

SOPHOS

Security made simple.



Pocket Guide

Configure Active-Passive High
Availability (HA)

Product: Sophos XG Firewall

Contents

Overview.....	3
Scenario	4
Models that do not support HA.....	4
HA Behavior	4
Prerequisites	5
Configuration	5
Step 1: Configure the Auxiliary Device	6
a. Enable SSH services for DMZ zone from System > Administration > Device.....	6
b. Configure HA parameters from Configure > System Services > High Availability.....	6
Step 2: Configure the Primary Device	7
b. Configure HA parameters from Configure > System Services > High Availability.....	7
Step 3: Verify HA status from the Primary Device	8
Result	9
Session Failover for Active-Passive Cluster.....	9
Manually Synchronizing HA Peers.....	10
Suggested Readings.....	10
Copyright Notice	11

Overview

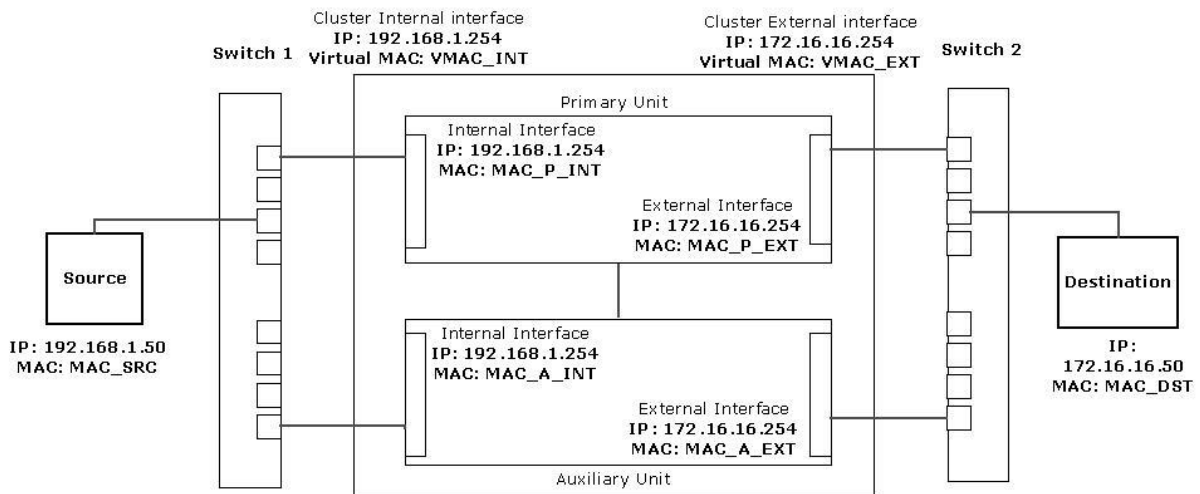
Sophos XG Firewall devices can be configured in Active-Active or Active-Passive High Availability (HA) modes to provide uninterrupted services in the event of power, hardware or software failures. The primary and auxiliary devices are physically connected over a dedicated HA link port to act as a 'cluster'.

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.

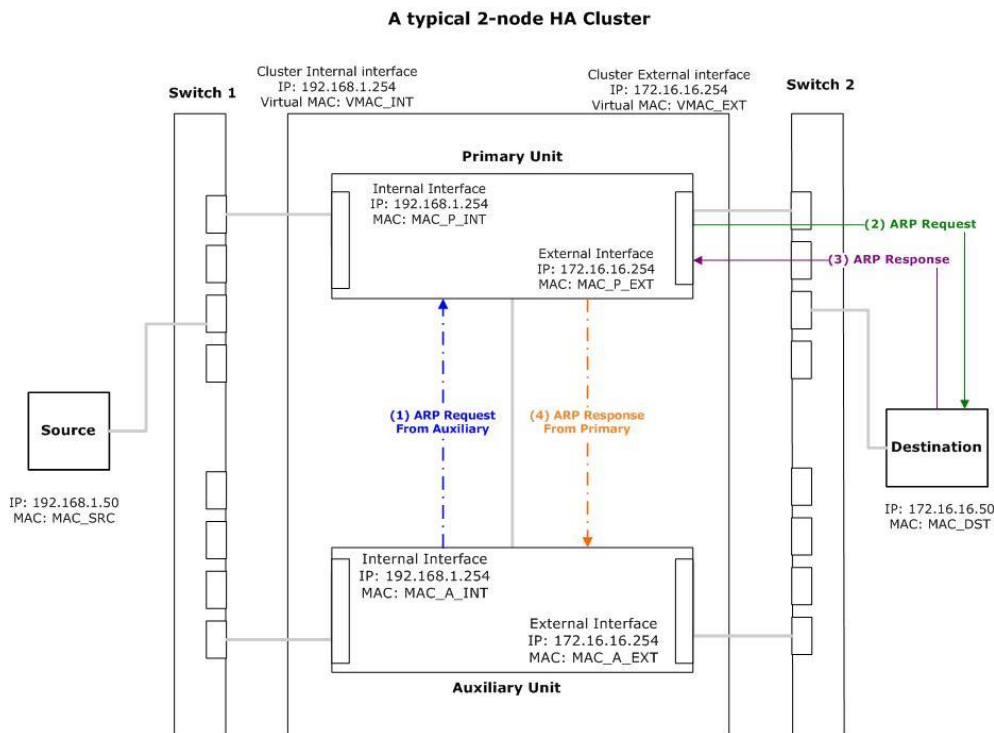
The auxiliary device monitors the primary device. If it does not receive communication from the primary device at preset intervals, the primary device is deemed to have failed and the auxiliary device takes ownership of the virtual MAC address, becoming the temporary primary device. Once the primary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

