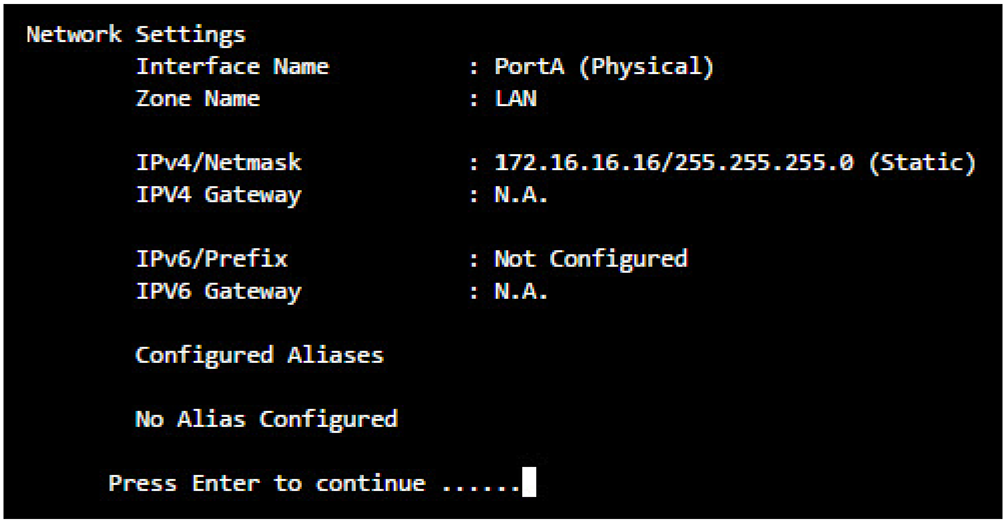
Network Configuration

Use this menu for:

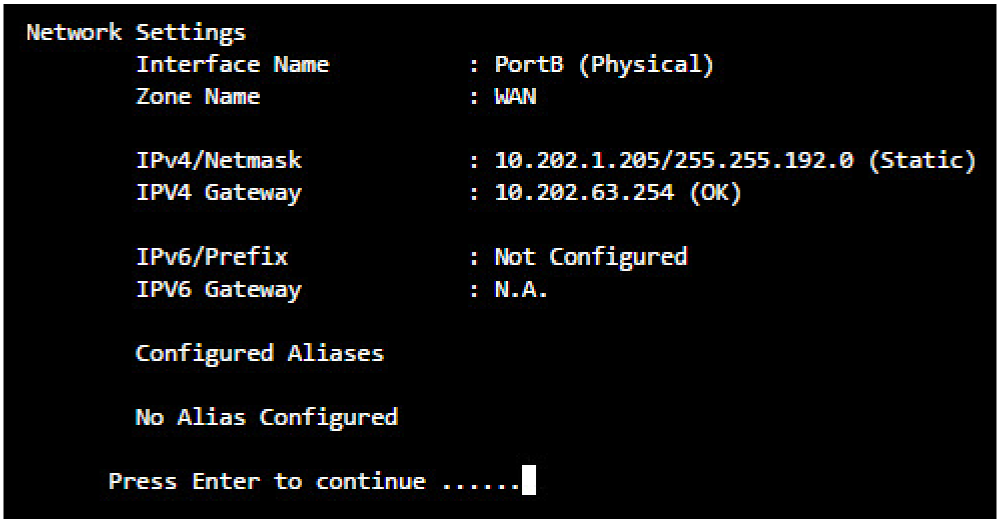
- *Configure and manage Interfaces*
- *Configure and manage DNS*

Interface Configuration

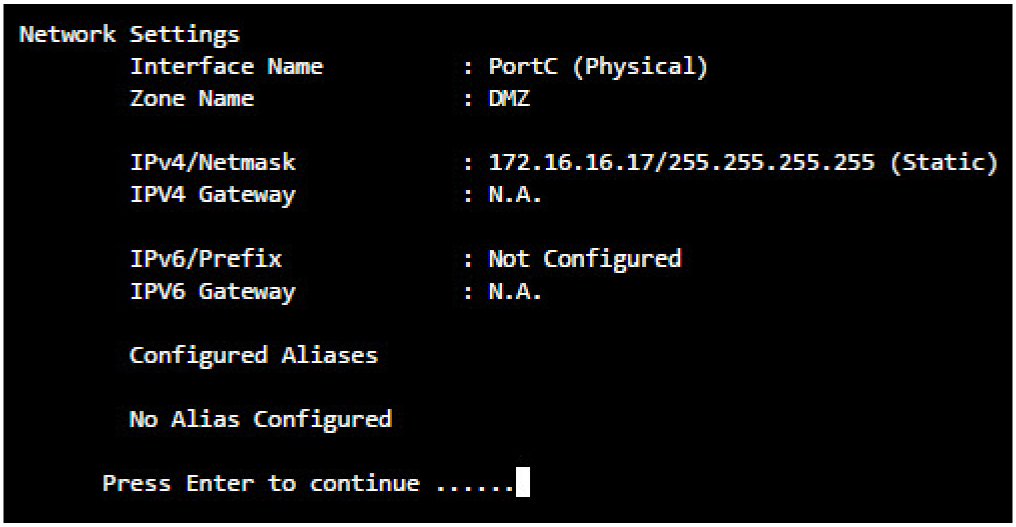
Following screen displays the current Network settings like IPv4 Address/Netmask and/or IPv6 Address/Prefix for all the Ports. In addition, it displays IPv4 Address/Netmask and/or IPv6 Address/Prefix of Aliases, if configured.



```
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            : 10.202.1.205/255.255.192.0 (Static)
        IPV4 Gateway            : 10.202.63.254 (OK)

        IPv6/Prefix             : Not Configured
        IPV6 Gateway            : N.A.

        Configured Aliases

        No Alias Configured

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

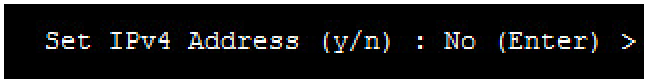


```
Network Settings
        Interface Name          : PortC (Physical)
        Zone Name               : DMZ

        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

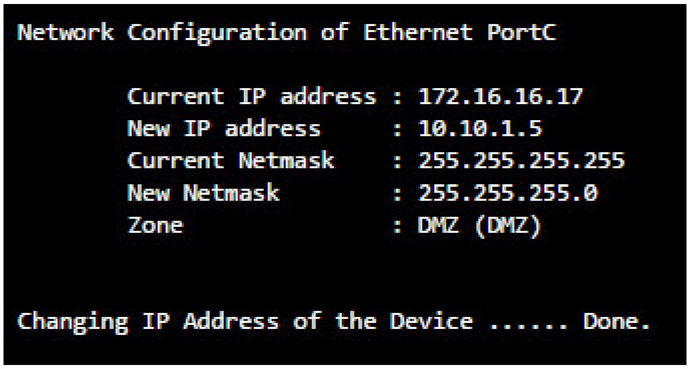
This section allows setting or modifying the Interface Configuration for any port. Following screen allows setting or modifying the IPv4 Address for any port. Type **y** and press **Enter** to set IP Address.



```
  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.
```

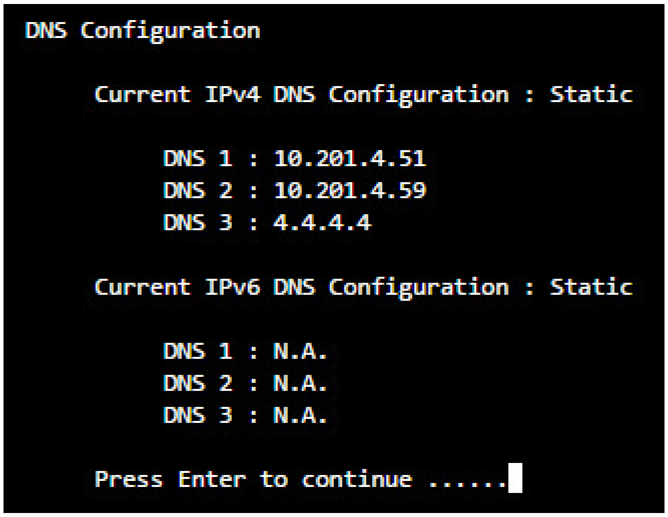
Note:

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

DNS Configuration

Configure and manage DNS

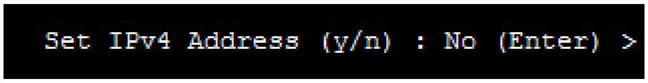
Following screen displays list of all the IPv4 and IPv6 DNS configured in the device:



```
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. Following screen allows setting or modifying the DNS configuration. Type **y** and press **Enter** to set DNS IP Address. Press just **Enter** to skip changing current DNS configuration.



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

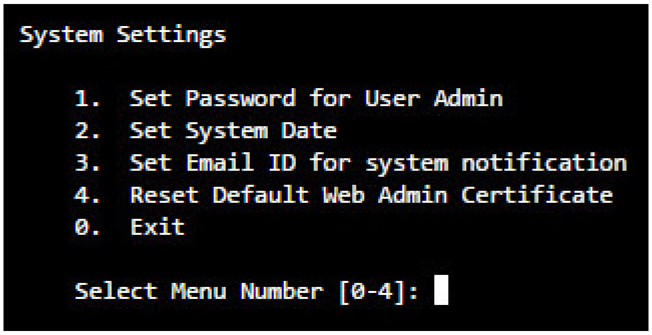
Press **Enter** to return to the **Main menu**.

Exit

Type **0** to exit from **Network Configuration** menu and return to the **Main Menu.**

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]:
```

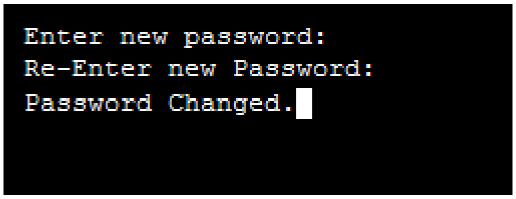
Figure 1: System Settings

Set Password for User Admin

Use to change the password of the user “admin”.

Type new password, retype for confirmation, and press **Enter**

Figure 2: Password for User Admin



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

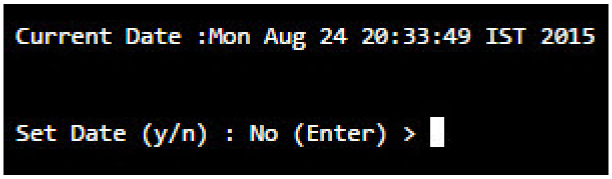
Displays successful completion message

Press **Enter** to return to the **System Settings** Menu.

Set System Date

Use to change time zone and system date.

Type **y** to set new time and press **Enter**.

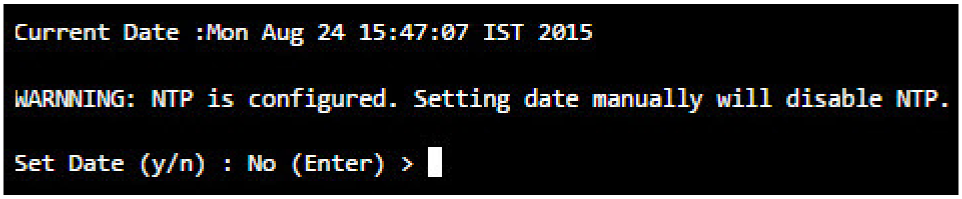


```
Current Date :Mon Aug 24 20:33:49 IST 2015


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

Figure 3: System Date

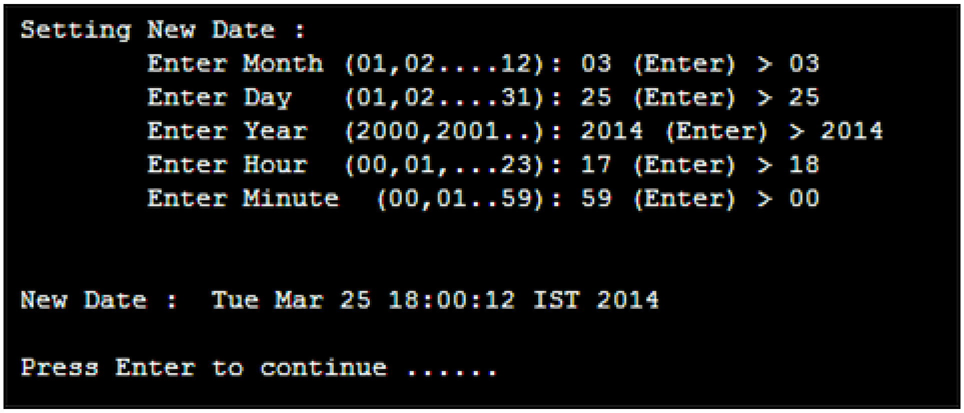
If NTP server is configured for synchronizing date and time, screen with the warning message as given below will be displayed. If you set date manually, NTP server will be disabled automatically.

Figure 4: NTP Configuration



```
Current Date :Mon Aug 24 15:47:07 IST 2015

WARNNING: NTP is configured. Setting 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 Day   (01,02....31): 25 (Enter) > 25
        Enter Year  (2000,2001..): 2014 (Enter) > 2014
        Enter Hour  (00,01,...23): 17 (Enter) > 18
        Enter Minute  (00,01..59): 59 (Enter) > 00


New Date :  Tue Mar 25 18:00:12 IST 2014

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

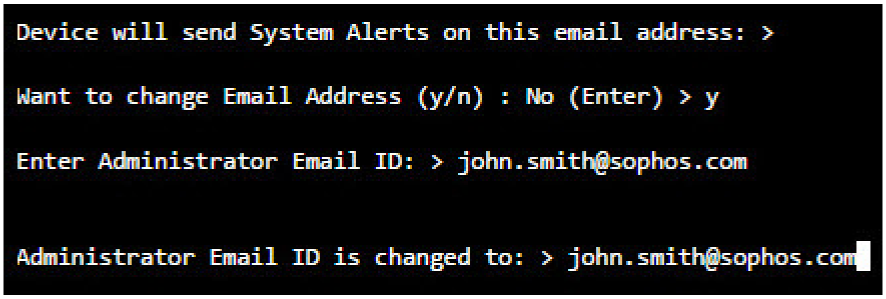
Figure 5: Setting new Date

Press Enter to return to the **System Settings** Menu.

