

SOPHOS

Security made simple.



Workflow Guide

Sophos Firewall OS CLI Guide

Document Date: November 2015

Contents

Preface	3
Guide Audience	3
Introduction	4
Accessing Sophos Firewall OS Command Line Console.....	4
1. Network Configuration	5
Configure and manage Interfaces	5
Configure and manage DNS.....	7
2. System Settings	8
2.1 Set Password for User Admin	8
2.2 Set System Date.....	8
2.3 Set Email ID for system notification	9
2.4 Reset Default Web Admin Certificate.....	9
2.0 Exit	10
3. Route Configuration	10
3.1 Configure Unicast Routing.....	10
3.1.1 Configure RIP.....	11
3.1.2 Configure OSPF.....	13
3.1.3 Configure BGP	14
3.1.0 Exit.....	16
3.2 Configure Multicast Routing.....	16
3.2.1 Enable/Disable Multicast forwarding.....	18
3.2.2 Configure Static multicast routes	18
3.2.0 Exit.....	21
3.0 Exit	21
4. Device Console	22
5. Device Management	23
5.1 Reset to Factory Defaults	23
5.2 Show Firmware	23
5.3 Advanced Shell.....	23
5.4 Flush Device Reports	23
5.0 Exit	24
6. VPN Management	24
6.1 Regenerate RSA Key	24
6.2 Restart VPN service	25
6.0 Exit	25
7. Shutdown/Reboot Device	25
0. Exit	25
Annexure A	26
Appendix A – DHCP Options (RFC 2132)	58
Appendix B – DHCPv6 Options (RFC 3315)	61

Preface

Welcome to Sophos Firewall OS Command Line Console (CLI) guide. This guide helps you configure and manage your Sophos Firewall with the help of CLI.

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 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.

If you are new to Sophos Firewall, use this guide along with the 'Sophos Firewall Admin Guide'.

Introduction

Sophos Firewall OS CLI guide describes CLI commands used to configure and manage a Sophos Firewall unit from the Command Line Console (CLI).

Accessing Sophos Firewall OS Command Line Console

There are two ways to access Sophos 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 Firewall CLI using a SSH client, e.g. PuTTY. IP Address of the Sophos Firewall is required. Start SSH client and create new connection with the following parameters:
 - Hostname - < Sophos 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.

1. Network Configuration

Use this menu for

- Configure and manage Interfaces
- Configure and manage DNS

Configure and manage Interfaces

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.

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

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

2. 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]: █
```

2.1 Set Password for User Admin

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

Type new password, retype for confirmation, and press <Enter>.

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

Displays successful completion message.

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

2.2 Set System Date

Use to change time zone and system date.

Type ‘y’ to set new time and press <Enter>:

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

Set Date (y/n) : No (Enter) > █
```

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.


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

WARNING: 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 .....
```

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

2.3 Set Email ID for system notification

Use to set the Email ID for system notifications. Sophos 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 █
```

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

2.4 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.
```

2.0 Exit

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

3. Route Configuration

Use this menu to configure static routes, RIP, OSPF and enable or disable multicast forwarding. Sophos 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]:
```

3.1 Configure Unicast Routing

```
Unicast Routing Configuration

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

Select Menu Number:
```

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

3.1.1 Configure RIP

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

Routing Information Protocol (RIP) is a distance-vector routing protocol documented in RFC 1058. RIP uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information.

The Sophos 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 2

RIP Configuration Task List

RIP must be enabled before carrying out any of the RIP commands. To configure RIP, use the following commands from CLI:

- Go to Option 3 (Route Configuration)
 - Go to Option 1 (Configure Unicast Routing)
 - Go to Option 1 (Configure RIP)
- To configure RIP, perform the tasks described in the following table:

Steps	Command	Purpose
Enable RIP	rip> enable	Enables RIP routing process and places you in Global Configuration mode.
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 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.
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.
	To set authentication mode as text and set the authentication string rip(config)# interface ifname	Defines authentication mode for the each interface. By, default, authentication is on for all the

	<pre>rip(config-if)# ip rip authentication mode {text [string]}</pre> <p>For example,</p> <pre>rip(config)# interface A rip(config-if)# ip rip authentication mode text rip(config-if)# ip rip authentication string teststring</pre> <p>To set authentication mode as MD5 and set the authentication string</p> <pre>rip(config)# interface ifname rip(config-if)# ip rip authentication mode {md5 [key-chain name of key chain]}</pre> <p>For example,</p> <pre>rip(config)# interface A rip(config-if)# ip rip authentication mode md5 key-chain testkeychain</pre> <p>To disable authentication</p> <pre>rip(config)# interface ifname rip(config-if)# no ip rip authentication mode</pre> <p>For example, disable authentication for interface A</p> <pre>rip(config)# interface A rip(config-if)# no ip rip authentication mode</pre>	<p>interfaces. If authentication is not required for any of the interface, it is to be explicitly disabled.</p> <p>RIP Version 1 does not support authentication.</p> <p>RIP Version 2 supports Clear Text (simple password) or Keyed Message Digest 5 (MD5) authentication.</p> <p>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.</p> <p>If authentication is not required for any of the interface, use the no form of this command</p>
	<pre>rip(config-if)# end</pre>	<p>Exits from the Router Configuration mode and places you into the Enable mode.</p>
<p>Exit to Router Management Menu</p>	<pre>rip(config-if)# exit</pre>	<p>Exits to the Router Management Menu.</p>

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 router rip
```

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

3.1.2 Configure OSPF

This option is available only when Sophos 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 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 Firewall participates in OSPF communications, when it has an interface to an OSPF area. Sophos 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 Firewall. After initial contact, the Sophos 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 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.

RIP Configuration Task List

OSPF must be enabled before carrying out any of the OSPF commands. To configure OSPF, use the following commands from CLI:

- Go to Option 3 (Route Configuration)
- Go to Option 1 (Configure Unicast Routing)
- Go to Option 1(Configure OSPF)
- To configure OSPF, perform the tasks described in the following table:

Steps	Command	Purpose
Enable OSPF	ospf> enable	Enables OSPF routing process and places you in Global Configuration mode.
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 rip	Allows to configure and start OSPF routing process.
	ospf(config-router)# network ip-address area area-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.

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 router ospf
```

3.1.3 Configure BGP

This option is available only when Sophos 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 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 Firewall advertises routing table updates to neighboring autonomous systems whenever any part of the Sophos Firewall routing table changes. Each AS, including the local AS of which the Sophos 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 Firewall unit receives a BGP update, the Sophos Firewall examines potential routes to determine the best path to a destination network before recording the path in the Sophos Firewall routing table.

