SOPHOS
Security made simple.

Pocket Guide

Configure Active-Active High Availability (HA)

Product: Sophos XG Firewall

Contents

Overview

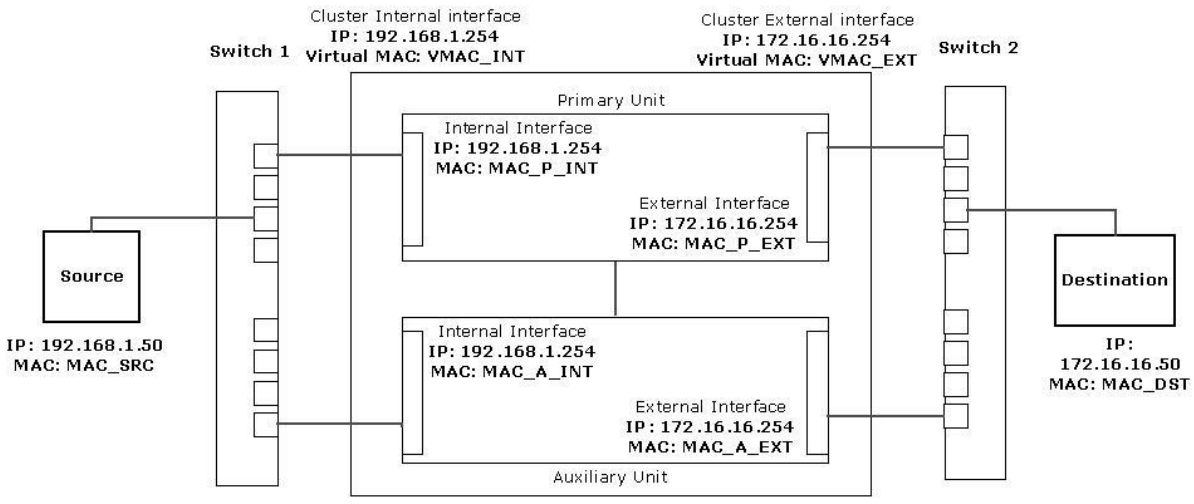
Sophos XG Firewall devices can be configured in Active-Active or Active-Passive High Availability (HA) modes to provide uninterrupted services in the event of power, hardware or software failures. The primary and auxiliary devices are physically connected over a dedicated HA link port to act as a 'cluster'.

In active-active mode, once traffic enters the network through a network switch, it is forwarded to the primary device which carries a virtual MAC address. The primary device load balances and forwards traffic to the peer, that is, the auxiliary device.

In active-passive mode, the primary device processes the entire traffic. The auxiliary device waits in ready mode to operate as the primary device when the primary device or a monitored link fails.

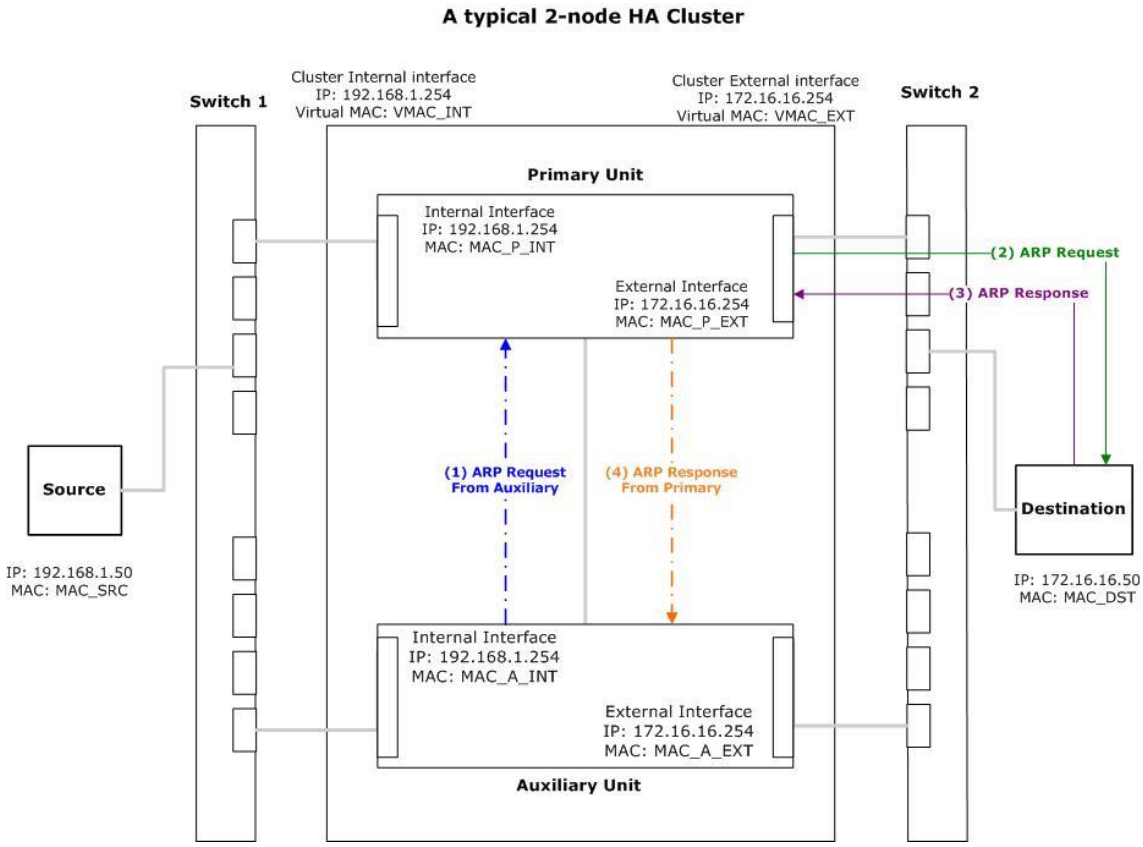
The auxiliary device monitors the primary device. If it does not receive communication from the primary device at preset intervals, the primary device is deemed to have failed and the auxiliary device takes ownership of the virtual MAC address, becoming the temporary primary device. Once the primary device becomes functional, it automatically takes over from the auxiliary device.