Set Email ID 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 Email ID and press **Enter**. It displays the new Email ID.



```
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
```

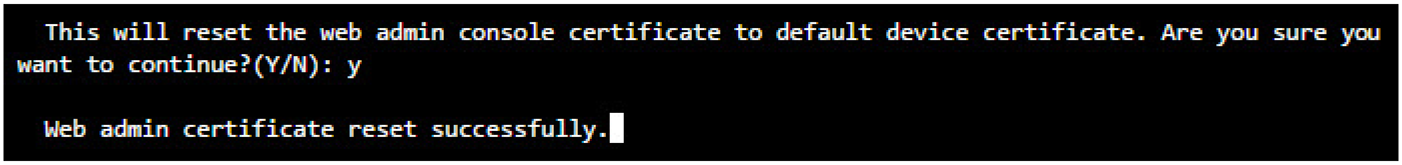
Figure 6: System Notification

Press **Enter** to return to the **System Settings** Menu.

Reset Default Web Admin Certificate

Use to reset the Web Admin certificate back to default.

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.
```

Exit

Type **0** to exit from **System Settings** menu and return to the **Main Menu.**

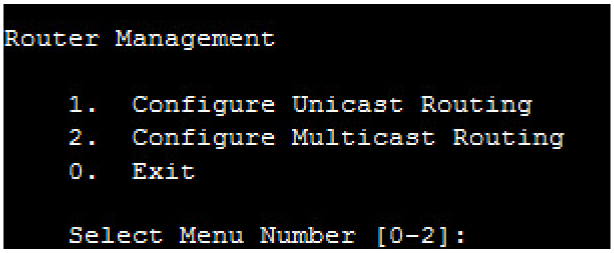
Route Configuration

Use this menu to configure:

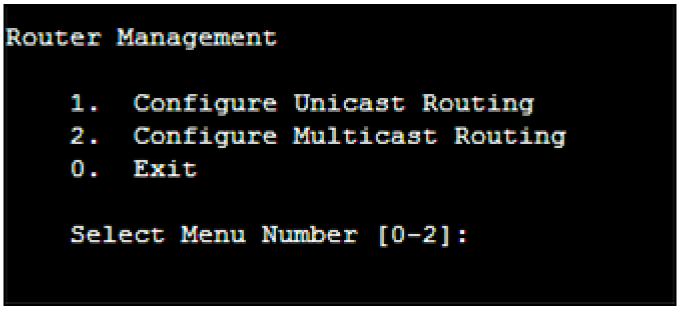
- Static routes
- RIP
- OSPF
- Enable/Disable multicast forwarding.

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

Traditionally, IP packets are transmitted in one of either two ways –Unicast (1 sender –1 receiver) or Broadcast (1 sender –everybody on the network). Multicast delivers IP packets simultaneously to a group of hosts on the network and not everybody and not just 1.



```
Router Management

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

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

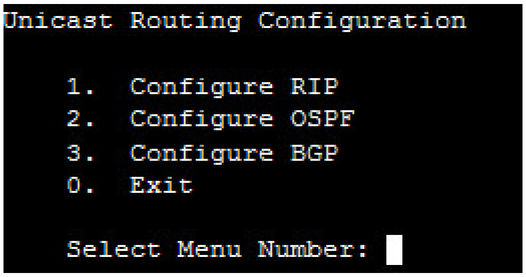


```
Router Management

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

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

Figure 7: Route Management

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

Configure RIP

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

Routing Information Protocol (RIP) is a distance-vector routing protocol documented in RFC1058. RIP uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information.

The Sophos XG Firewall implementation of RIP supports

- RIP version 1 (as described in RFC 1058)
- RIP version 2 (as described in RFC 2453
- Plain text and Message Digest 5 (MD5) authentication for RIP Version

This section covers the following topics:

- ***Configure RIP***
- ***Removing Routes***
- ***Disabling RIP***

Removing routes

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

rip(config-router)#`no network`*ip address*

Disabling RIP

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

rip(config)#`no network rip`

Execute `exit` command to return to the previous mode.

RIP Configuration Task List

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

To configure RIP, perform the steps described below:

1. Navigate to **Option 3 (Route Configuration)** > **Option 1 (Configure Unicast Routing)** > **Option 1 (Configure RIP)**
2. Enable RIP

   `rip>enable`

   Enables RIP routing process and places you in Global Configuration mode.
3. Specify a list of networks for the RIP routing process

   `rip#configure terminal`

   Enables the RIP configuration mode which places you in the Router Configuration mode and allows you to configure from the terminal.

rip(config)#`router rip`

Allows to configure and start RIP routing process.

rip(config-router)#`network` ***ip-address/subnet mask***

Specify ip-address with the subnet information

For example, if the network for 10.0.0.0/24 is RIP enabled, this would result 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 will be sent and received only through interfaces on this network.

Also, if the network of an interface is not specified, the interface will not be advertised in any RIP update. The interfaces which have addresses matching with network are enabled.

rip(config-router)#`end`

Exits from the Router Configuration mode and places you into the Enable mode.

4. Configure Authentication

rip#`configure terminal`

Enables the RIP configuration mode which places you in the Router Configuration mode and allows you to configure from the terminal.

rip(config)#`interface ifname`
rip(config-if)#`ip rip authentication mode{`text`[` string`]}`

To set authentication mode as text and set the authentication string. Defines authentication mode for the each interface. By, default, authentication is on for all the interfaces. If authentication is not required for any of the interface, it is to be explicitly disabled.

RIP Version 1 does not 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 is not required for any of the interface, use the no form of this command.

For example,

rip(config)#`interface` *A*

rip(config-if)#`ip rip authentication mode`text

rip(config-if)#`ip rip authentication string`*teststring*

rip(config)#`interface ifname`
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.

For example,

rip(config)#`interface`*A*

rip(config-if)#`ip rip authentication mode`md5key-chain *testkeychain*

rip(config)#`interface ifname`
rip(config-if)#`no ip rip authentication mode`

To disable authentication

For example, disable authentication for interface A

rip(config)#`interface` *A*

rip(config-if)#`no ip rip authentication mode`

rip(config-if)#`end`

Exits from the Router Configuration mode and places you into the Enable mode.

5. Exit to Router Management Menu

   rip(config-if)#`exit`

   Exits to the Router Management Menu.

Configure OSPF

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

OSPF is one of IGPs (Interior Gateway Protocols). Compared with RIP, OSPF can serve much more networks and 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 to an OSPF 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 OSPF network is stable, link-state advertisements between OSPF neighbors does 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 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 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.

This section covers the following topics:

- ***Configure OSPF***
- ***Removing Routes***
- ***Disabling OSPF***

Removing routes

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

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

Disabling OSPF

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

ospf(config)#`no network ospf`

OSPF Configuration Task List

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

To configure OSPF, perform the steps described below:

1. Navigate to **Option 3 (Route Configuration)** > **Option 1 (Configure Unicast Routing)** > **Option 2 (Configure OSPF)**
2. Enable OSPF

   ```
   OSPF>enable
   ```

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

   ```
   ospf#configure terminal
   ```

   Enables the OSPF configuration mode which places you in the Router Configuration mode and allows you to configure from the terminal .

   ```
   ospf(config)#router ospf
   ```

   Allows to configure and start 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 we want the interface to be in. The area - id can be an integer between 0 and 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 configuration.

   ```
   ospf(config-router)#end
   ```

   Exits from the Router Configuration mode and places you into the Enable mode.

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

   Exits to the Router Management Menu.

Configure BGP

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

Border Gateway Protocol (BGP) is a path vector protocol that is used to carry routing between routers that are in the different administrative domains (Autonomous Systems) e.g. 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 is to be configured for the zone for which the BGP traffic is to be allowed i.e. 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 particular destination network.

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

This section covers the following topics:

- *Configure BGP*
- *Removing Routes*
- *Disabling BGP*

Removing routes

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

bgp(config-router)#`no network`*ip address*

Disabling BGP

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

bgp(config)#`no network bgp`*AS number*

BGP Configuration Task List

BGP must be enabled before carrying out any of the OSPF commands.

To configure BGP, perform the steps described below:

1. Navigate to **Option 3 (Route Configuration)** > **Option 1 (Configure Unicast Routing)** > **Option 3 (Configure BGP)**
2. Enable BGP

   `bgp>enable`

   Enables BGP routing process and places you in Global Configuration mode.
3. Specify a list of networks for the BGP routing process

   `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 to configure and start OSPF routing process.AS number is the number of the local AS that Sophos Firewall unit is a member of

   bgp(config-router)#`network` *ip-address*

   Specify ip-address with the subnet information of the network to be advertised.

   The IP Addresses and network masks/prefixes of networks to advertise to BGP peers. The Sophos Firewall may have a physical or VLAN interface connected to those networks.

   bgp(config - router)#`show running - config`

   View configuration.By default, router ID is Sophos Firewall IP Address. Router ID is used to identify the Sophos 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.

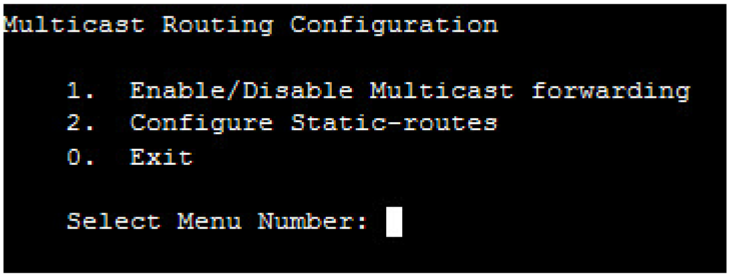
Exit

Type **0** to exit from **Unicast Routing configuration** menu and return to **Router Management**.

Configure Multicast Routing

This section covers the following topics:

- Enable/Disable Multicast forwarding
- Configure Static multicast routes
- Viewing routes
- Removing Routes



```
Multicast Routing Configuration

    1.  Enable/Disable Multicast forwarding
    2.  Configure Static-routes
    0.  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, source is required to send more than one copy of a packet or individual copy to each receiver. In such case, high-bandwidth applications like Video or Stock where data is to be send more frequently and simultaneously, uses 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 particular 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 flowing to a particular 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 (toward 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—which is not necessarily all paths.

Enable/Disable 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.