BGP Configuration Task List

BGP must be enabled before carrying out any of the BGP commands. To configure BGP, use the following commands from CLI:

- Go to Option 3 (Route Configuration)
- Go to Option 1 (Configure Unicast Routing)
- Go to Option 1(Configure BGP)
- To configure BGP, perform the tasks described in the following table:

Steps	Command	Purpose
Enable BGP	<code>bgp> enable</code>	Enables BGP routing process and places you in Global Configuration mode.
Specify a list of networks for the OSPF routing process	<code>bgp# configure terminal</code>	Enables the BGP configuration mode which places you in the Router Configuration mode and allows you to configure from the terminal.
	<code>bgp(config)# router bgp AS number</code>	Allows to configure and start BGP routing process. AS number is the number of the local AS that Sophos Firewall unit is a member of.
	<code>bgp(config-router)# network ip-address</code> 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.

	<code>bgp(config-router)# show running-config</code>	<p>View configuration</p> <p>By default, router ID is Sophos Firewall IP Address. Router ID is used to identify the Sophos Firewall to other BGP routers.</p> <p>You can change the router ID using the following command:</p> <pre>bgp(config-router)#bgp router-id IP address</pre> <p>The router-id can be an integer or can take a form similar to an IP Address A.B.C.D</p>
	<code>bgp(config-router)#end</code>	Exits from the Router Configuration mode and places you into the Enable mode.
Exit to Router Management Menu	<code>bgp# exit</code>	Exits to the Router Management Menu.

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 router bgp AS number
```

3.1.0 Exit

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

3.2 Configure Multicast Routing

```
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.

3.2.1 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, go to Option 3 (Route Configuration)> Option 2 (Configure Multicast Routing), Option 1 (Enable/Disable Multicast forwarding) and execute following command:

console> enable multicast-forwarding

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

Select Menu Number: 1
```

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

3.2.2 Configure Static multicast routes

Note: Multicast routes cannot be added before enabling multicast forwarding.

Go 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 <ipaddress> dest-ip <ipaddress>
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,

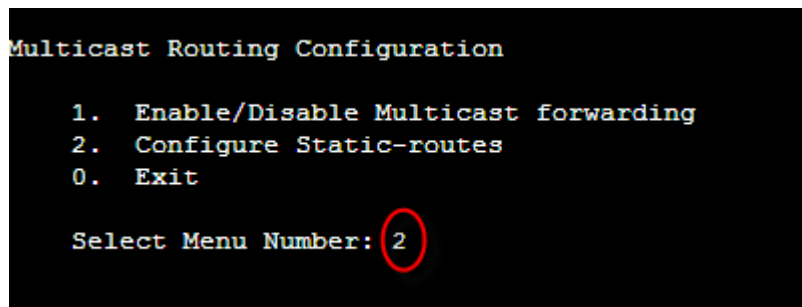
```
console> mroute add input-interface PortA source-ip 1.1.1.1 dest-ip 230.1.1.2 output-interface PortB
```

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

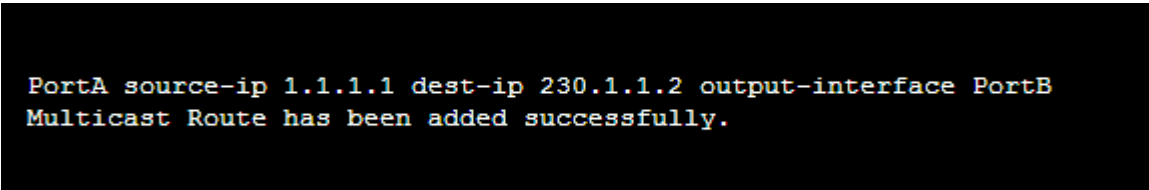
If you want to inject multicast traffic to more than one interface, you have to add routes for each destination interface. For example,

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

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



```
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

Go 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)
console>
```

Removing route

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

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

```
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 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.

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

- Command: `mroute add input-interface Port<port number> source-ip <ipaddress> dest-ip <ipaddress> output-interface Port<port number>`
To forward multicast traffic coming from a given interface to another interface
E.G. `mroute add input-interface PortA source-ip 192.168.1.2 dest-ip 239.0.0.55 output-interface PortB`
- Command: `mroute add input-interface Port<port number> source-ip <ipaddress> dest-ip <ipaddress> output-tunnel gre name <gre tunnel name>`
To forward multicast traffic coming from a given interface to GRE tunnel.
E.G. `mroute add input-interface PortA 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`
To forward multicast traffic coming from a given interface to IPsec tunnels. Sophos Firewall automatically selects the appropriate tunnel to be used depending upon the Local Network and Remote Network configuration.
E.G. `mroute add input-interface PortA 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>`

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

E.G. `mroute add input-tunnel IPsec name Net2Net source-ip 192.168.1.2 dest-ip 239.0.0.55 output-interface PortB`

- **Command:** `mroute add input-tunnel IPsec name <IPsec connection name> source-ip <ipaddress> dest-ip <ipaddress> output-tunnel IPsec`
To forward multicast traffic coming from a given IPsec tunnel to other IPsec tunnels. Sophos Firewall automatically selects the appropriate tunnel to be used depending upon the Local Network and Remote Network configuration
E.G. `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 <IPsec connection name> source-ip <ipaddress> dest-ip <ipaddress> output-tunnel gre name <gre tunnel name>`
To forward multicast traffic coming from a given IPsec tunnel to GRE tunnel.
E.G. `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>`
To forward multicast traffic coming from a GRE tunnel to an interface.
E.G. `mroute add input-tunnel gre name Elitecore source-ip 192.168.1.2 dest-ip 239.0.0.55 output-interface PortB`
- **Command:** `mroute add input-tunnel gre name <gre tunnel name> source-ip <ipaddress> dest-ip <ipaddress> output-tunnel gre name <gre tunnel name>`
To forward multicast traffic coming from a GRE tunnel to another GRE tunnel.
E.G. `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`
To forward multicast traffic coming from a given GRE tunnel to IPsec tunnels. Sophos Firewall automatically selects the appropriate tunnel to be used depending upon the Local Network and Remote Network configuration.
E.G. `mroute add input-tunnel gre name Elitecore source-ip 192.168.1.2 dest-ip 239.0.0.55 output-tunnel IPsec`
- **Command:** `mroute del source-ip <ipaddress> dest-ip <ipaddress>`
To delete multicast route
E.G. `mroute del source-ip 192.168.1.2 dest-ip 239.0.0.`

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).

3.2.0 Exit

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

3.0 Exit

Type '0' to exit from Routing tables menu and return to Main Menu.

4. 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 Firewall has inbuilt help at the command prompt itself.

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 question mark, 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.

Note: Refer to [Annexure A](#) for the detailed help on various commands supported.