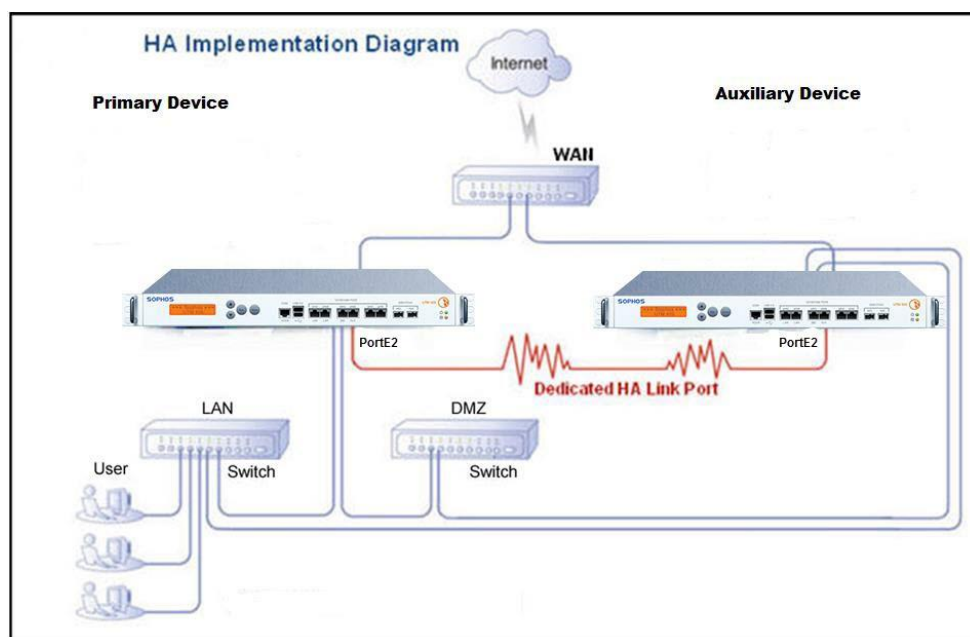
- Software and Virtual Appliances: Activation and registration of the auxiliary device is not required.
- Subscription Licenses: Required only for the primary (active) device. These licenses are used in the cluster.
- DHCP, PPPoE, WWAN: HA cannot be configured on dynamically assigned interfaces, that is, on 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 on the primary device.
 - If Quarantine Digest is configured, both the devices 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
- 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 must be 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**

Zone	Admin Services			Authentication Services				Network Services		Other Services					
	HTTP	HTTPS	Telnet	SSH	NTLM	Captive Portal	Radius SSO	Client Authentication	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Web Proxy	User Portal	Dynamic Routing
LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DMZ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VPN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WiFi	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply

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.

High Availability Details

Serial Number: S210055D733A428

Peer Serial Number: -

Initial HA Device State *

Passphrase *

Dedicated HA Link Port *

Save Reset

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**

System / Administration / Device Access Sophos Test Account

Local Service ACL

Zone	Admin Services			Authentication Services				Network Services		Other Services					
	HTTP	HTTPS	Telnet	SSH	NTLM	Captive Portal	Radius SSO	Client Authentication	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Web Proxy	User Portal	Dynamic Routing
LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DMZ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VPN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WiFi	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

1. Set **HA Configuration Mode** to **Active-Passive**.
2. Set **Initial HA Device State** to **Auxiliary**.
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.

High Availability Details

Serial Number: S210055D2BDFDDD

Peer Serial Number: -

HA Configuration Mode *

Initial HA Device State *

Passphrase *

Dedicated HA Link Port *

Peer HA Link IPv4 *

Peer Administration Port *

Peer Administration IP * IPv4

Select ports to be monitored

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)

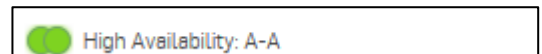
Auxiliary Device: Disable HA, Sync Primary (to synchronize auxiliary device and primary device configurations)

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

```
console> system ha show details
HA status           : Enabled
Current Appliance Key : S210055D2BDFDD0
Peer Appliance Key   : S210055D733A428
Current HA state     : Primary
Peer HA state        : Auxiliary
HA Config Mode       : Active-Active
Load Balancing       : on
Dedicated Port       : PortE2
Current Dedicated IP : 5.5.5.2
Peer Dedicated IP    : 5.5.5.1
Monitoring Port      :
Auxiliary Admin Port : PortE0
Auxiliary Admin IP   : 10.198.36.39
Auxiliary Admin IPv6 :
```

Result

The primary device will process the traffic. The auxiliary device takes over only when the primary device fails.

Session Failover for Active-Passive Cluster

Traffic	Session failover
Forwarded TCP traffic	Yes
Proxy Subsystem (Transparent/Direct)	No
VPN Traffic	No
IPv4 and IPv6 traffic other than TCP. Example: UDP, ICMP, multicast, broadcast etc.	No
System-generated traffic	No
AV-Scanned sessions	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.

Suggested Readings

1. Disable HA
2. Backup and Restore

Copyright Notice

Copyright 2015-2016 Sophos Limited. All rights reserved.

Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.