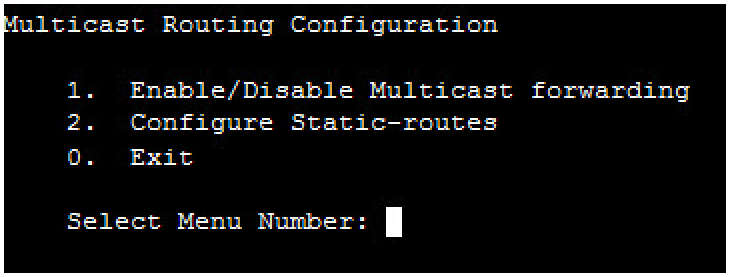
Setting up IP Multicast forwarding

Configuring multicast forwarding is two-step process:

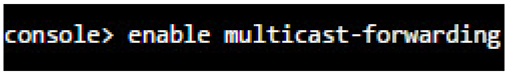
- Enable multicast forwarding (both the modes)
- Configure multicast routes (only in Gateway mode)

To enable multicast forwarding, navigate to **Option 3 (Route Configuration)** > **Option 2 (Configure Multicast Routing)** > **Option 1 (Enable/Disable Multicast forwarding)** and execute the following command:

```
console>enable multicast-forwarding
```



```
Multicast Routing Configuration

    1.  Enable/Disable Multicast forwarding
    2.  Configure Static-routes
    0.  Exit

    Select Menu Number:
```



```
console> enable multicast-forwarding
```

Configure Static multicast routes

Multicast routes cannot be added before enabling multicast forwarding.

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

console>`mroute add input-interface Port`*port number*`source-ip`*source-ip-address*`dest-ip`*destination-ip-address*`output-interface Port`*port number*

where,

- **input-interface -** interface from which the 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 destination of multicast traffic). This is the port through which traffic goes.

For example,

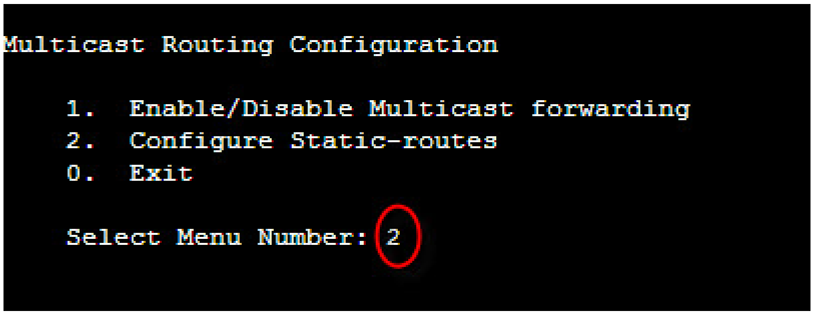
```
console>mroute add input-interface PortAsource-ip1.1.1.1dest-ip230.1.1.2output-interface PortB
```

Sophos XG Firewall will forward multicast traffic received on interface PortA from IP Address 1.1.1.1 to 230.1.1.2 through interface PortB.

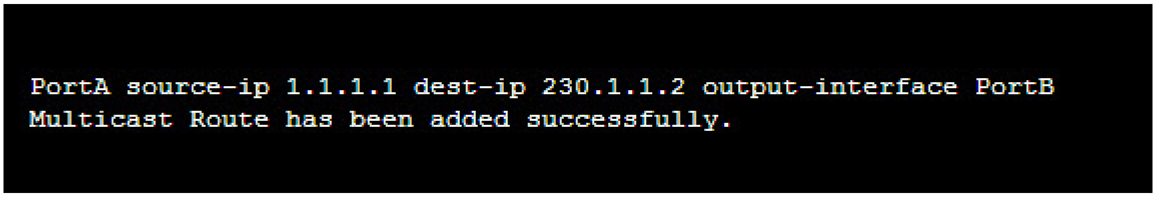
If you want to inject multicast traffic to more than one interface, you have to add routes for each destination interface. For example,

```
console>mroute add input-interface PortAsource-ip1.1.1.1dest-ip230.1.1.2output-interface PortB
```

```
console>mroute add input-interface PortAsource-ip1.1.1.1dest-ip230.1.1.2output-interface PortC
```



```
Multicast Routing Configuration

    1.  Enable/Disable Multicast forwarding
    2.  Configure Static-routes
    0.  Exit

    Select Menu Number: 2
```

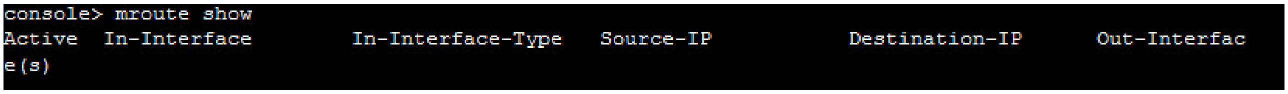


```
 PortA source-ip 1.1.1.1 dest-ip 230.1.1.2 output-interface PortB
 Multicast Route has been added successfully.
```

Viewing routes

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

```
console>mroute show
```

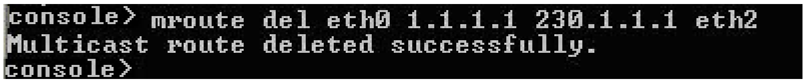


```
console> mroute show
Active  In-Interface        In-Interface-Type   Source-IP           Destination-IP      Out-Interfac
e(s)
```

Removing route

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

```
console>mroute del source-ipsource-ip-addressdestination-ipdestination-ip-address
```



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

Note:

- Source and destination interfaces cannot be same for multicast route.
- Multiple destination interfaces cannot be defined. Route manipulation per interface is required to add/ delete such routes.
- Non-Ethernet interfaces like - IPsec0, etc. are not supported.

Multicast routes over IPsec VPN tunnel

Sophos XG Firewall supports secure transport of multicast traffic over un-trusted network using IPsec/VPN connection.

It is possible to send/receive both unicast and multicast traffic between two or more VPN sites connected through 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 host shall require to be configured as a explicit host (with netmask /32) in VPN configuration.

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

- **Command:** console>`mroute add input-interface Port`*port number*`source-ip`*ipaddress*`dest-ip`*ipaddress*`output-interface Port`*port number*

  Description: To forward multicast traffic coming from a given interface to another interface

  For example:

  `mroute add input-interface Port`*A*`source-ip`*192.168.1.2*`dest-ip`*239.0.0.55*`output-interface Port`*B*
- **Command:** `mroute add input-interface Port`*port number*`source-ip`*ipaddress*`dest-ip`*ipaddress*`output-tunnel gre name`*gre tunnel name*

  Description: To forward multicast traffic coming from a given interface to GRE tunnel.

  For example:

  `mroute add input-interface Port`*A*`source-ip`*192.168.1.2*`dest-ip`*239.0.0.55*`output-tunnel gre name`*Elitecore*
- **Command:** `mroute add input-interface Port`*port number*`source-ip`*ipaddress*`dest-ip`*ipaddress*`output-tunnel IPsec`

  Description: To forward multicast traffic coming from a given interface to IPsec tunnels. Sophos XG Firewall automatically selects the appropriate tunnel to be used depending upon the Local Network and Remote Network configuration.

  For example:

  console>`mroute add input-interface Port`*A*`source-ip`*192.168.1.2*`dest-ip`*239.0.0.55*`output-tunnel IPsec`
- **Command:** `mroute add input-tunnel IPsec name`*IPsec connection name*`source-ip`*ipaddress*`dest-ip`*ipaddress*`output-interface Port`*port number*

  Description: To forward multicast traffic coming from IPsec tunnel to an interface.

  For example:

  console>`mroute add input-tunnel IPsec name`*Net2Net*`source-ip`*192.168.1.2*`dest-ip`*239.0.0.55*`output-interface Port`*B*
- **Command:** `mroute add input-tunnel IPsec name`*IPsec connection name*`source-ip`*ipaddress*`dest-ip`*ipaddress*`output-tunnel IPsec`

  Description: To forward multicast traffic coming from a given IPsec tunnel to other IPsec tunnels. Sophos XG Firewall automatically selects the appropriate tunnel to be used depending upon the Local Network and Remote Network configuration.

  For example:

console>`mroute add input-tunnel IPsec name`*Net2Net*`source-ip`*192.168.1.2*`dest-ip`*239.0.0.55*`output-tunnel IPsec`

- **Command:** `mroute add input-tunnel IPsec name`*port number*`source-ip`*ipaddress*`dest-ip`*ipaddress*`output-tunnel gre name`*gre tunnel name*

  Description: To forward multicast traffic coming from a given IPsec tunnel to GRE tunnel.

  For example:

  console>`mroute add input-tunnel IPsec name`*Net2Net*`source-ip`*192.168.1.2*`dest-ip`*239.0.0.55*`output-tunnel gre name`*Elitecore*
- **Command:** `mroute add input-tunnel gre name`*gre tunnel name*`source-ip`*ipaddress*`dest-ip`*ipaddress*`output-interface Port`*port number*

  Description: To forward multicast traffic coming from a GRE tunnel to an interface.

  For example:

  console>`mroute add input-tunnel gre name`*Elitecore*`source-ip`*192.168.1.2*`dest-ip`*239.0.0.55*`output-interface Port`*B*
- **Command:** `mroute add input-tunnel gre name`*gre tunnel name*`source-ip`*ipaddress*`dest-ip`*ipaddress*`output-tunnel gre name`*gre tunnel name*

  Description: To forward multicast traffic coming from a GRE tunnel to another GRE tunnel.

  For example:

  console>`mroute add input-tunnel gre name`*Elitecore*`source-ip`*192.168.1.2*`dest-ip`*239.0.0.55*`output-tunnel gre name`*Terminal1*
- **Command:** `mroute add input-tunnel gre name`*gre tunnel name*`source-ip`*ipaddress*`dest-ip`*ipaddress*`output-tunnel IPsec`

  Description: To forward multicast traffic coming from a given GRE tunnel to IPsec tunnels. Sophos XG Firewall automatically selects the appropriate tunnel to be used depending upon the Local Network and Remote Network configuration.

  For example:

  console>`mroute add input-tunnel gre name`*Elitecore*`source-ip`*192.168.1.2*`dest-ip`*239.0.0.55*`output-tunnel IPsec`
- **Command:** `mroute delsource-ip`*ipaddress*`dest-ip`*ipaddress*

  Description: To delete multicast route.

  For example:

  console>mroute del`source-ip`*192.168.1.2*`dest-ip`*239.0.0.55*

Note: CLI shows only static interfaces as input and output interface whereas Web Admin Console shows both, static as well as dynamic interfaces (PPPoE, DHCP).

Exit

Type **0** to exit from **Multicast Routing Configuration** menu and return to **Router Management**.

Exit

Type **0** to exit from **Router Management** menu and return to **Main Menu**.

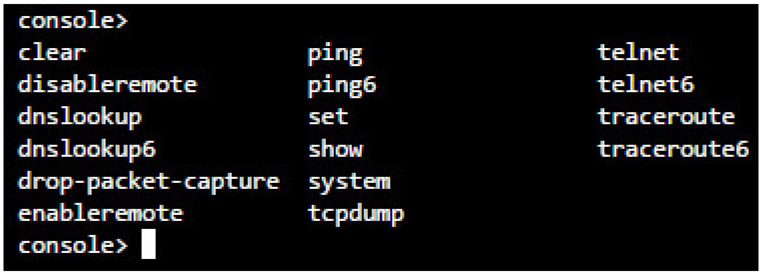
Device Console

Use to perform various checks and view logs for troubleshooting.

Generally, when using command line help, one has to remember parameters/arguments of the command and has to go to the help and check for the parameters. Users using command line for the first time face difficulty in such situations.

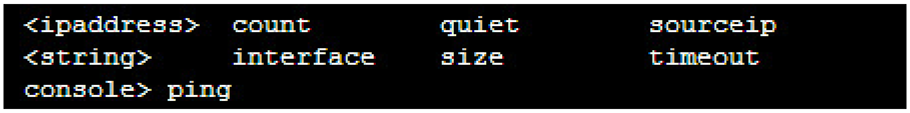
To remove the above difficulty, Sophos XG Firewall has inbuilt help at the command prompt itself.

Navigate to **Option 4 (Device Console)** and Press **Tab** or **?** to view the list of commands supported.