5. 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]: █
```

5.1 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.

5.2 Show Firmware

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

5.3 Advanced Shell

This option directs you to the Advanced Shell.

5.4 Flush Device Reports

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

Note: This option is not available in Cyberoam models CR 15i, CR 15wi, CR 10iNG, CR 10wiNG, CR 15iNG and CR 15wiNG.

5.0 Exit

Type '0' to exit from Device Management menu and return to the Main menu.

6. VPN Management

Below given menu will be displayed only when Sophos 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]:
```

6.1 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
```


Note: As evident from the screen above, every time you regenerate RSA Key, you need to change your RSA Key at all the remote locations too.

6.2 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]: 2

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

6.0 Exit

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

7. Shutdown/Reboot Device

Use to shut down or reboot Sophos 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) > █
```

0. Exit

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

Annexure A

clear

Clears the screen

Syntax

clear

system

Sophos Firewall System Management

Syntax

system [[appliance_access](#) | [application_classification](#) | [auth](#) | [bridge](#) | [dhcp](#) | [dhcpv6](#) | [diagnostics](#) | [discover-mode](#) | [firewall_acceleration](#) | [fsck-on-nextboot](#) | [gre](#) | [ha](#) | [IPsec_route](#) | [link_failover](#) | [restart](#) | [route_precedence](#) | [shutdown](#) | [system_modules](#) | [vlan-tag](#) | [wireless-controller](#) | [wwan](#) | [serial_dialin](#)]

Keywords & Variables	Description
<code>appliance_access [disable enable show]</code>	<p>To override or bypass the configured Device Access settings and allow access to all the Sophos Firewall services.</p> <p>Disable to re-apply Device Access. Default – Disabled.</p> <p>Enable and disable event will be logged in Admin Logs.</p>
<code>application_classification [off on show microapp_discovery { on off show }]</code>	<p>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.</p> <p>Once application_classification is enabled, you can enable microapp_discovery, which identifies and classifies microapps used within web browsers.</p> <p>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.</p> <p>Default – ON</p> <p>Note: application_classification must be ON to enable Micro App_Discovery.</p>

<p><u>Authentication Options</u></p> <p>auth [cta thin-client]</p> <p><u>1. Manage cta options</u></p> <p>auth [cta {collector enable unauth-traffic disable show vpnzonenetwork }]</p> <p><u>Manage collector options</u></p> <p>auth cta [collector {add delete}]</p> <ul style="list-style-type: none"> ▪ To add a collector in new group auth cta [collector {add <collector-ip> collector-port <port> create-new-collector-group}] ▪ To add a collector in an existing collector group auth cta [collector {add <collector-ip> collector-port <port> collector-group <group-number>}] ▪ To delete a collector IP auth cta [collector {delete <collector-ip>}] <p><u>To enable cta</u></p> <p>auth cta [enable]</p> <p><u>Manage drop period for unauthenticated traffic options</u></p> <p>auth cta [unauth-traffic <drop-period>]</p> <ul style="list-style-type: none"> ▪ To configure the default drop period for unauthenticated traffic auth cta [unauth-traffic drop-period <default>] ▪ To manually configure the drop period for unauthenticated traffic auth cta [unauth-traffic drop-period <0-120>] <p><u>To disable cta</u></p> <p>auth cta [disable]</p> <p><u>To display all cta configurations</u></p> <p>auth cta [show]</p> <p><u>Manage VPN zone Network options</u></p> <p>auth cta [vpnzonenetwork]</p> <ul style="list-style-type: none"> ▪ To add source-network IP Address 	<p>Enable authentication: transparent authentication, thin client authentication for AD users</p> <p>cta - Add and remove CTA collector IP Address for clientless Single Sign On configuration</p> <p>thin-client – add and remove citrix server IP Address for thin-client support</p>
--	---

<p>auth cta [vpnzonenetwork{add source network <ipaddress>}]</p> <ul style="list-style-type: none"> To delete source-network IP Address <p>auth cta [vpnzonenetwork{delete source network <ipaddress>}]</p> <p>2. Manage thin-client options</p> <p>auth [thin-client {add delete show}]</p> <p>To add a thin-client IP Address</p> <p>auth [thin-client{ add citrix-ip <ipaddress>}]</p> <p>To delete a thin-client IP Address</p> <p>auth [thin-client{ delete citrix-ip <ipaddress>}]</p> <p>To display thin-client IP Address</p> <p>auth [thin-client{ show}]</p>	
<p><u>VLAN tag</u></p> <p>vlan-tag [reset set show]</p> <p><u>To reset vlanid</u></p> <p>vlan-tag [reset { interface <interface-bridge> }]</p> <p><u>To set vlanid</u></p> <p>vlan-tag [set { interface test vlanid <number > }]</p> <p><u>To display the configured vlanid</u></p> <p>vlan-tag [show]</p>	<p>Set vlan tag on traffic which is originated by Sophos Firewall and do not fall in any Security Policy.</p> <p>set – set vlanid <0-4094> on bridge interface.</p> <p>reset - reset or remove vlanid on bridge-interface</p> <p>show – show configured vlan tags on bridge interface(s).</p>
<p><u>Configure Wireless Protection</u></p> <p>wireless-controller global [ap_autoaccept ap_debuglevel log_level show store_bss_stats tunnel_id_offset]</p> <p><u>To enable auto-accept of Access Points (APs)</u></p> <p>wireless-controller global [ap_autoaccept {1}]</p> <p><u>To disable auto-accept of Access Points (APs)</u></p> <p>wireless-controller global [ap_autoaccept {0}]</p>	<p>The debuglevel parameter configures the debugging level the device will use when logging. The level parameter must be between 0 (lowest) and 15 (highest).</p> <p>The log_level parameter configures the loggin 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).</p> <p>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, and</p>