A typical 2-node HA Cluster



Note:
1. Only one internal and one external interface are shown for each unit in the cluster for simplicity. Actual setup may have more interfaces on each unit

ARP



Scenario

This guide describes how to configure Active-Active cluster of two Sophos XG Firewall devices.

Models that do not support HA

All wireless models of XG, SG and CR series as well as CR15i

HA Behavior

- DHCP, PPPoE, WWAN: HA cannot be configured on dynamically assigned interfaces, that is, through DHCP and PPPoE.
- Alias and VLAN cannot be configured on the dedicated link port.
- All masqueraded connections are dropped during manual synchronization events from one of the HA cluster devices.
- Quarantined Mails:
    - Mails are quarantined separately on both the devices because SMTP Proxy traffic is load balanced in round robin manner.
    - If Quarantine Digest is configured, both the devices will send the Quarantine Digest.
    - Administrator can release the quarantined mails of all users from both the devices.

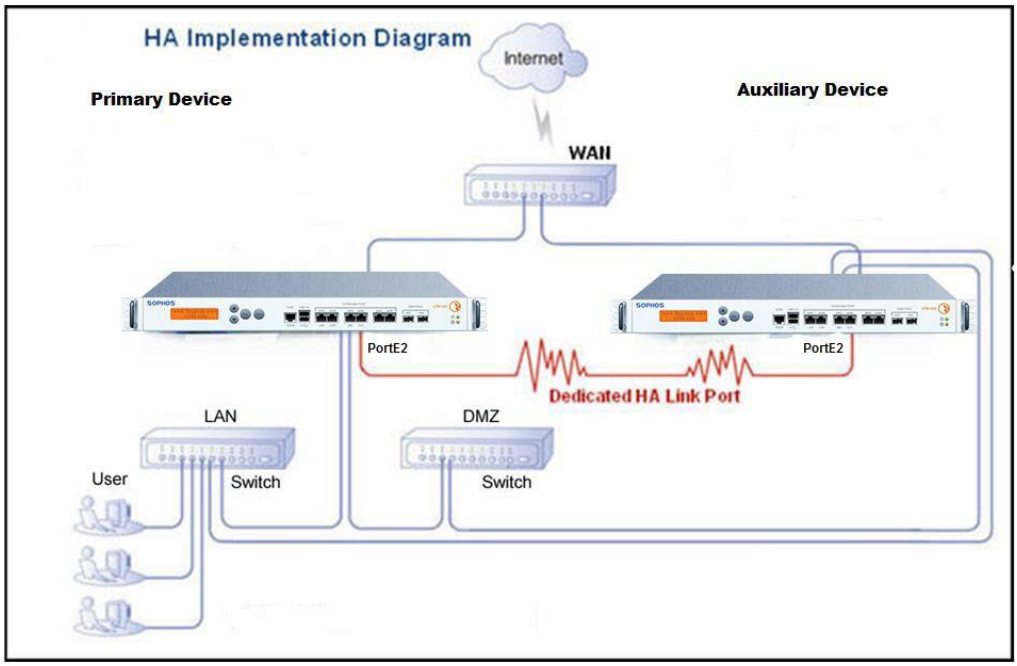
    - Users can release quarantined mails from the Quarantine Digest after logging into the user portal. The user portal displays mails quarantined of only the primary device.
- Deployment Wizard
    - HA is disabled if you run the Deployment Wizard.
    - The Deployment Wizard is not accessible from the auxiliary device.