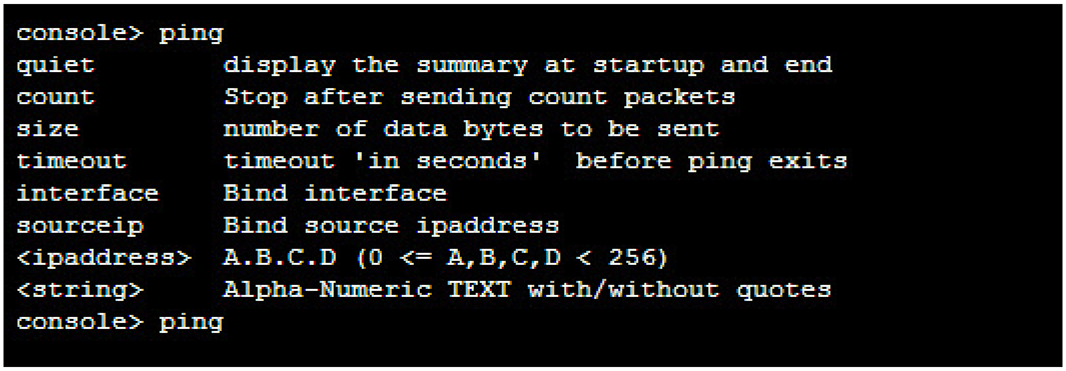
```
console>
clear                ping                 telnet
disableremote        ping6                telnet6
dnslookup            set                  traceroute
dnslookup6           show                 traceroute6
drop-packet-capture  system
enableremote         tcpdump
console> 
```

Type command and then press tab to view the list of argument(s) supported or required. For example after typing `ping` press tab, it shows what all parameters are required or allowed.



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

Type command and then press **?** to view the list of argument(s) supported with its description. For example after typing `ping` , press **?**, it shows what all parameters are required or allowed, along with description.



```
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
console> ping
```

Type **Exit** to return to the **Main menu.**

Clear

Clears the screen

Syntax

`clear`

disableremote

Disables the remote (SSH) connection, if enabled. By default, it is not allowed. Refer to enable remote to allow to establish the remote connection.

Syntax

`disableremote`

dnslookup

Query Internet domain name servers for hostname resolving

Syntax

`dnslookup[`host`{`*ipaddress*`|`*string*`}]`

Parameter list & description

Keywords & Variables	Description
`Host[`*ipaddress*`|`*String*`]`	Host to be searched
`Server[`*ipaddress*`[`host`]]`	Internet name or address of the name server

dnslookup6

Query Internet domain name servers for IPv6 hostname resolving.

Syntax

`dnslookup6[`host`{`*ipaddress*`|`*string*`}]`

Parameter list & description

Keywords & Variables	Description
`Host[`*ipaddress6*`|`*String*`]`	Host to be searched
`Server[`*ipaddress6*`[`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 errant firewall rules. You can also filter the dropped packets.

Syntax

`drop-packet-capture[`*text*`|`interface`{Port`*Port number*`}|`snaplen `{`*20-65535*`} ]`

Keywords & Variables	Description
text	BPF (Berkeley Packet Filter) Compatible Packet Filter Expression.
`interface port`*Port number*	Listen on interface
`snaplen`*20-68835*	Number of bytes to capture

BPF String Parameters

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 or port 21
specific source port	src port 21
specific destination port	dst port 21
specific host for the particular port	host 10.10.10.1 and port 21
the specific host for all the ports except SSH	host 10.10.10.1 and port not 22
specific protocol	proto ICMP, proto UDP , proto TCP

enableremote

Allows to connect to the Sophos XG Firewall remotely i.e. allows to establish remote (SSH) connection. By default, remote connection is not allowed.

Syntax

`enableremote[port`*number*`|serverip`*ipaddress*`]`

Keywords & Variables	Description
`port`*number*	Port through which the remote SSH connection can be established
`serverip`*ipaddress*	IP Address of the Sophos XG Firewall to which the remote connection can be established

ping

Sends ICMP ECHO_REQUEST packets to network hosts.

Syntax

`ping[`*ipaddress*|*string*| count | interface | quiet | size | sourceip | timeout

Keywords & Variables	Description
ipaddress	IP Address to be pinged
string	Domain to be pinged
count*number*	Stop sending packets after count
interface [Port*port ID*]	Set outgoing interface
quiet	Display the summary at startup and end
size*number*	Number of data bytes to be sent

Keywords & Variables	Description
sourceip*ipaddress*	IP Address of the source
timeout*number*	Stop sending packets and exit after specified time

ping6

Sends ICMPv6 ECHO_REQUEST packets to network hosts.

Syntax

`ping` [*ipaddress6* | | count | interface | quiet | size]

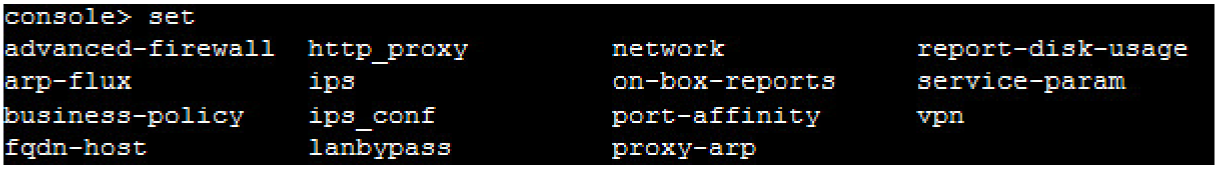
Keywords & Variables	Description
ipaddress6	IPv6 Address to be pinged
count*number*	Stop sending packets after count
interface [Port*port ID*]	Set outgoing interface
quiet	Display the summary at startup and end
size*number*	Number of data bytes to be sent

set

Navigate to **Option 4 (Device Console)** and Press **Tab** or **?** to view the list of commands supported.

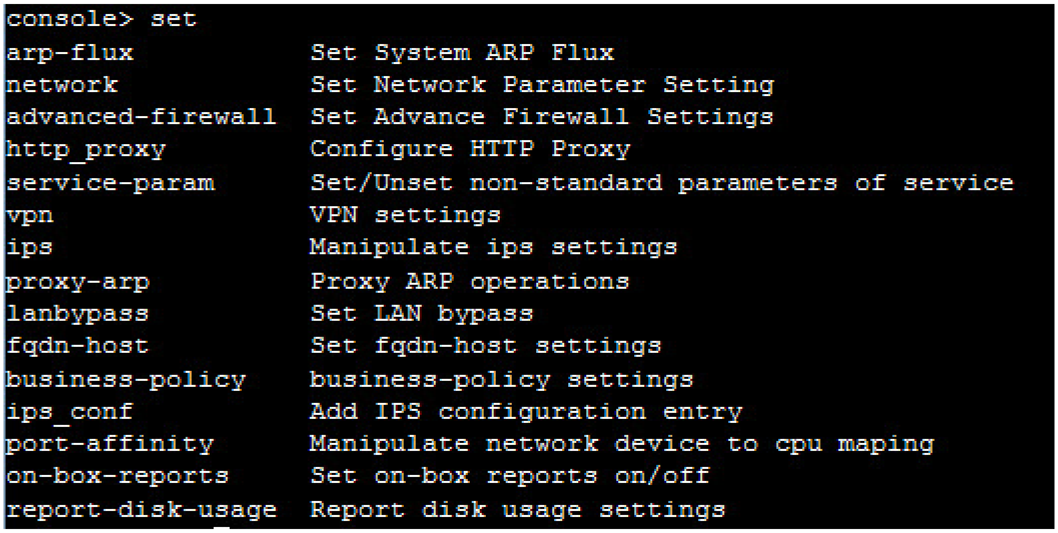
Type `set`command and then press tab to view the list of argument(s) supported or required. Use `set` command to set entities.

For example after typing `set` press tab, it shows what all parameters are required or allowed.



```
console> set
advanced-firewall  http_proxy         network            report-disk-usage
arp-flux           ips                on-box-reports     service-param
business-policy    ips_conf           port-affinity      vpn
fqdn-host          lanbypass          proxy-arp
```

Type command and then press **?** to view the list of argument(s) supported with its description. For example after typing `set` , press **?**, it shows what all parameters are required or allowed, along with description.



```
console> set
arp-flux            Set System ARP Flux
network             Set Network Parameter Setting
advanced-firewall   Set Advance Firewall Settings
http_proxy          Configure HTTP Proxy
service-param       Set/Unset non-standard parameters of service
vpn                 VPN settings
ips                 Manipulate ips settings
proxy-arp           Proxy ARP operations
lanbypass           Set LAN bypass
fqdn-host           Set fqdn-host settings
business-policy     business-policy settings
ips_conf            Add IPS configuration entry
port-affinity       Manipulate network device to cpu maping
on-box-reports      Set on-box reports on/off
report-disk-usage   Report disk usage settings
```

advanced_firewall

`advance_firewall` [bypass-stateful-firewall-config | icmp-error-message | tcp-appropriate-byte-count | fragmented-traffic | tcp-est-idle-timeout | ftpbounce-prevention | tcp-frto | midstream-connection-pickup | tcp-selective-acknowledgement | strict-icmp-tracking | tcp-seq-checking | strict-policy | tcp-timestamp | sys-traffic-nat | tcp-window-scaling | udp-timeout-stream]

- **bypass-stateful-firewall-config**

  Add host or network when the outbound and return traffic does not always traverse through Sophos XG Firewall.

  `bypass-stateful-firewall-config` [add { dest_host *ipaddress* | dest_network *ipaddress* | source_host *ipaddress* | source_network *ipaddress* } | del { dest_host *ipaddress* | dest_network *ipaddress* | source_host *ipaddress* | source_network *ipaddress* }
- **icmp-error-message**

  icmp-error-message{allow| deny}

  Allow or deny ICMP error packets describing problems such as network/host/port unreachable, destination network/host unknown and so on.
- **tcp-appropriate-byte-count**

  Controls Appropriate Byte Count (ABC) settings. ABC is a way of increasing congestion window (cwnd) more slowly in response to partial acknowledgments.

  `tcp-appropriate-byte-count` [on | off]
- **fragmented-traffic**

  Allow or deny fragmented traffic. IP Fragmentation is the process of breaking down an IP datagram into smaller packets to be transmitted over different types of network media and then reassembling them at the other end. While Fragmentation is an integral part of the IP protocol, there are numerous ways in which attackers have used fragmentation to infiltrate and cause a denial of service to networks.

  `fragmented-traffic` [allow | deny]
- **tcp-est-idle-timeout**

  Set Idle Timeout between 2700 - 432000 seconds for TCP connections in the established state

  `tcp-est-idle-timeout` [*2700 - 432000*]
- **ftpbounce-prevention**

  Prevent FTP Bounce attack on FTP control and data connection. An FTP Bounce attack is when an attacker sends a PORT command to an FTP server, specifying the IP Address of a third party instead of the attacker's own IP Address. The FTP server then sends data to the victim machine.

```
ftpbounce-prevention [ control | data ]
```

- **tcp-frto**

  tcp-frto Off – Disables 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.

  ```
  tcp-frto [ on | off ]
  ```

- **midstream-connection-pickup**

  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 the deployment modes.

  ```
  midstream-connection-pickup [ on | off ]
  ```

- **tcp-selective-acknowledgement**

  tcp-selective-acknowledgement Off – Disables selective acknowledgement. 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-selective-acknowledgement [ on | off ]
  ```

- **strict-icmp-tracking**

  Allow or Drop ICMP reply packets. Setting this option ‘on’ drops all ICMP reply packets.

  ```
  strict-icmp-tracking [ on | off ]
  ```

- **tcp-seq-checking**

  Every TCP packet contains a Sequence Number (SYN) and an Acknowledgement 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 in invalid sequence numbers and expect an acknowledgement. For this reason, Sophos Firewall offers the ability to disable this feature. Default – ON

  ```
  tcp-seq-checking [ on | off ]
  ```

- **strict-policy**

  When strict policy is off, strict firewall policy is disabled.

  ```
  strict-policy [ on | off ]
  ```

- **tcp-timestamp**

  tcp-timestamp Off – Disables timestamps. Timestamp is an TCP option used to calculate the Round Trip Measurement in a better way than the retransmission timeout method.

  ```
  tcp-timestamp [ on | off ]
  ```

- **sys-traffic-nat**

  ```
  sys-traffic-nat [ add { destination ipaddress } | delete { destination ipaddress } | fragmentedtraffic {
  allow | deny } ]
  ```

- **tcp-window-scaling**

  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.

  ```
  tcp-window-scaling [ on | off ]
  ```

- **udp-timeout-stream**

  Set up UDP timeout value between 30 - 3600 seconds for established UDP connections.

```
udp-timeout-stream [ 30 - 3600 ]
```

Default - 60 Seconds

arp-flux

ARP flux occurs when multiple ethernet adaptors, 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.

```
arp-flux[ on|off]
```

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 interface when Sophos XG Firewall has multiple physical connections to the same medium or broadcast domain.

business-policy

Enable/disable mail notification for Fail-over of your application server.