<p><u>Set the debugging output level</u> wireless-controller global [ap_debuglevel <number>]</p> <p><u>Set the log level value</u> wireless-controller global [log_level <number>]</p> <p><u>To enable storing of basic service set (BSS) identifier</u> wireless-controller global [store_bss_stats {1}]</p> <p><u>To disable storing of basic service set (BSS) identifier</u> wireless-controller global [store_bss_stats {0}]</p> <p><u>To set tunnel ID offset value</u> wireless-controller global [tunnel_id_offset <number>]</p> <p><u>To view the configured Wireless Protection settings</u> wireless-controller global [show]</p>	<p>there 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.</p> <p>The tunnel_id_offset parameter value must be between 0 (lowest) and 65535 (highest).</p>
<p><u>Bridge Management</u> bridge [bypass-firewall-policy { unknown-network-traffic } static-entry]</p> <p><u>1. Manage bypass-firewall-policy options</u> bypass-firewall-policy [unknown-network traffic {allow drop show}]</p> <p><u>To allow unknown network traffic</u> bypass-firewall-policy [unknown-network traffic {allow}]</p> <p><u>To drop unknown network traffic</u> bypass-firewall-policy [unknown-network traffic {drop}]</p> <p><u>To view bypass status for unknown network traffic</u> bypass-firewall-policy [unknown-network traffic {show}]</p> <p><u>2. Manage static-entry options</u> static-entry [add delete show]</p> <p><u>To add a static entry</u></p>	<p>Use the bypass-firewall-policy command to configure policy for unknown network traffic (non-routable traffic) on which no Security Policy is applied.</p> <p>allow - allow unknown network traffic to pass through system</p> <p>drop - do not allow unknown network traffic to pass through system</p> <p>show - display unknown traffic bypass status</p> <p>Use static-entry for 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.</p> <p>add - add a new static entry in bridge MAC table.</p>

<pre>staticentry [add {interface (<bridge name>:<Port>) macaddr <MAC Address> priority (dynamic static)}</pre>	<p>Examples:</p> <pre>system bridge static-entry [add {interface <Bridge1:Member1> macaddr <00:16:76:49:33:CE> priority (static)</pre> <pre>system bridge static-entry [add {interface <Bridge1:Member1> macaddr <00:16:76:49:33:CE> priority (dynamic)</pre> <p>delete - delete an existing static entry from bridge MAC table</p> <p>Example: system bridge static-entry [delete 00:16:76:49:33:CE]</p> <p>show - show all static entries in bridge table</p>
<p>DHCP Management</p> <pre>dhcp [dhcp-options lease-over-IPSec one-lease-per-client static-entry-scope]</pre> <p>1. Manage DHCP options</p> <pre>dhcp [dhcp-options {add binding delete list}]</pre> <p>To add a custom DHCP option</p> <pre>dhcp [dhcp-options {add optioncode <1-255> optionname <string> optiontype (array-of one-byte two-byte four- byte ipaddress string boolean)}</pre> <p>To delete a custom DHCP option</p> <pre>dhcp [dhcp-options {delete optionname <Option name>}]</pre> <p>To display all configurable DHCP option</p> <pre>dhcp [dhcp-options{list}]</pre> <p>To manage additional options for DHCP server</p> <ul style="list-style-type: none"> ▪ Add option to DHCP Server <pre>dhcp [dhcp-options {binding add (dhcpname <DHCP server name> optionname <DHCP Options> value <text>)}]</pre> ▪ Delete option from DHCP Server <pre>dhcp [dhcp-options {binding delete (dhcpname <DHCP server name>)}]</pre> ▪ Show options assigned to DHCP Server <pre>dhcp [dhcp-options {binding show (dhcpname <DHCP server name>)}>]</pre> 	<p>Sophos 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.</p> <p>Appendix A provides a list of DHCP options by RFC-assigned option number.</p>

<p><u>2. Manage IP Lease over IPsec</u></p> <p><u>To disable IP Lease over IPsec for all DHCP Servers (Default Value)</u> dhcp [lease-over-IPsec {disable}]</p> <p><u>To enable IP Lease over IPsec for all DHCP Servers</u> dhcp [lease-over-IPsec {enable}]</p> <p><u>To display all IP Lease over IPsec configuration</u> dhcp [lease-over-IPsec {show}]</p> <p><u>3. Manage IP lease for Client</u></p> <p>dhcp [one-lease-per-client {enable disable show}]</p> <p><u>To enable one lease per client for all DHCP servers</u> dhcp [one-lease-per-client {enable}]</p> <p><u>To disable one lease per client for all DHCP servers</u> dhcp [one-lease-per-client {disable}]</p> <p><u>To view one lease per client configuration</u> dhcp [one-lease-per-client {show}]</p> <p>4. Manage scope of Static lease dhcp static-entry-scope {global network show}</p>	
<p><u>DHCPv6 Management</u> dhcpv6 [dhcpv6-options]</p> <p><u>Manage DHCPv6 options</u> dhcpv6 [dhcpv6-options {add binding delete list}]</p> <p><u>To add a custom DHCPv6 option</u> dhcpv6 [dhcpv6-options {add optioncode <1-65535> optionname <string> optiontype (array-of one-byte two-byte four-byte ipv6address string boolean)}]</p>	<p>Sophos 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.</p> <p>Appendix B provides a list of DHCPv6 options by RFC-assigned option number.</p>

<p><u>To delete a custom DHCPv6 option</u></p> <pre>dhcpv6 [dhcpv6-options {delete optionname <Option name>}]</pre> <p><u>To display all configurable DHCPv6 option</u></p> <pre>dhcpv6 [dhcpv6-options{list}]</pre> <p><u>To manage additional options for DHCPv6 server</u></p> <ul style="list-style-type: none"> ▪ Add option to DHCPv6 Server <pre>dhcpv6 [dhcpv6-options {binding add (dhcpname <DHCPv6 server name> optionname <DHCP Options> value <text>)}]</pre> ▪ Delete option from DHCPv6 Server <pre>dhcpv6 [dhcpv6-options {binding delete (dhcpname <DHCPv6 server name>)}]</pre> ▪ Show options assigned to DHCPv6 Server <pre>dhcpv6 [dhcpv6-options {binding show (dhcpname <DHCPv6 server name>)}>]</pre> 	
<p><u>Device Diagnostics</u></p> <pre>diagnostics [ctr-log-lines purge-old-logs subsystems purge-all-logs show utilities]</pre> <p><u>1. To take last n lines for Consolidated Troubleshooting Report (CTR)</u></p> <pre>diagnostics [ctr-log-lines <250-10000>]</pre> <p><u>2. To truncate all rotated logs</u></p> <pre>diagnostics [purge-old-logs]</pre> <p><u>3. To configure Subsystems</u></p> <pre>diagnostics [subsystems {Access-Server Bwm CSC IM IPSEngine LoggingDaemon Msyncd POPIMAPDaemon Pktcapd SMTPD SSLVPN SSLVPN-RPD WebProxy Wifiauthd}]</pre> <p><u>Manage Access Server options</u></p> <pre>diagnostics [subsystems {Access-Server (debug purge-log purge-old-log)}]</pre> <ul style="list-style-type: none"> ▪ Enable/Disable Access Server debug <pre>diagnostics [subsystems {Access-Server debug <off on>}]</pre> ▪ To truncate all logs <pre>diagnostics [purge-log]</pre> 	<p>Various tools to check device health.</p> <p>ctr-log-lines – set number of lines to display in Consolidated Troubleshooting Report (CTR) log file.</p> <p>Default – 1000.</p> <p>purge-old-logs – purge all rotated log files</p> <p>subsystems – configure each subsystem individually. Configuration options include: debug, purge-logs and purge-old-logs</p> <p>purge-all-logs – truncate all log files</p> <p>show – view diagnostics statistics</p> <p>utilities – view utilities statistics</p>

- To truncate all rotated logs

diagnostics [purge-old-log]

Manage CSC options

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

- Toggle CSC debug mode
diagnostics [subsystems {CSC debug }]
- To truncate all logs
diagnostics [subsystems {CSC (purge-log)}]

- To purge all rotated logs
diagnostics [subsystems {CSC (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 | bandwidth-monitor | 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, CR10iING, CR10wiING, CR 15iING, CR15wi, CR 15wiING, CR25wi, CR25wiING/6P CR35wi and CR35wiING models.