Prerequisites

- You must have read-write permissions on the SF-OS Admin Console of both devices for the relevant features.
- Both devices in the HA cluster must:
    1. be of the same model
    2. have the same number of ports
    3. be of the same SF-OS version

- On both the devices, the same set of subscription modules must be licensed and enabled. However, expiry dates of the subscription modules can be different.
- Both the devices must be physically connected through a cable. Cables must be connected to all the monitored ports of both the devices. We recommend that you connect the dedicated HA link port of both the devices with the crossover cable.
- Dedicated Link Port on both devices must be the member of DMZ zone only, must have a unique IP Address and must have default link speed and MTU-MSS.
- IP Address of the HA link port of the primary and auxiliary devices must be in the same subnet.
- DHCP, PPPoE, WWAN and WLAN configuration must be disabled before HA configuration.
- Monitoring ports are up.

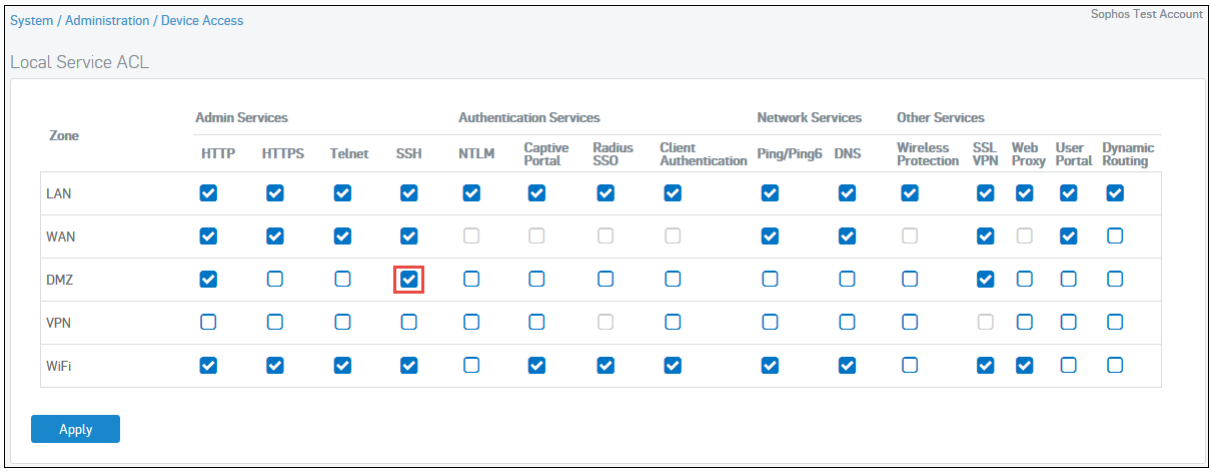
Configuration



Step 1: Configure the Auxiliary Device

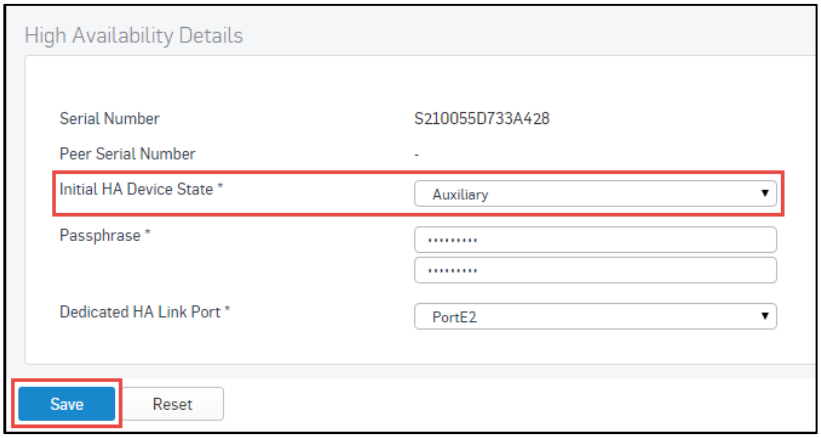
Log in to the device to be configured as the auxiliary device.

a. Enable SSH services for DMZ zone from **System > Administration > Device**



b. Configure HA parameters from Configure > System Services > High Availability

1. Set **Initial HA Device State** to **Auxiliary**
2. Set **Passphrase.** This passphrase must be entered in the primary device.