```
business-policy application-server[ failover {mail- notification (enable|disable) } ]
```

fqdn-host

Cache 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

```
fqdn-host[ cache-ttl number | dns-reply-ttl ]
```

dns-reply-ttl – use the ttl value in DNS reply packet as cache-ttl

Idle Timeout

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

```
fqdn-host[ idle-timeout { number | default } ]
```

http_proxy

Set proxy parameters

```
http_proxy [ add_via_header {on|off} | relay_invalid_http_traffic {on|off} | core_dump {on|off} ]
```

ips

Configure IPS settings

Syntax

`ips` [enable_appsignatures | http_response_scan_limit | ips-instance | ips_mmap | lowmem-settings | maxpkts | maxsesbytes-settings | packet-streaming]

Options

`enable_appsignatures` [on | off]

`http_response_scan_limit` <*number*>

Specify maximum file size (in KB) for scanning. Files exceeding this size received through HTTP will not be scanned.

Default: 64 KB

`ips-instance` [add | apply | clear]

Manipulate number of IPS process instances created by init process

add – Add IPS instance to the init list

apply – Start IPS processes as given in the list

clear – Clear IPS list for init process

`ips_mmap` [on | off]

Enable mmap to optimize RAM usage, especially in low-end devices.

on – enable ips mmap

off – disable ips mmap

Default - on

`lowmem-settings` [on | off]

Set whether low memory settings to be applied or not.

Low memory settings are applied in case of system having memory issues.

on – enable low memory settings

off – disable low memory settings

`maxpkts`[<*number*> | all | default]

Set number of packets to be sent for Application Classification

number – any number above 8

all - pass all of the session packets for application classification

default - pass first 8 packets of the session of each direction for application classification (total 16)

`maxsesbytes-settings` [update <*number*>]

maxsesbytes-settings allows you to set the maximum allowed size. Any file beyond the configured size is bypassed and not scanned.

Update – set the value for maximum bytes allowed per session

`packet-streaming`[on | off]

Set whether packet streaming is to be allowed or not.

packet-streaming is used to restrict streaming of packets in situations where system is experiencing memory issues.

on - Enables packet streaming.

off - disable packet streaming.

ips_conf

Use this to add, delete or edit an existing IPS configuration entry.

`on-box-reports` [add { key *text* value *text* } | del { key *text* } | update { key *text* value *text* }]

lanbypass

Enable/disable LAN Bypass

`lanbypass` [off | on]

network

`network` [interface-speed <*port*> | interfaces | macaddr <*port*> | mtu-mss<*port*> | lag-interface | static-route | static-route6]

interface-speed – Shows current interface speed settings.

interfaces – Shows all network interfaces configuration

Note:

One or more LAG interface must be configured in the device to be able to view its configuration using the SHOW command from CLI.

macaddr – Shows original and overrided mac address of interface.

on-box-reports

Generate on-box reports.

Default – ON

`on-box-reports` [off | on]

port-affinity

Configure Port Affinity settings. Administrator can manually assign/unassign a CPU Core to a particular Interface. Once configured, all the network traffic for the Interfaces is handled by the assigned CPU Cores.

`port-affinity` [add { port *Port Name* (bind-with *cpu* | start-with *cpu* | cpu *CPU Core*) } | defsetup | del { port *Port Name* } | fwonlysetup]

By default, your device is shipped with the factory-default Port Affinity settings.

Note:

- CPU Cores can be assigned to the binded Interfaces only.
- Port-affinity is not supported with ‘Legacy Network Adaptors’, when Virtual Security appliance is deployed in Microsoft Hyper-V.

proxy-arp

Add or delete proxy ARP

```
proxy-arp[ add { interface Port port name ( dst_ip ipaddress | dst_iprange < from_ip ipaddress | to_ip
ipaddress > ) } | del { interface Port port name ( dst_ip ipaddress | dst_iprange < from_ip ipaddress | to_ip
ipaddress > ) } ]
```

report-disk-usage

Set Watermark in percentage for the Report Disk usage. Watermark represents the allowed level up to which data can be written to the Report Disk.

Watermark range: 60 – 85

Default – 80%

```
report-disk-usage [ watermark { number | default } ]
```

In case the Report Disk usage increases more than the set Watermark level, administrator is shown a warning message saying the Report Disk usage is more than the set Watermark level.

In case the Report Disk usage increases more than 90%, no additional data will be allowed to be written to the Report Disk until the Report Disk usage is reduced to the set Watermark level.

service-param

By default, Sophos XG Firewall inspects all inbound HTTP, HTTPS, FTP, SMTP/S, POP and IMAP traffic on the standard ports. “service-param” enables inspection of HTTP, HTTPS, FTP, SMTP/S, POP, IMAP, IM – MSN and Yahoo traffic on nonstandard ports also.

```
service-param[ FTP { add port number | delete port number } | HTTP { add | delete } | HTTPS (
deny_unknown_proto { on | off } ) | IMAP { add | delete } | IM_MSN { add | delete } | IM_YAHOO { add
| delete } | POP { add | delete } | SMTP { add | delete | faliure_notification ( on | off ) | notification-port (
add < port port_value > ) | strict-portal-check ( on | off ) } | SMTPS { add ( port port_value ) | delete ( port
port_value ) | invalid-certificate ( allow | block ) } ]
```

- add Port < port name > – enable inspection for a specified port number.
- delete Port < port name > - disable inspection for a specified port number.
- deny_unknown_proto - Allow/deny traffic not following HTTPS protocol i.e. invalid traffic through HTTPS port
- Default – ON
- invalid_certificate - If you enable HTTPS or SMTPS scanning, you need to import SecurityAppliance_SSL_CA certificate in your browser for decryption of SSL traffic, otherwise your browser will always give a warning page when you try to access any secure site. “Invalid Certificate error” warning appears when the site is using an invalid SSL certificate. Sophos XG Firewall blocks all such sites. Use this command, if you want to allow access to such sites.

Note: For SMTPS Scanning - CA certificate used by Sophos XG Firewall to sign certificate should be added in the certificate store of your Email client.

vpn

Set authentication protocol for l2tp and pptp connections. For l2tp, Maximum Transmission Unit (MTU) can be configured.

MTU range: 576 – 1460

Default: 1410

```
vpn[ l2tp { authentication ( ANY | CHAP | MS_CHAPv2 | PAP ) | mtu ( number ) } | pptp { authentication
( ANY | CHAP | MS_CHAPv2 encryption < NONE | SOME | STRONG | WEAK > | PAP ) } ]
```

Partition Reset support

File System Integrity check verifies all the partitions for corruption. Check is enabled automatically when the device goes in failsafe mode.

It is required to flush the partitions if device comes up in failsafe mode even after the integrity check. RESET command is extended to include commands to flush partitions. With these commands, administrator can reset the config, signature and report partition. Entire data will be lost, as the partition will be flushed.

Integrity check repairs the partition while resetting partition removes entire data from the partition.

Command Usage:

When you type RESET at the Serial Console Password prompt, menu with 3 options is provided:

- Reset configuration.
- Reset configuration and signatures.
- Reset configuration, signatures and reports.

show

Displays various parameters configured for firewall.

`advance_firewall` [arp-flux | business-policy | country-host | date | fqdn-host | http_proxy | ips-settings | ips-config | lan-bypass | lcd | network | on-box-reports | port-affinity | pppoe | proxy-arp | report-disk-usage | service-param | vpn]

- **advanced-firewall**

  Shows firewall configuration.

  1. Strict policy
  2. FtpBounce Prevention
  3. TCP Conn. Establishment Idle Timeout
  4. UDP Timeout Stream
  5. Fragmented Traffic Policy
  6. Midstream Connection Pickup
  7. TCP Seq Checking
  8. TCP Window Scaling
  9. TCP Appropriate Byte Count
  10. TCP Selective Acknowledgements
  11. TCP Forward RTO-Recovery [F-RTO]
  12. TCP TIMESTAMPS
  13. Strict ICMP Tracking
  14. ICMP error message

system

You can perform following SF system configurations using system command:

- Allow access to SF services
- Application classification/categorization
- Enable authentication
- Configure VLAN tags
- Configure wireless protection and WWAN
- Bridge management
- DHCP and DHCPv6 management
- Device diagnostics
- Firewall acceleration configuration
- HA

- Manage static IPsec routes, link failover over VPN, route precedence, system modules

appliance_access

To override or bypass the configured Device Access settings and allow access to all the Sophos Firewall services.

Default –Disabled.

Enable and disable event will be logged in Admin Logs.

Syntax

appliance_access [disable | enable | show]

Options / Keywords & Variables

Disable - Disable to re-apply Device Access.

Enable - Enable Device Access.

Show - Show Device Access Status.

application_classification

```
application_classification[ microapp-discovery { on | off | show } | on | off | show ]
```

If application classification is enabled, traffic is categorized on the basis of application, and traffic discovery live connections that is displayed on Admin Console, is displayed based on the 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, traffic is categorized on port-based applications, and traffic discovery based on applications does not display any signature-based application.

Default – ON

Note: application_classification must be ON to enable Micro App_Discovery.

auth

```
auth[cta|thin-client]
```

Manage cta options

```
auth[cta{collector|enable|unauth-traffic|disable|show|vpnzonenetwork}]
```

Enable authentication: transparent authentication, thin client authentication for AD users

- **Manage collector options**

  cta - Add and remove CTA collector IP Address for clientless Single Sign On configuration.

  - To add a collector in new group

    ```
    auth cta[collector{addcollector-ip collector-port port create-new-collector-group)}]
    ```
  - To add a collector in an existing collector group

    ```
    auth cta[collector{addcollector-ip collector-port port collector-groupgroup-number)}]
    ```
  - To delete a collector IP

    ```
    dhcp[dhcp-options {binding show {dhcpname dhcp server name)}]
    ```
- **To enable cta**

  ```
  auth cta[ enable]
  ```
- **Manage drop period for unauthenticate traffic options**

```
auth cta[unauth-trafficdrop-period]
```

  - To configure the default drop period for unauthenticated traffic

    ```
    auth cta[unauth-trafficdrop-perioddefault]
    ```

  - To manually configure the drop period for unauthenticated traffic

    ```
    auth cta[unauth-trafficdrop-period0-120]
    ```

- **To disable cta**

  ```
  auth cta[disable]
  ```

- **To display all cta configurations**

  ```
  auth cta[show]
  ```

- **Manage VPN zone Network options**

  ```
  auth cta[vpnzonenetwork]
  ```

  - To add source-network IP address

    ```
    auth cta[vpnzonenetwork{add source networkipaddress}]
    ```

  - To delete source-network IP Address

    ```
    auth cta[vpnzonenetwork{delete source networkipaddress}]
    ```

Manage thin-client options

thin-client – add and remove citrix server IP Address for thinclient support.

```
auth[thin-client{add|delete|show}]
```

- **To add a thin-client IP Address**

  ```
  auth[thin-client{addcitrix-ipipaddress}]
  ```

- **To delete a thin-client IP Address**

  ```
  auth[thin-client{deletecitrix-ipipaddress}]
  ```

- **To add a thin-client IP Address**

  ```
  auth[thin-client{show}]
  ```

bridge

Use the bypass - firewall - policy command to configure policy for unknown network traffic (non - routable traffic) on which no Security Policy is applied

```
bridge[bypass-firewall-policy{unknown-network-traffic}|static-entry]
```

Manage bypass-firewall-policy options

```
bypass-firewall-policy[unknown-network traffic{allow|drop|show}]
```

- **To allow unknown network traffic**

  allow - allow unknown network traffic to pass through system

  ```
  bypass-firewall-policy[unknown-network traffic{allow}]
  ```

- **To drop unknown network traffic**

  drop - do not allow unknown network traffic to pass through system