<p><u>Discover Mode Configuration</u></p> <p>discover-mode [tap { (add <Port_Name> delete <Port_Name>) show}]</p>	<p>Use to configure one of more interfaces of Sophos Firewall in Discover Mode.</p> <p>add - configure an interface in Discover mode Example - discover-mode [tap { add <PortD >}]</p> <p>delete - remove an interface from Discover mode Example - discover-mode [tap { delete <PortD >}]</p> <p>show - use to view ports configured in Discover mode, if any</p>
<p><u>Firewall Acceleration Configuration</u></p> <p>Firewall-acceleration (enable disable show)</p>	<p>Use to enable Firewall Acceleration that uses advanced data-path architecture that enables Sophos Firewall with faster processing of data packets for known traffic.</p> <p>enable - use to to enable firewall acceleration. This is the default option.</p> <p>disable - use to to disable firewall acceleration</p> <p>show - use to view status of firewall acceleration configuration</p>
<p>fsck-on-nextboot [off on show]</p>	<p>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:</p> <ul style="list-style-type: none"> ▪ Unable to start Config/Report/Signature Database ▪ Unable to Apply migration ▪ Unable to find the deployment mode <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> ▪ Factory reset ▪ Flush Device Report
<p><u>GRE Tunnelling</u></p> <p>gre [route tunnel]</p> <p>1. <u>For GRE tunnel</u></p> <p>gre tunnel [add show set delete]</p> <p><u>To add a GRE Tunnel</u></p> <p>gre tunnel [add {name <tunnel-name> local-gw <WAN_Interface> remote-gw <Remote_WAN_IP> local-ip <LcalIP > remote-ip <RemotelIP>}]</p>	<p>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.</p> <p>NOTE:</p> <ol style="list-style-type: none"> 1. GRE tunnel cannot be configured over dynamic WAN interface such as PPPoE and DHCP. 2. After creating a GRE Tunnel, information regarding same will be displayed on Multicast page. 3. Ping the IP Address of remote GRE interface to check status of GRE tunnel.

To list GRE Tunnel

```
gre tunnel [show {local-gw | name }]
```

To set TTL for GRE Tunnel

```
gre tunnel [set {name <tunnel-name> ttl<ttlvalue>}]
```

To set state of GRE Tunnel

```
gre tunnel [set {name <tunnel-name> state (enable | disable)}]
```

To delete GRE Tunnel

1. gre tunnel [del {name <tunnel-name> local-gw <WAN_Interface> remote-gw <Remote_WAN_IP>}]
2. gre tunnel [del {name <tunnel-name>}]
3. gre tunnel [del {ALL}]

To check status of GRE Tunnel

```
gre tunnel [show {name <tunnel-name>} | {local-gw <WAN_Interface> remote-gw <Remote_WAN_IP>}]
```

2. Unicast Routing Support in GRE

```
gre route [add | delete | show]
```

To add an Unicast Route for Network

```
gre route [add {net <Network Address /Mask> tunnelname <Tunnel Name>}]
```

To add an Unicast Route for Host

```
gre route [add {host <IP> tunnelname <Tunnel Name>}]
```

To delete an Unicast Route for Network

```
gre route [del{net <Network Address/Mask> tunnelname <Tunnel Name>}]
```

To delete an Unicast Route for Host

```
gre route [del{host <IP> tunnelname <Tunnel Name>}]
```

To see all the networks and hosts with respective GRE Tunnels

```
gre route [show]
```

Configure, delete and verify the details of Unicast Routes for a network or a host, with respective GRE tunnel.

<p><u>High Availability Options</u></p> <p>ha [disable load-balancing {off on} show {details logs lines <number>}]</p>	<p>disable - Option to disable HA. One can enable HA from Admin Console – System > HA.</p> <p>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.</p> <p>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.</p>
<p><u>Manage Static IPsec Routes</u></p> <p>IPsec_route [add del show]</p> <p><u>To add an IPsec Route for Host</u></p> <p>IPsec_route [add {host <IP> tunnelname <Tunnel Name>}]</p> <p><u>To add an IPsec Route for Network</u></p> <p>IPsec_route [add {net <Network Address/Mask> tunnelname <Tunnel Name>}]</p> <p><u>To delete an IPsec Route for Host</u></p> <p>IPsec_route [del {host <IP> tunnelname <Tunnel Name>}]</p> <p><u>To delete an IPsec Route for Network</u></p> <p>IPsec_route [del {net <Network Address/Mask> tunnelname <Tunnel Name>}]</p> <p><u>To see all the networks and hosts with respective IPsec Tunnels</u></p> <p>IPsec_route [show]</p>	<p>Configure IPsec routes and view route details like tunnel name, host/network and netmask</p>
<p><u>Manage link failover over VPN</u></p> <p>link_failover [add del show]</p>	<p>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.</p>

<p><u>1. Manage Add Link Fail-over options</u></p> <p>link_failover [add {primarylink Port <Port Name> backuplink (gre vpn)}]</p> <p><u>To configure GRE Tunnel as a Backup link using PING</u></p> <p>link_failover [add {primarylink Port <Port Number> backuplink gre tunnel <gre tunnel name> monitor PING host <ip address>}]</p> <p><u>To configure GRE Tunnel as a Backup link using TCP</u></p> <p>link_failover [add {primarylink Port <Port Number> backuplink gre tunnel <gre tunnel name> monitor TCP host <ip address> Port <Port Number>}]</p> <p><u>To configure an IPsec/VPN connection as a Backup link using PING</u></p> <p>link_failover [add {primarylink Port <Port Number> backuplink vpn tunnel <IPsec connection name> monitor PING host <ip address>}]</p> <p><u>To configure an IPsec/VPN connection as a Backup link using TCP</u></p> <p>link_failover [add {primarylink Port <Port Number> backuplink vpn tunnel <vpn connection name> monitor TCP host <ip address> Port <Port Number>}]</p> <p><u>2. To delete link failover configuration</u></p> <p>link_failover del primarylink <Port name></p> <p><u>3. To display all link failover configuration</u></p> <p>link_failover [show]</p>	
<p>restart [all]</p>	<p>Restart Sophos Firewall</p>
<p><u>Manage Route Precedence</u></p> <p>route_precedence [set show]</p> <p><u>1. Manage Set Route Precedence options</u></p> <p>route_precedence [set {static vpn}]</p> <p><u>To configure Static Routes Precedence</u></p> <p>route_precedence [set {static vpn}]</p>	<p>Set the route precedence</p>