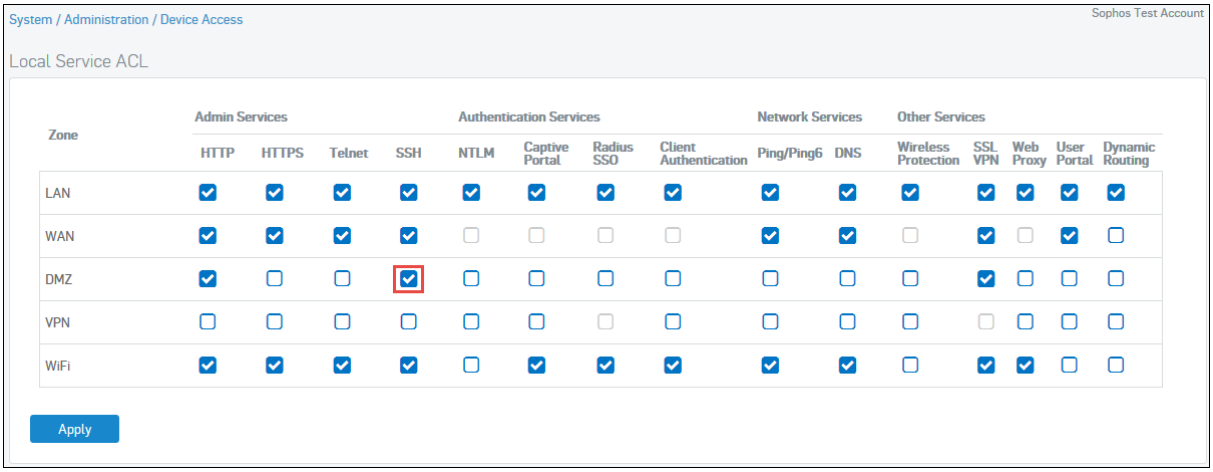


Click **Save**.

Step 2: Configure the Primary Device

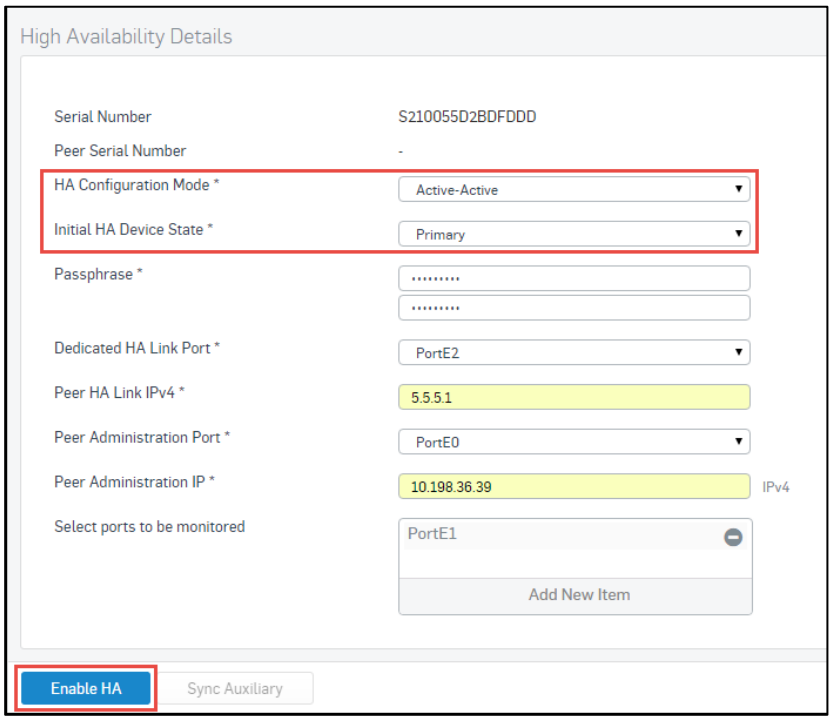
Log in to the device to be configured as the primary device.

a. Enable SSH services for DMZ zone from **System > Administration > Device**



b. Configure HA parameters from Configure > System Services > High Availability

1. Set **HA Configuration Mode** to **Active-Active.**
2. Set **Initial HA Device State** to **Primary** .
3. Enter the **Passphrase** which was entered on the auxiliary device.



Note:
Only administrators with Device Access Profile – HAProfile, can access the auxiliary device using the IP address configured in Peer Administration IP.