  ```
  bypass-firewall-policy[unknown-network traffic{drop}]
  ```

- **To view bypass status for unknown network traffic**

  show -display unknown traffic bypass status `bypass-firewall-policy` [unknown-network traffic { show }]

Manage static-entry options

Use static - entry fo r Static MAC configuration in Bridge Mode. Bridge forwarding table stores all the MAC addresses learned by the Bridge and is used to determine where to forward the packets.

`static-entry` [add | delete | show]

add -add a new static entry in bridge MAC table.

delete - delete an existing static entry from bridge MAC table

show - show all static entries in bridge table

- **To add a static entry**

  `staticentry` [add { interface (*bridge name* : *Port*) macaddr*MAC address*priority (dynamic | static) }]

dhcp

Sophos XG Firewall supports configuration of DHCP options, as defined in RFC 2132. DHCP options allow users 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.

`dhcp` [dhcp-options | lease-over-IPsec | one-lease-per-client | static-entry-scope]

Manage DHCP options

`dhcp` [dhcp-options { add | binding | delete | list }]

- **To add a custom DHCP option**

  `dhcp`[dhcp-options { add optioncode *1-255* optionname *String* optiontype { array-of | one-byte | two-byte | four-byte | ipaddress | string | boolean }]
- **To delete a custom DHCP option**

  `dhcp` [dhcp-options { delete optionname *optionname* }]
- **To display all configurable DHCP option**

  `dhcp` [dhcp-options { list }]
- **To manage additional options for DHCP Server**
  - Add option to DHCP Server

    `dhcp` [dhcp-options { binding add (dhcpname *DHCP Server name* optionname *DHCP options* value *text*) }]
  - Delete option from DHCP Server

    `dhcp` [dhcp-options { binding delete { dhcpname *dhcp server name*) }]
  - Show options assigned to DHCP Server

    `dhcp` [dhcp-options { binding show { dhcpname *dhcp server name*) }]

Manage IP Lease over IPsec

- To disable IP Lease over IPsec for all DHCP Servers (Default Value)

  `dhcp` [lease-over-IPsec { disable }]
- To enable IP Lease over IPsec for all DHCP Servers

  `dhcp` [lease-over-IPsec { enable }]
- To display all IP Lease over IPsec configuration

`dhcp` [lease-over-IPsec { enable }]

Manage IP lease for Client

`dhcp`one-lease-per-client { enable | disable | show}]

- To enable one lease per client for all DHCP servers

  `dhcp` [one-lease-per-client { enable }]
- To disable one lease per client for all DHCP servers

  `dhcp` [one-lease-per-client { disable }]
- To view one lease per client configuration

  `dhcp` [one-lease-per-client { show }]

Manage scope of Static lease

`dhcp` static-entry-scope { global | network | show }

dhcpv6

Sophos XG Firewall supports configuration of DHCPv6 options, as defined in RFC 3315. DHCPv6 options allow users 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.

`dhcpv6` [dhcpv6-options]

Manage DHCPv6 options

`dhcpv6` [dhcpv6-options { add | binding | delete | list }]

- **To add a custom DHCPv6 option**

  `dhcpv6`[dhcpv6-options { add optioncode *1-65535* optionname *String* optiontype { array-of | one-byte | two-byte | four-byte | ipv6address | string | boolean }]
- **To delete a custom DHCPv6 option**

  `dhcpv6` [dhcpv6-options { delete optionname *optionname* }]
- **To display all configurable DHCPv6 option**

  `dhcpv6` [dhcpv6-options { list }]
- **To manage additional options for DHCPv6 Server**
  - Add option to DHCPv6 Server

    `dhcpv6` [dhcpv6-options { binding add { dhcpname *DHCPv6 Server name* optionname *DHCP options* value *text*) }]
  - Delete option from DHCPv6 Server

    `dhcpv6` [dhcpv6-options { binding delete { dhcpname *dhcpv6 server name*) }]
  - Show options assigned to DHCPv6 Server

    `dhcpv6` [dhcpv6-options { binding show { dhcpname *dhcpv6 server name*) }]

diagnostics

Various tools to check device health.

Syntax

`diagnostics` [ctr-log-lines | purge-old-logs | subsystems | purge-all-logs | show | utilities]

1. To take last n lines for Consolidated Troubleshooting Report (CTR)

   `diagnostics` [ctr-log-lines <*250-10000*>]

   ctr-log-lines – set number of lines to display in Consolidated Troubleshooting Report (CTR) log file.

   Default – 1000.
2. To truncate all rotated logs

   `diagnostics` [purge-old-logs]

   purge-old-logs – purge all rotated log files
3. To configure Subsystems

   `diagnostics` [subsystems { Access-Server | Bwm | CSC | IM | IPSEngine | LoggingDaemon | Msyncd | POPIMAPDaemon | Pktcapd | SMTPD | SSLVPN | SSLVPN-RPD | WebProxy | Wifiauthd }]

   subsystems – configure each subsystem individually.

   Configuration options include: debug, purge-logs and purge-oldlogs

   Manage Access Server options

   `diagnostics` [subsystems { Access-Server (debug | purge-log | purge-old-log) }]

   Enable/Disable Access Server debug

   `diagnostics` [subsystems { Access-Server (debug <on | off> }]

   To truncate all logs

   `diagnostics` [purge-log]

   To truncate all rotated logs

   `diagnostics` [purge-old-log]

   Manage CSC options

   `diagnostics` [subsystems { CSC (debug | purge-log | purge-old-log) }]

   Enable/Disable CSC debug mode

   `diagnostics` [subsystems { CSC (debug <on | off> }]

   To truncate all logs

   `diagnostics` [purge-log]

   To truncate all rotated logs

   `diagnostics` [purge-old-log]

   Note:

   - Here we are showing management options for two subsystems only since all except CSC offers same three

     configuration options i.e. to enable/disable debug mode, to truncate all logs and to purge old logs.
   - In case of CSC, the debug mode differs a little. In all the subsystems administrator has an option to enable/disable

     debug mode, while in CSC the debug mode can only be toggled.
4. To truncate all logs

   `diagnostics` [purge-all-logs]
5. To view diagnostic statistics

`diagnostics` [show { cpu | interrupts | syslog | version-info | ctr-log-lines | memory | sysmsg | disk | subsystem-info | uptime }]

6. To view utilities statistics

   `diagnostics` [utilities { arp | dnslookup6 | route | bandwidthmonitor | drop-packet-capture | route6 | connections | ping | traceroute | dnslookup | ping6 | traceroute6 }]

   Note:

   - SSLVPN option will be visible in all the models except CR15i and CR15wi models.
   - Wifiauthd option will be visible in Local Wi-Fi Devices only.
   - Msyncd option will be visible in all the models except CR15i, CR10iNG, CR10wiNG, CR 15iNG, CR15wi, CR

     15wiNG, CR25wi, CR25wiNG/6P CR35wi and CR35wiNG models.

discover-mode

Use to configure one of more interfaces of Sophos XG Firewall in Discover Mode.

`discover-mode` [tap { (add *Port_Name* | delete *Port_Name*) | show }]

- add - configure an interface in Discover mode

  For Example: `discover-mode` [tap { add *Port-D* }]

- delete - remove an interface from Discover mode

  For example: `discover-mode` [tap { delete *Port-D* }]
- show - use to view ports configured in Discover mode, if any

firewall-acceleration

Use to enable Firewall Acceleration that uses advanced data-path architecture that enables Sophos XG Firewall with faster processing of data packets for known traffic.

`Firewall-acceleration` (enable | disable | show)

- enable -use to enable firewall acceleration. This is the default option.
- disable -use to disable firewall acceleration.
- show -use to view status of firewall acceleration configuration.

fsck-on-nextboot

Check file system integrity of all the partitions. Turning ON this option forcefully checks the file system integrity on next device reboot. By default, check is OFF but whenever device goes in failsafe due to following reasons, this check is automatically turned ON:

- Unable to start Config/Report/Signature Database
- Unable to Apply migration
- Unable to find the deployment mode

`fsck-on-nextboot` [off | on | show]

Once the check is turned ON, on the boot, all the partitions will be checked. The check will be turned OFF again on the next boot.

If the option is ON and the device boots up due following reasons, then file system check will not be enforced and option will be disabled after boot:

- Factory reset
- Flush Device Report

gre

`gre` [route | tunnel]

Configure, delete, set TTL and status of gre tunnel, view route details like tunnel name, local gateway network and netmask, remote gateway network and netmask.

For GRE Tunnel

`gre` [tunnel { add | del | set | show }]

1. To add a GRE Tunnel

   `gre` [tunnel { add (name *tunnel-name* local-gw *WAN_Interface* remote-gw *Remote_WAN_IP* local-ip *LcalIP* remote-ip *RemoteIP*) }]
2. To list GRE Tunnel

   `gre` [tunnel { show (local-gw | name) }]
3. To set TTL for GRE Tunnel

   `gre` [tunnel { set (name *tunnel-name* ttl *ttlvalue*) }]
4. To set state of GRE Tunnel

   `gre` [tunnel { set (name *tunnel-name* state < *enable* | disable >) }]
5. To delete GRE Tunnel

   a. `gre` [tunnel { del (name *tunnel-name* local-gw *WAN_Interface* remote-gw *Remote_WAN_IP*) }]
   b. `gre` [tunnel { del (name *tunnel-name*) }]
   c. `gre` [tunnel { del (All) }]
6. To check status of GRE Tunnel

   `gre` [tunnel { show (name *tunnel-name* local-gw *WAN_Interface* remote-gw *Remote_WAN_IP*) }]

Unicast Routing Support in GRE

`gre` [route { add | del | show }]

1. To add an Unicast Route for Network

   `gre` [route { add (net *network* tunnelname *tunnel-name*) }]
2. To add an Unicast Route for Host `gre` [route { add (host *IP* tunnelname *tunnel-name*) }]
3. To delete an Unicast Route for Network

   `gre` [route { del (net *network* tunnelname *tunnel-name*) }]
4. To delete an Unicast Route for Host

   `gre` [route { del (host *IP* tunnelname *tunnel-name*) }]
5. To see all the networks and hosts with respective GRE Tunnels

   `gre` [route { show }]

ha

High Availability Options

`ha` [disable | load-balancing { off | on } | show { details | logs (lines *number*) }]

disable - Option to disable HA. One can enable HA from Admin Console – System > HA.

load-balancing – Option to disable traffic load balancing between the cluster device. By default, as soon as Active-Active is configured, traffic load balancing is enabled.

show – Displays HA configuration details like HA status and state, current and peer device key, dedicated port and IP Address, load balancing and Auxiliary Administrative port and IP Address. It also displays HA logs if HA is configured.

hardware_acceleration

This command is available only for XG 125, XG 135 and XG 750 appliances.

Use to enable hardware acceleration for IPsec VPN traffic to increase throughput of Sophos XG Firewall.

`hardware_acceleration`(disable|enable|statistics|status)

- disable - use to disable hardware acceleration.
- enable - use to enable hardware acceleration. This is the default option.
- statistics - reserved for future use.
- status - use to view current configuration status.

ipsec_route

Configure IPSec routes and view route details like tunnel name, host/network and netmask.

`IPsec_route`[add|delete|show]

- **To add an IPSec Route for Host**

  `IPsec_route`[add {host*IP* tunnelname *Tunnel name* }]
- **To add an IPsecRoute for Network**

  `IPsec_route`[add {net*Network address/Mask* tunnelname *Tunnel name* }]
- **To delete an IPsecRoute for Host**

  `IPsec_route`[del {host*IP* tunnelname *Tunnel name* }]
- **To delete an IPsecRoute for Network**

  `IPsec_route`[del {net*Network address/Mask* tunnelname *Tunnel name* }]
- **To see all the networks and hosts with respective IPsecTunnels**

  `IPsec_route`[show]

link_failover

VPN can be configured as a Backup link. With this, whenever primary link fails, traffic will be tunneled through VPN connection and traffic will be routed again through the primary link once it is UP again.

Syntax

`link_failover`[add | del | show]

1. Manage Add Link Fail-over options

`link_failover`[add { primarylink Port<*Port Name*> backuplink (gre| vpn) }]

To configure GRE Tunnel as a Backup link using PING

`link_failover`[add { primarylink Port<*Port Name*> backuplink gre tunnel <*gre tunnel name*> monitor PING host <*ip address*> }]

To configure GRE Tunnel as a Backup link using TCP

`link_failover`[add { primarylink Port<*Port Name*> backuplink gre tunnel <*gre tunnel name*> monitor TCP host <*ip address*> port <*Port Number*> }]

To configure an IPsec/VPN connection as a Backup link using PING

```
link_failover[ add { primarylink Port<Port Name> backuplink vpn tunnel <IPSec Connection Name> monitor PING host <ip address> } ]
```

To configure an IPsec/VPN connection as a Backup link using TCP

```
link_failover[ add { primarylink Port<Port Name> backuplink vpn tunnel <IPSec Connection Name> monitor TCP host <ip address> port <Port Number> } ]
```

2. To delete link failover configuration

```
link_failover del primarylink <port name>
```

3. To display all link failover configuration

```
link_failover show
```

restart

Restart Sophos XG Firewall.

```
restart[all]
```

route_precedence

Set the route precedence.

```
route_precedence[set|show]
```

Default route lookup order is as follows:

1. Policy Route
2. VPN Route
3. Static Route
4. Default Route

Manage Set Route Precedence options

```
route_precedence[set{policyroute|vpn|static}]
```

- **To configure higher precedence for Static Routes**

  ```
  route_precedence[set{static vpn policyroute}]
  ```
- **To configure higher precedence for VPN Routes**

  ```
  route_precedence[set{vpn static policyroute}]
  ```

To display Route Precedence configuration

```
route_precedence[show]
```

shutdown

Shutdown Sophos XG Firewall.