<p><u>To configure VPN Routes Precedence</u></p> <pre>route_precedence [set {vpn static}]</pre> <p><u>2. To display Route Precedence configuration</u></p> <pre>route_precedence [show]</pre>	
<pre>serial_dialin [enable disable modem-nvram (reset save- init-string)]</pre>	<p>This command is available only in CR15i, CR10iNG, CR10wiNG, CR15iNG, CR15wi and CR 15wiNG devices.</p> <p>Enable/Disable serial dial-in or DB9.</p> <p>enable – Enables serial dial-in feature. Modem can be connected to Sophos Firewall's serial (COM) port.</p> <p>disable – Disable serial dial-in feature.</p> <p>modem-nvram to save/reset init string in modem.</p> <p>reset – Reset init string in modem to factory default value</p> <p>save – Save pre-configured init string in modem's memory</p>
<pre>shutdown</pre>	<p>Shutdown Sophos Firewall</p>
<p><u>Load/Unload System Modules</u></p> <pre>system_modules [h323 {load unload} irc {load unload} pptp {load unload} show sip {load unload} tftp {load unload}]</pre>	<p>Load or unload the system modules like h23, irc, sip, tftp</p> <p>By default, all the modules are loaded.</p> <p>Load/unload modules to enhance the network performance and reduce the potential security risk.</p> <p>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.</p> <p>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.</p> <p>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.</p>

	<p>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.</p> <p>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.</p>
<p><u>Wireless WAN</u></p> <p>wwan [disable enable query set show]</p> <p><u>1. To disable WWAN</u> wwan [disable]</p> <p><u>2. To enable WWAN</u> wwan [enable]</p> <p><u>3. Manage WWAN Query options</u> wwan [query {serialport <serial pot number> ATcommand <at command string>}]</p> <p><u>4. Manage WWAN Set options</u> wwan [set {disconnect-on-systemdown (off on)} {modem-setup-delay <number>}]</p> <p><u>5. To display WWAN configuration</u> wwan [show]</p>	<p>Enable or disable wireless WAN and view information of the Wi-Fi modem information (if plugged - in)</p> <p>Wireless WAN menu will be available on Admin Console only when wwan is enabled from CLI.</p>

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 {<ipaddress6> | <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

ping

Sends ICMP ECHO_REQUEST packets to network hosts

Syntax

ping [<ipaddress> | <string> | count | interface | quiet | size | sourceip | timeout]

Parameter list & description

Keywords & Variables	Description
lppaddress	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
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]

Parameter list & description

Keywords & Variables	Description
lppaddress6	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

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

Keywords & Variables	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

Keywords & Variables	Description
flush-cache	Flush entire route cache
lookup	Route lookup

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]

Keywords & Variables	Description
<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' 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 | max-ttl | probes | source | timeout | tos]

Keywords & Variables	Description
<ipaddress6> [size <number>]	Set the IPv6 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
max-ttl	Set the max time-to-live

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

connections

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

Syntax

connections [count | v4 | v6]

Parameter list & description

Keywords & Variables	Description
count <number>	Count of current connections
v4 [delete show]	View and delete IPv4 connections
v6 [delete show]	View and delete IPv6 connections

enableremote

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

Syntax

enableremote [port <number> | serverip <ipaddress>]

Parameter list & description

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

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

set

Set entities

Syntax

set [[advanced-firewall](#) | [arp-flux](#) | [http_proxy](#) | [ips](#) | [ips_conf](#) | [network](#) | [on-boxreports](#) | [proxy-arp](#) | [service-param](#) | [vpn](#) | [lanbypass](#) | [report-disk-usage](#) | [fqdn-host](#) | [business-policy](#) | [port-affinity](#)]

Parameter list & description

Keywords & Variables	Description
advanced-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>>} sys-traffic-nat {add (destination <ipaddress> delete (destination <ipaddress>)} fragmented-traffic <allow deny> ftpbounce-prevention <control data> midstream-connection-pickup <on off> strict-icmp -tracking <on off> strict-policy <on off> tcp-appropriate-byte-count <on off> tcp-est-idle-timeout <2700 - 432000> tcp-frto <on off> tcp-selective-acknowledgement <on off> tcp-seq-checking <on off> tcp-timestamp <on off> tcp-window-scaling <on off>]	Configure advanced firewall settings. bypass-stateful-firewall-config – Add host or network when the outbound and return traffic does not always traverse through Sophos Firewall. 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. 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. midstream-connection-pickup - Configure midstream connection pickup settings. Enabling midstream pickup of TCP connections will help while plugging in the Sophos 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, Sophos Firewall is configured to drop all untracked (mid-stream session) TCP connections in both the deployment modes.

strict-icmp-error-tracking - Allow or Drop ICMP reply packets. Setting this option 'on' drops all ICMP reply packets.

strict-policy on - Applies strict firewall policy. It drops UDP Dst Port 0, TCP Src Port 0 and/or Dst Port 0, Land Attack, Winnuke Attack, Data On TCP Sync, Zero IP Protocol, TTL Value 0 traffic.

strict-policy off - Disables strict firewall policy

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

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-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-seq-checking -

Every TCP packet contains a Sequence Number (SYN) and an Acknowledgement Number (ACK). Sophos 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.