Click **Enable HA.**

Step 3: Verify HA status from the Primary device

If cabling and configuration is correct and HA has been enabled successfully:

1. Both the appliances carry the same configuration except the HA link port IP Address.
2. Additional options made available after HA is enabled:

   Primary Device: Disable HA, Sync Auxiliary (to synchronize auxiliary device and primary device configurations)
   Auxiliary Device: Disable HA, Sync Primary (to synchronize auxiliary device and primary device configurations)
3. By default, as soon as HA is enabled successfully, both the appliances will synchronize automatically.

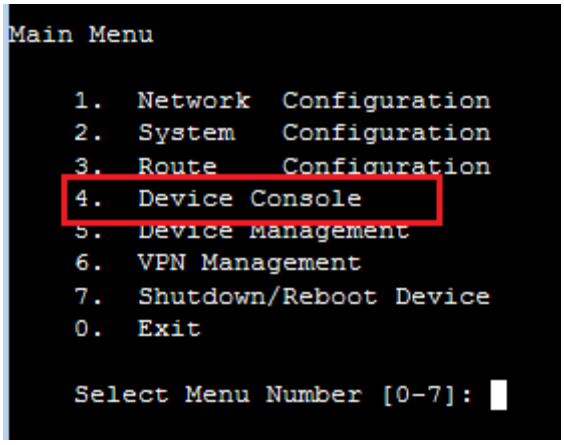
HA status can be verified from:

1. Control Center

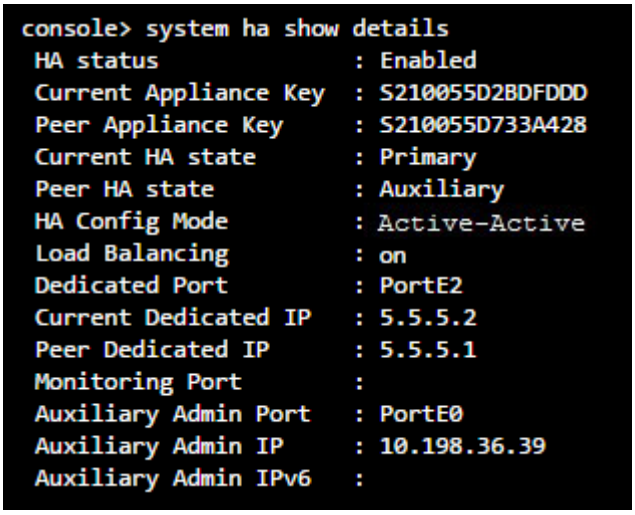
System panel of Control Center must display the configured mode: “High Availability A-A”.

2. CLI console

a. Select option **4. Device Console** from the **Main Menu** list



b. Execute the following command at the console prompt:
Console > system ha show details



Result

Both primary and auxiliary devices will process traffic. Traffic load balancing is enabled and the primary device is in charge of balancing the traffic. You can disable this from the CLI console using the "**system ha load-balancing off**" command. The auxiliary device takes over only when the primary device fails.

Traffic Load Balancing and Session Failover for Active-Active Cluster

Traffic	Load Balancing	Session failover
Forwarded TCP traffic	Yes	Yes
Proxy Subsystem (Transparent/Direct)	Yes	No
VPN Traffic	No	No
IPv4 and IPv6 forwarded traffic like UDP, ICMP, multicast, broadcast, etc.	No	No
System-generated traffic	No	No
AV Scanned sessions		No
Parent proxy traffic		No
NATed traffic	Yes	No
HTTPS connection	Yes	No
VLAN traffic	Yes	No
Traffic coming through wireless RED devices and Access Points	No	No
TCP Traffic for User Portal, Admin Console or Telnet Console	No	No
H323 Traffic sessions	No	No
Scanned FTP traffic	No	No

Manually Synchronizing HA Peers

The auxiliary device synchronizes automatically with the primary device. You can also forcefully synchronize it with the primary device.

Manual synchronization can be initiated from either of the devices. If synchronized from the primary device, the primary device pushes the updates. If synchronized from the auxiliary device, the auxiliary device pulls the updates from the primary device.

Go to **Configure > System Services > High Availability** and click **Sync Auxiliary** to manually synchronize the auxiliary device with the primary device.

With manual synchronization, you receive all the data and configuration updates except reports from the primary device.

(Optional) Upgrading Firmware for HA Cluster

When a new version of the SF-OS firmware becomes available, firmware on both the devices can be upgraded with zero downtime.

Upgrade Flow:

1. Upload firmware on the primary device
2. Primary device upgrades the secondary device
3. Secondary device comes up with the new version and takes control
4. Primary device upgrades and comes up with the new firmware
5. HA is active

Suggested Readings

1. Disable HA
2. Backup and Restore

Copyright Notice