```
shutdown
```

system_modules

Load or unload the system modules like h23, irc, sip, tftp.

By default, all the modules are loaded.

Load/unload modules to enhance the network performance and reduce the potential security risk.

`system_modules` [h323 { load | unload } | irc { load (port < *string* | default >) | `unload` } | pptp { load | unload } | sip { load (port < *string* | default >) | `unload` } | tftp { load (port < *string* | default >) | `unload` } | show]

H323 - The H.323 standard provides a foundation for audio, video, and data communications across IP-based networks, including the Internet. H.323 is an umbrella recommendation from the International Telecommunications Union (ITU) that sets standards for multimedia communications over Local Area Networks (LANs) that do not provide a guaranteed Quality of Service (QoS). It enables users to participate in the same conference even though they are using different videoconferencing applications.

PPTP - 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 - IRC (Internet Relay Chat) is a multi-user, multi-channel chatting system based on a client-server model. Single Server links with many other servers to make up an IRC network, which transport 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.

SIP – 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 - Trivial File Transfer Protocol (TFTP) is a simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP) and provides no security features.

vlan-tag

Set vlan tag on traffic which is originated by Sophos XG Firewall and do not fall in any Security Policy.

- **VLAN tag**

  `vlan-tag` [reset | set | show]
- **To reset vlanid**

  reset-reset or remove vlanid on bridge-interface

  `vlan-tag` [reset { interface*interface-bridge* }]
- **To set vlanid**

  set –set vlanid *0-4094* on bridge interface.

  `vlan-tag` [set { interface test vlanid*number* }]
- **To display the configured vlanid**

  show –show configured vlan tags on bridge interface(s).

  `vlan-tag` [show]

dos-config

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

`dos-config` [add | delete | flush |show]

Add DoS policy/rule

- To add a DoS policy.

  `dos-config` [add { dos-policy policy_name *policy_name* { ICMP-Flood | IP-Flood | SYN-Flood | UDP-Flood } *1-10000* pps { global | per-dst | per-src } }]

per-src : Configure packets per second (pps) allowed from a single source, above which device will drop the packets. The limit is applicable to individual source requests per user/IP address.

per-dest: Configure packets per second (pps) allowed to a single destination. The limit is applicable to individual destination requests per user/IP address.

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.

- Add a DoS rule, specify the criteria to match the traffic in the DoS rule and attach it to a DoS policy.

  `dos-config` [add { dos-rule rule_name *rule_name* srcip *sourceip* dstip *desinationip* netmask *netmask* protocol { icmp | ip | tcp | udp } rule-position *number* src-interface *Physical Interface Name* src-zone { DMZ | LAN | VPN | WAN | WiFi | custom zone } dos-policy *policy_name* }]

  Specify the source/destination IP address for which you want to enable flood protection.

  `dos-config` [add { dos-rule rule_name *rule_name* srcip *sourceip* dstip *desinationip* netmask *netmask* }] dos-policy *policy_name*

  Enable flood protection for the protocol.

  `dos-config` [add dos-rule rule_name *rule_name* protocol { icmp | ip | tcp | udp } dos-policy *policy_name*]

  Enable flood protection for ICMP protocol.

  `dos-config` [add dos-rule rule_name *rule_name* protocol { icmp icmptype *0-40* icmpcode *0-15* } dos-policy *policy_name*]

  Enable flood protection for IP protocol.

  `dos-config` [add dos-rule rule_name *rule_name* protocol { ip protonumber *0-142* } dos-policy *policy_name*]

  Enable flood protection for TCP protocol.

  `dos-config` [add dos-rule rule_name *rule_name* protocol { tcp dport *1-65535* } dos-policy *policy_name*]

  Enable flood protection UDP protocol.

  `dos-config` [add dos-rule rule_name *rule_name* protocol { udp dport *1-65535* } dos-policy *policy_name*]

  Specify the zone/interface you want to protect.

  `dos-config` [add dos-rule rule_name *rule_name* src-interface *Physcial Interface Name* src-zone { DMZ | LAN | VPN | WAN | WiFi | custom zone } dos-policy *policy_name*]

Delete DoS policy/rule

- To delete a DoS policy

  `dos-config` { delete { dos-policy policy-name *policy_name* } }

- To delete a DoS rule

  `dos-config` { delete { dos-rule rule-name *rule_name* } }

Flush Dos rules

`dos-config` { flush { dos-rules } }

View configured DoS rules/policies

- `dos-config` [show { dos-rules | dos-policies }]

- To view a DoS rule

  ```
  dos-config[show{dos-rules rule-name rule_name}]
  ```
- To view a DoS policy

  ```
  dos-config[show{dos-policies policy-name policy_name}]
  ```
- To view all configured DoS policies

  ```
  dos-config[show{dos-policies }]
  ```
- To view all configured DoS rules

  ```
  dos-config[show{dos-rules }]
  ```

In terms of precedence, DoS policies are applied in the following order:

- **DoS Bypass rules**: They have the highest precedence and traffic will be matched first with configured bypass rules.
- **Policies/rules configured using CLI commands**: If traffic does not match any configured bypass rule, then policies configured through CLI will be applied.
- **Global DoS Settings**: DoS Settings are applied last if traffic doesn't match either of DoS bypass rule or policies.

For e.g., If a DoS policy is configured with 500 maximum packets per second for a source and the traffic hitting the DoS policy exceeds the limit, device will ignore flooding, as bypass rule for the same source is configured. If no bypass rule is configured and traffic hitting the DoS policy exceeds the limit, then device will consider it an DoS attack.

wireless-controller

The debuglevel parameter configures the debugging level the device will use when logging. The level parameter must be between 0 (lowest) and 15 (highest).

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 between 0 (lowest) and 7 (highest).

Packets bound for devices within the WLAN need to go to the correct destination. The SSID keeps the packets within the correct WLAN, even when overlapping WLANs are present. However, there are usually multiple Aps within each WLAN, andt here has to be a way to identify those APs and their associated clients. This identifier is called a basic service set identifier (BSSID) and is included in all wireless packets. Put simply, each AP Has its own BSS, which helps identify clients associated with each AP.

The tunnel_id_offset parameter value must be between 0 (lowest) and 65535 (highest).

Syntax

```
wireless-controller global[ ap_autoaccept | ap_debuglevel | log_level | show | store_bss_stats |
tunnel_id_offset ]
```

To enable auto-accept of Access Points (APs)

```
wireless-controller global[ ap_autoaccept {1}]
```

To disable auto-accept of Access Points (APs)

```
wireless-controller global[ ap_autoaccept {0}]
```

Set the debugging output level

```
wireless-controller global[ ap_debuglevel <number>]
```

Set the log level value

```
wireless-controller global[ log_level <number>]
```

To enable storing of basic service set (BSS) identifier

```
wireless-controller global[ store_bss_stats {1}]
```

To disable storing of basic service set (BSS) identifier

```
wireless-controller global[ store_bss_stats {0}]
```

To set tunnel ID offset value

```
wireless-controller global[ tunnel_id_offset <number>]
```

To view the configured Wireless Protection settings

```
wireless-controller global show
```

cellular_wan

Enable or disable Cellular WAN and view information of the Wi-Fi modem information (if plugged -in).Cellular WAN menu will be available on Admin Console only when cellular wan is enabled from CLI.

```
cellular_wan[disable|enable|query|set|show]
```

To disable Cellular WAN

```
cellular_wan[disable]
```

To enable Cellular WAN

```
cellular_wan[enable]
```

Manage Cellular WAN Query options

```
cellular_wan[{serialportserial port numberAT commandat command string}]
```

Manage Cellular WAN Set options

```
cellular_wan[set{disconnect-on-systemdown(off|on)}|{modem-setup-delaynumber}]
```

To display Cellular WAN configuration

```
cellular_wan[show]
```

Serial dial-in

This command is available only in CR15i, CR10iNG, CR10wiNG, CR15iNG, CR15wi and CR 15wiNG devices.

```
serial_dialin[ enable | disable | modem-nvram { reset | save-init-string } ]
```

Enable/Disable serial dial-in or DB9.

enable – Enables serial dial-in feature. Modem can be connected to Sophos XG Firewall’s serial (COM) port.

disable – Disable serial dial-in feature.

modem-nvram to save/reset init string in modem.

reset – Reset init string in modem to factory default value.

save – Save pre-configured init string in modem's memory.

tcpdump

tcpdump prints out the headers of packets on a network interface that match the boolean expression. Only packets that match expression will be processed by tcpdump.

Syntax

`tcpdump` [*<text>* | count | filedump | hex | interface | llh | no_time | quite | verbose]

Parameter list & description

<text>

Packet filter expression. Based on the specified filter, packets are dumped. If no expression is given, all packets are dumped else only packets for which 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 given table on writing filtering expressions.

count

Exit after receiving count packets.

filedump

Tcpdump output can be generated based on criteria required.

hex

Print each packet (minus its link level header) in hexadecimal notation.

interface

Listen on <interface>.

llh

View packet contents with Ethernet or other layer 2 header information.

no_time

Do not print a timestamp on each dump line.

quite

Print less protocol information so 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.

How to view traffic of the	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 <port-number>’	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 for the particular port	tcpdump ‘host <ipaddress> and port <port-number>’	tcpdump ‘host 10.10.10.1 and port 21’
the specific host for all the ports except SSH	tcpdump ‘host <ipaddress> and port not <port-number>’	tcpdump ‘host 10.10.10.1 and port not 22’

How to view traffic of the	tcpdump command	Example
specific protocol	tcpdump ’proto ICMP’ tcpdump ’proto UDP’ tcpdump ’proto TCP’ tcpdump ‘arp’	
particular interface	tcpdump interface <interface>	tcpdump interface PortA
specific port of a particular interface	tcpdump interface <interface> ‘Port <port-number>’	tcpdump interface PortA ‘port 21’

Note: Expressions can be combined using logical operators AND or OR and with NOT also. Make sure to use different combinations within single quotes.

telnet

Use telnet protocol to connect to another remote computer.

Syntax

`telnet[<ipaddress>]`

Parameter list & description

ipaddress {<port number>}

official name, an alias, or the Internet address of a remote host

Port - indicates a port number (address of an application). If a number is not specified, the default telnet port is used.

telnet6

Use telnet protocol to connect to another remote computer.

Syntax

`telnet6[<ipaddress6>]`

Parameter list & description

ipaddress6 {<port number>}

official name, an alias, or the Internet address of a remote host

Port - indicates a port number (address of an application). If a number is not specified, the default telnet port is used.

traceroute

Use to trace the path taken by a packet from the source system to the destination system, over the Internet.

The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route one's packets follow (or finding the miscreant gateway that is discarding your packets) can be difficult.

Traceroute utilizes the IP protocol `time to live (TTL)' field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host.

Syntax

`traceroute [`*<ipaddress>*`|`*<string>*`|` first-ttl `|` icmp `|` max-ttl `|` no-frag `|` probes `|` source `|` timeout `|` tos`]`

Parameter list & descriptions

<ipaddress> [size <number>]

Set the IP Address to be traced.

<string> [size <number>]

Set the domain to be traced.

first-ttl

Set the initial time-to-live used in the first outgoing probe packet.

icmp

Use ICMP ECHO instead of UDP datagrams.

max-ttl

Set the max time-to-live.

no-frag

Set the 'don't fragment' bit.

probes

Probes are sent at each ttl.

Default - 3

source

Use given IP Address as source address.

timeout

Set the timeout -in seconds for a response to a probe.

Default 5

tos

Set the type-of-service.

traceroute6

Use to trace the path taken by a packet from the source system to the destination system, over the Internet.

The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route one's packets follow (or finding the miscreant gateway that is discarding your packets) can be difficult. Traceroute utilizes the IP protocol `time to live (TTL)' field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host.

Syntax

`traceroute6 [`*<ipaddress6>*`|`*<string>*`|` first-ttl `|` icmp `|` max-ttl `|` no-frag `|` probes `|` source `|` timeout `|` tos`]`

Parameter list & descriptions

<ipaddress6> [size <number>]

Set the IP Address to be traced.

<string> [size <number>]

Set the domain to be traced.

first-ttl

Set the initial time-to-live used in the first outgoing probe packet.

icmp

Use ICMP ECHO instead of UDP datagrams.

max-ttl

Set the max time-to-live.

no-frag

Set the 'don't fragment' bit.

probes

Probes are sent at each ttl.

Default - 3

source

Use given IP Address as source address.

timeout

Set the timeout -in seconds for a response to a probe.

Default 5

tos

Set the type-of-service.

route

Use to view / manipulate the IP routing table. Route manipulates the kernel’s IP routing tables. Its primary use is to set up temporary routes to specific hosts or networks via an interface. When the add or del options are used, route modifies the routing tables. Without these options, route displays the current contents of the routing tables.

Syntax