	<p>Default – ON</p> <p>tcp-timestamp Off – Disables timestamps. Timestamp is a TCP option used to calculate the Round Trip Measurement in a better way than the retransmission timeout method.</p> <p>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.</p>
<p>arp-flux [on off]</p>	<p>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 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 Firewall has multiple physical connections to the same medium or broadcast domain.</p> <p>on - Sophos Firewall may respond to ARP requests from both Ethernet interfaces when Sophos Firewall has multiple physical connections to the same medium or broadcast domain.</p> <p>off - Sophos Firewall responds to ARP requests from respective Ethernet interface when Sophos Firewall has multiple physical connections to the same medium or broadcast domain.</p>
<p>http_proxy [add_via_header <on off > relay_invalid_http_traffic <on off> core_dump <on off >]</p>	<p>Set proxy parameters</p> <p>add via header - Default – ON</p>
<p>ips</p>	<p>Configure IPS settings</p>
<p><u>Set Network Interface Parameters</u></p> <p>network [interface-speed mtu-mss macaddr lag-interface]</p> <p><u>1. Set Interface Speed Settings</u></p> <p>network [interface-speed {port <port name> speed (1000fd 1000hd 100fd 100hd 10fd 10hd auto)}]</p> <p><u>2. Set MTU-MSS</u></p> <p>network [mtu-mss {port <port name> mtu <number default> mss <number default>}]</p> <p><u>3. Set MAC Address</u></p> <p>network [macaddr {port <port name> (default override)}]</p>	<p>Configure network interface parameters</p> <p>interface speed - Speed mismatch between Sophos Firewall and third party routers and switches can result into errors or collisions on interface, no connection or traffic latency, slow performance.</p> <p>mss – Maximum Segment Size – It defines the amount of data that can be transmitted in a single TCP packet</p> <p>Range – 576 – 1460 bytes</p> <p>mtu - Maximum Transmission Unit - It specifies the largest physical packet size, in bytes, that a network can transmit. This parameter becomes an issue when networks are interconnected and the networks have different MTU sizes. Any packets larger than the MTU value are divided (fragmented) into smaller packets before being sent.</p> <p>Default – 1500 bytes</p>

4. Set LAG Interface Properties

`network [lag-interface {port <port name> (lag-mgt | link-mgt)}]`

Set LAG related properties

- Set the LAG mode

`lag-mgt mode {802.3ad | active-backup}`

- Set properties for active-backup mode

`lag-mgt active-backup {primary interface <interface name> | auto} failback-policy <link-speed | none | takeover>`

- Set properties for LACP (802.3ad) mode

`lag-mgt lacp {lacp-rate <fast | slow> static-mode <disable | enable>`

`xmit-hash-policy <layer2 | layer2+3 | layer3+4>`

Set Link related properties

`link-mgt {monitor-interval <1 – 10000> | up-delay <0 – 10000> | down-delay <0 – 10000> | garp-count <0 – 255>}`

MTU size is based on addressing mode of the interface.

Range – 576 – 1500 bytes for static mode

Range – 576 – 1500 bytes for DHCP mode

Range – 576 – 1492 bytes for PPPoE mode

`mcaddr` – Configure MAC Address for the available network interfaces.

Note:

- LAG interface properties can be configured or edited from command line but a LAG interface cannot be added from CLI.
- One or more LAG interface must be configured in the device to be able to configure or edit LAG interface properties from CLI.

`lag-interface` – Configure or edit LAG interface properties.

`lag-mgt` – Configure the LAG mode and its properties. LAG supports two modes:

- Active-Backup: Provides automatic link failover facility. In this a single slave remains active. If the active slave fails then other slave in the LAG becomes the active slave.

`failback-policy` – Sophos Firewall decides failback interface based on 3 criteria:

1. `link-speed`: failback is done if speed of the failed active slave is greater than the current active slave interface.
2. `takeover`: failback is done, irrespective of the speed of rest of member interfaces.
3. `none`: failback is never done.

Note that 'failback-policy' is applicable only when a LAG interface is configured using 3 or more member interfaces.

- LACP (802.3ad): Provides load balancing and automatic failover. In this mode all the links are used for serving the traffic.

`static-mode` – You must enable static-mode if the terminating network device does not support LACP.

`link-mgt` – Configure Link related properties for the LAG interface.

	<p>monitor-interval – Set interval for monitoring link state, in milliseconds. Sophos Firewall will check link status of each participant interface, as per the configured monitor interval.</p> <p>Range – 1 – 10000</p> <p>up-delay – Set the time, in milliseconds, to wait before enabling a slave after a link recovery has been detected.</p> <p>Range – 0 – 10000</p> <p>down-delay – Set the time, in milliseconds, to wait before disabling a slave after a link failure has been detected.</p> <p>Range – 0 – 10000</p> <p>garp-count – Set number of garp packets to be sent to the terminating network device.</p> <p>Range – 0 – 255</p> <p>Note: garp-count is not supported in LACP (802.3ad) mode.</p>
<p>on-box-reports [on off]</p>	<p>Generate on-box reports</p> <p>Default – ON.</p>
<p>proxy-arp [add [interface Port<port name> dst_ip <ipaddress> dst_iprange (from_ip <ipaddress> to_ip <ipaddress>) del [interface Port<port number> dst_ip <ipaddress> dst_iprange (from_ip <ipaddress> to_ip <ipaddress>)]]</p>	<p>Add and delete proxy ARP</p>
<p>service-param [FTP {add delete} HTTP {add delete} HTTPS {deny_unknown_proto <on off> invalid_certificate <allow block> } IMAP {add delete} IM_MSN {add delete} IM_YAHOO {add delete} POP {add delete} SMTP {add delete failure_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> }]</p>	<p>By default, Sophos 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 non-standard ports also.</p> <p>add Port<port name > – enable inspection for a specified port number.</p> <p>delete Port<port name> - disable inspection for a specified port number.</p> <p>deny_unknown_proto - Allow/deny traffic not following HTTPS protocol i.e. invalid traffic through HTTPS port</p> <p>Default – ON</p>

	<p>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 Firewall blocks all such sites. Use this command, if you want to allow access to such sites.</p> <p>Note for SMTPS scanning:</p> <p>CA certificate used by Sophos Firewall to sign certificate should be added in the certificate store of your Email client.</p>
<p>vpn [l2tp {authentication (ANY CHAP MS_CHAPv2 PAP)} {mtu <number>} pptp {authentication (ANY CHAP MS_CHAPv2 { encryption (NONE SOME STRONG WEAK) } PAP)]</p>	<p>Set authentication protocol for l2tp and pptp connections.</p> <p>For l2tp, Maximum Transmission Unit (MTU) can be configured.</p> <p>MTU range: 576 – 1460</p> <p>Default: 1410</p>
<p>lanbypass [off on]</p>	<p>Enable/disable Lan Bypass</p>
<p>report-disk-usage [watermark <number>]</p>	<p>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.</p> <p>Watermark range: 60 – 85</p> <p>Default – 80%</p> <p>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.</p> <p>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.</p>
<p>fqdn-host [{cache-ttl <number> dns-reply-ttl idle-timeout {<number default }}]</p>	<p>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.</p> <p>Range: 1 – 86400 seconds</p> <p>Default – 3600 seconds</p> <p>dns-reply-ttl – use the ttl value in DNS reply packet as cache-ttl</p> <p>The idle-timeout value represents the time (in seconds) after which the cached FQDN Host to IP Address binding is removed.</p> <p>Range: 60 – 86400 seconds</p> <p>Default – 3600 seconds</p>

business-policy application-server <code>{{failover mail-notification (disable enable)}}</code>	Enable/disable mail notification for Fail-over of your application server.
port-affinity <code>[add {port <Port Name> (bind-with <cpu> start-with <cpu> cpu <CPU Core>} defsetup del { port <Port Name> } fwonlysetup]</code>	<p>Configure Port Affinity settings. Administratir 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.</p> <p>By default, your device is shipped with the factory-default Port Affinity settings.</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ In Cyberoam devices, Port-affinity is visible only in CR 35iNG and above. ▪ CPU Cores can be assigned to the binded Interfaces only. ▪ Port-affinity is not supported with 'Legacy Network Adaptors', when Cyberoam Virtual Security appliance is deployed in Microsoft Hyper-V.
Add IPS configuration entry ips_conf <code>[add key <text> del {key <text> update <key>]</code>	Use this to add, delete or edit an existing IPS configuration entry.