```
diagnostics [ utilities { route ( flush-cache | lookup ) } ]
```

Parameter list & description
flush-cache

Flush entire route cache.

lookup

Route lookup.

route6

Use to view / manipulate the IP routing table. Route manipulates the kernel’s IP routing tables. Its primary use is to set up temporary routes to specific hosts or networks via an interface. When the add or del options are used, route modifies the routing tables. Without these options, route displays the current contents of the routing tables.

Syntax

```
diagnostics [ utilities { route6 ( flush-cache | lookup ) } ]
```

Parameter list & description

flush-cache

Flush entire route cache.

lookup

Route lookup.

Connections

Allows to view and delete connections to the Sophos XG Firewall device.

Syntax

`connections [ count | v4 | v6 ]`

Parameter list & description

count <number>

Count of current connections.

v4 [delete | show]

View and delete IPv4 connections.

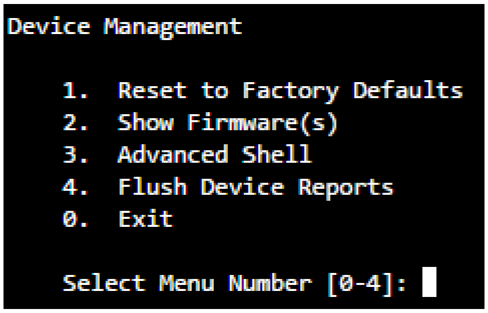
v6 [delete | show]

View and delete IPv6 connections.

Device Management

Use this menu to:

- Reset to Factory Defaults
- Show Firmware(s)
- Advanced Shell
- Flush Device Reports



```
Device Management

    1.  Reset to Factory Defaults
    2.  Show Firmware(s)
    3.  Advanced Shell
    4.  Flush Device Reports
    0.  Exit

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

Reset to Factory Defaults

This option resets all the customized configurations to their original state. All customization done after the initial deployment will be deleted including network configuration, HTTP proxy cache, passwords, groups, users and policies.

Show Firmware

This option displays all the firmware installed on the device. Moreover, the firmware currently active on the device is also mentioned.

Advanced Shell

This option directs you to the Advanced Shell.

Flush Device Reports

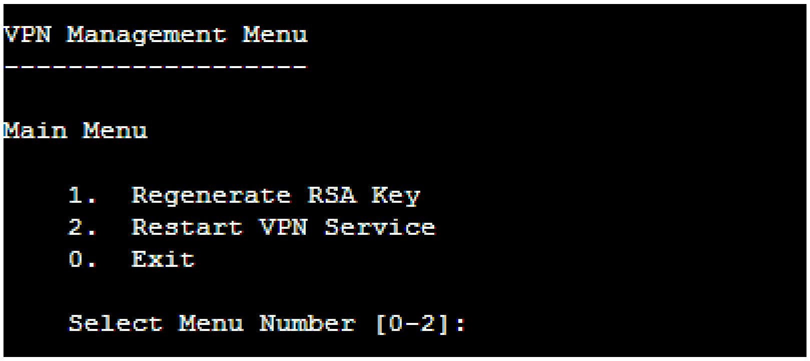
This option flushes all the On-box reports. This makes device inaccessible for a few minutes as flushing reports takes time.

Exit

Type **0** to exit from **Device Management** menu and return to **Main Menu**.

VPN Management

Below given menu will be displayed only when Sophos XG Firewall is deployed in Gateway mode.

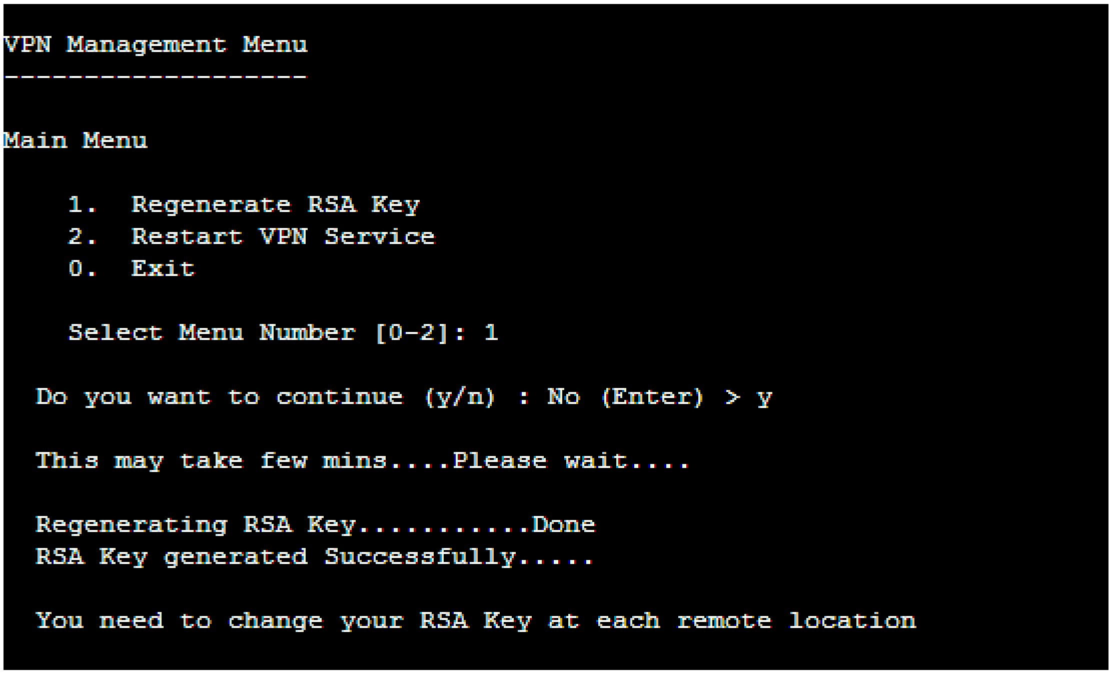


```
VPN Management Menu
-------------------

Main Menu

    1.  Regenerate RSA Key
    2.  Restart VPN Service
    0.  Exit

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

Regenerate RSA Key

RSA is used as one of the authentication methods to authenticate IPsec end-points in Site-to-Site and Host-to-Host VPN connections.

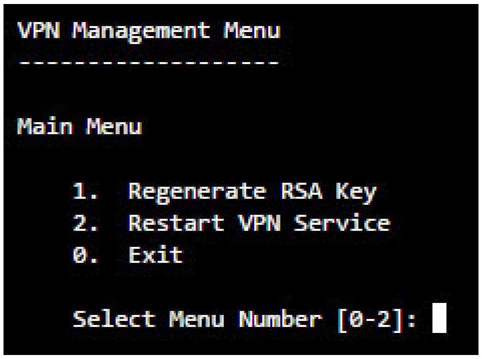
Use this option to regenerate the RSA Key i.e. New Public-Private Key pair, on the Sophos Firewall device.



```
VPN Management Menu
-------------------

Main Menu

    1.  Regenerate RSA Key
    2.  Restart VPN Service
    0.  Exit

    Select Menu Number [0-2]: 1

  Do you want to continue (y/n) : No (Enter) > y

  This may take few mins....Please wait....

  Regenerating RSA Key...........Done
  RSA Key generated Successfully.....

  You need to change your RSA Key at each remote location
```

Restart VPN Service

Use to restart VPN Service:



```
VPN Management Menu
-------------------

Main Menu

    1.  Regenerate RSA Key
    2.  Restart VPN Service
    0.  Exit

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

Figure 8: Restart VPN Service

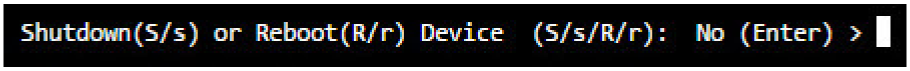
Exit

Type **0** to exit from **VPN** menu and return to the **Main Menu**.

Shutdown/Reboot Device

Use to shut down or reboot Sophos XG Firewall.

Type ‘s’ to shut down the device, “r” to soft reboot the device, “R” to hard reboot the device; else press “Enter” key to exit.



```
Shutdown(S/s) or Reboot(R/r) Device  (S/s/R/r):  No (Enter) >
```

Figure 9: Shutdown Device

Exit

Type **0** to exit from Device Command Line Console (CLI) Management.

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-Address
5	Name Servers	N/4 IEN-116 server addresses	Array of IP-Address
7	Log Servers	N/4 logging server addresses	Array of IP-Address
8	Cookie Servers	N/4 quote server addresses	Array of IP-Address
9	LPR Servers	N/4 printer server addresses	Array of IP-Address
10	Impress Servers	N/4 impress server addresses	Array of IP-Address
11	RLP Servers	N/4 RLP server addresses	Array of IP-Address
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 Ser ver	Swap ser ver addresses	IP-Address
17	Root Path	Path name for root disk	String
18	Extension File	Patch name for more BOOTP info	String
19	IP Layer Forwarding	Enable or disable IP forwarding	Boolean
20	Src route enabler	Enable or disable source routing	Boolean

Option Number	Name	Description	Data Type
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 Time to Live	Default TCP time to live	One Byte Numeric Value
38	TCP Keepalive Interval	TCP keepalive inter val	Four Byte Numeric Value
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-Address
42	NTP Ser vers Addresses	NTP ser vers addresses	Array of IP-Address
43	Vendor Specific Information	Vendor specific information	String
45	NetBIOS Datagram Distribution	NetBIOS datagram distribution	Array of IP-Address
46	NetBIOS Node Type	NetBIOS node type	One Byte Numeric Value
47	NetBIOS Scope	NetBIOS scope	String
48	X Window Font Ser ver	X window font ser ver	Array of IP-Address
49	X Window Display Manager	X window display manager	Array of IP-Address
50	Requested IP Address	Requested IP Address	IP-Address
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

Option Number	Name	Description	Data Type
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
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-Address
66	TFTP Ser ver Name	TFTP ser ver name	String
67	Boot File Name	Boot file name	String
68	Home Agent Addresses	Home agent addresses	Array of IP-Address
69	Simple Mail Server Addresses	Simple mail ser ver addresses	Array of IP-Address
70	Post Office Server Addresses	Post office server addresses	Array of IP-Address
71	Network News Server Addresses	Network news server addresses	Array of IP-Address
72	WWW Server Addresses	WWW server addresses	Array of IP-Address
73	Finger Server Addresses	Finger server addresses	Array of IP-Address
74	Chat Server Addresses	Chat server addresses	Array of IP-Address
75	StreetTalk Ser ver Addresses	StreetTalk server addresses	Array of IP-Address
76	StreetTalk Directory Assistance Addresses	StreetTalk directory assistance addresses	Array of IP-Address

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	Alpha-Numeric TEXT with/without quotes
22	SIP-Servers-Addresses	Specifies a list of IPv6 addresses indicating SIP outbound proxy servers available to the client	Alpha-Numeric TEXT with/without quotes
24	Domain-Search	Specifies the domain search list the client is to use when resolving hostnames with DNS	Alpha-Numeric TEXT with/without quotes
27	NIS-Servers	Provides a list of one or more IPv6 addresses of NIS servers available to the client	Alpha-Numeric TEXT with/without quotes
28	NISP-Servers	Provides a list of one or more IPv6 addresses of NIS + servers available to the client	Alpha-Numeric TEXT with/without quotes
29	NIS-Domain-Name	Used by the server to convey client's NIS Domain Name info to the client	Alpha-Numeric TEXT with/without quotes
30	NISP-Domain-Name	Used by the server to convey client's NIS+ Domain Name info to the client	Alpha-Numeric 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	Alpha-Numeric TEXT with/without quotes
32	INFO-Refresh-Time	Specifies an upper bound for how long a client should wait before refreshing information retrieved from DHCPv6	Alpha-Numeric TEXT with/without quotes
33	BCMS-Server-D	Broadcast and Multicast Service Controller Domain Name List Option for DHCPv6	Alpha-Numeric TEXT with/without quotes
34	BCMS-Server-A	Broadcast and Multicast Service Controller IPv6 Address Option for DHCPv6	Alpha-Numeric TEXT with/without quotes