ips

Configure IPS settings

Syntax

ips [enable_appsignatures | [http_response_scan_limit](#) | ips-instance | ips_mmap | lowmem-settings | maxpkts | maxsesbytes-settings | packet-streaming]

Parameter list & description

Keywords & Variables	Description
enable_appsignatures [on off]	<p>Set enable appsignature ON or OFF</p> <p>on – Set enable appsignature ON</p> <p>off – Set enable appsignature OFF</p>
http_response_scan_limit [<number>]	<p>Specify maximum file size (in KB) for scanning. Files exceeding this size received through HTTP will not be scanned.</p> <p>Default – 64 KB</p>

ips-instance [add apply clear]	<p>Manipulate number of IPS process instances created by init process</p> <p>add – Add IPS instance to the init list</p> <p>apply – Start IPS processes as given in the list</p> <p>clear – Clear IPS list for init process</p>
ips_mmap [off on]	<p>Enable mmap to optimize RAM usage, especially in low-end devices.</p> <p>on – enable ips mmap</p> <p>off – disable ips mmap</p> <p>Default - on</p>
lowmem-settings [off on]	<p>Set whether low memory settings to be applied or not.</p> <p>Low memory settings are applied in case of system having memory issues.</p> <p>on – enable low memory settings</p> <p>off – disable low memory settings</p>
maxpkts [<number> all default]	<p>Set number of packets to be sent for Application Classification</p> <p>number – any number above 8</p> <p>all - pass all of the session packets for application classification</p> <p>default - pass first 8 packets of the session of each direction for application classification (total 16)</p>
maxsesbytes-settings [update <number>]	<p>maxsesbytes-settings allows you to set the maximum allowed size. Any file beyond the configured size is bypassed and not scanned.</p> <p>Update – set the value for maximum bytes allowed per session</p>
packet-streaming [on off]	<p>Set whether packet streaming is to be allowed or not.</p> <p>packet-streaming is used to restrict streaming of packets in situations where system is experiencing memory issues.</p> <p>on - Enables packet streaming.</p> <p>off - disable packet streaming.</p>

show

Displays various parameters configured

Syntax

show [[advanced-firewall](#) | [arp-flux](#) | [business-policy](#) | [country-host](#) | [date](#) | [fqdn-host](#) | [http_proxy](#) | [ips_conf](#) | [ips-settings](#) | [lanbypass](#) | [network](#) | [on-box-reports](#) | [pppoe](#) | [port-affinity](#) | [proxy-arp](#) | [report-disk-usage](#) | [service-param](#) | | [vpn](#)]

Keywords & Variables	Description
advanced-firewall	Shows firewall configuration <ol style="list-style-type: none"> 1. Strict policy, 2. FtpBounce Prevention 3. TCP Conn. Establishment Idle Timeout 4. Fragmented Traffic Policy 5. Midstream Connection Pickup 6. TCP Seq Checking 7. TCP Window Scaling 8. TCP Appropriate Byte Count 9. TCP Selective Acknowledgements 10. TCP Forward RTO-Recovery[F-RTO] 11. TCP TIMESTAMPS 12. Strict ICMP Tracking
arp-flux	Displays ARP – Flux status
<p><u>View Country-Host listing and IP Address to Country mapping</u></p> <p><u>To enlist the countries</u></p> <p>country-host {list}</p> <p><u>To map IP Address to its country</u></p> <p>country-host {ip2country ipaddress <IP Address>}</p>	<ol style="list-style-type: none"> 1. Command: show country-host list To enlist all the countries for which the policies are configured. 2. Command: show country-host ip2country ipaddress <IP Address> Shows the name of country to which the given IP Address belongs.
date	Shows system date and time
fqdn-host	Shows fqdn-host status
http_proxy [add_via_header]	Displays information about HTTP Proxy
ips_conf	Shows IPS configuration entries
ips-settings	Shows IPS engine settings
lanbypass	Shows whether Lan bypass is on/off
<p>network [interface-speed <Port> interfaces macaddr <Port> mtu-mss <Port> lag-interface static-route static-route6]</p>	<p>interface-speed – Shows current interface speed settings.</p> <p>interfaces – Shows all network interfaces configuration</p> <p>Note:</p> <p>One or more LAG interface must be configured in the device to be able to view its configuration using the SHOW command from CLI.</p> <p>macaddr – Shows original and overridden mac address of interface.</p>

	mtu-mss – Shows mtu and mss of interface.
on-box-reports	Shows whether On-box reporting is On/Off
pppoe [connection status]	Shows all configured PPPoE connection status
port-affinity	Displays network device to CPU mapping
proxy-arp	Displays configured Proxy ARP on the interfaces
report-disk-usage [watermark]	Reports disk usage configurations
service-param	Displays configured non-standard parameters of services
business-policy application-server [failover mail-notification]	Displays mail notification status for application server failover/failback event
vpn [connection IPsec-logs configuration PPTP-logs L2TP-logs]	Displays VPN settings. connection – Shows vpn connection status IPsec-logs – Shows IPsec VPN logs configuration – Shows whether PPTP and L2TP is configured or not PPTP-logs – Shows PPTP VPN logs L2TP-logs – Shows L2TP logs

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

Keywords & Variables	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) preceded 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'
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

Keywords & Variables	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

Keywords & Variables	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.

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:

1. Reset configuration
2. Reset configuration and signatures
3. Reset configuration, signatures and reports

Appendix A – DHCP Options (RFC 2132)

A DHCP server can provide optional configurations to the client. Sophos 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
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 interval	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 Servers Addresses	NTP servers 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 Server	X window font server	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
55	Parameter Request List	Parameter request list	Array of One Byte Numeric Values
56	Message	DHCP error message	String
57	DHCP Maximum Message	DHCP maximum message size	Two Byte Numeric Value

	Size		
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 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