

SOPHOS

Security made simple.



Pocket Guide

Disable High Availability (HA)

Product: Sophos XG Firewall

Contents

Scenario	3
Prerequisites	3
Configuration	3
Disable from Admin console	3
Disabling HA from CLI.....	4
Behavior after disabling HA.....	4
Result.....	4
Copyright Notice	5

Scenario

This guide describes how to disable High Availability (HA) cluster between two Sophos XG Firewall devices.

Prerequisites

- You must have read-write permissions for the relevant features on the SF-OS Admin Console of the device from which HA is to be disabled.
- You must have super administrator privileges for CLI.

Configuration

1. You can disable HA from the Admin Console or from CLI of both the devices: If disabled from the primary device, HA is disabled on both the devices.
2. If disabled from the auxiliary device, HA is not disabled on the primary device which continues to act as a stand-alone device.

Disable from Admin console

1. Log in to the device from which you want to disable HA.
2. Go to **Configure > System Services > High Availability**.
3. Click **Disable HA**.

High Availability Details

Serial Number	S21005502BDFDDD Primary
Peer Serial Number	S2100550733A428 Auxiliary
HA Configuration Mode *	Active-Active
Dedicated HA Link Port *	PortE2
Peer HA Link IPv4 *	7.7.7.1
Peer Administration Port *	PortE0
Peer Administration IP *	10.198.36.39 IPv4
Select ports to be monitored	PortE1
	Add New Item

Disabling HA from CLI

1. Log in to the device from which you want to disable HA.
2. Choose option 4 **Device Console**.

```
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]:
```

3. Execute the command: *system ha disable*

```
console> system ha disable
```

```
console> system ha disable
console> system ha show details
HA is disabled.

console>
```

Behavior after disabling HA

1. IP schema of the primary device does not change.
2. Auxiliary device reboots and all the ports are disabled except the Dedicated HA link port and Peer Administration port.
 - a. Peer HA Link IP address is assigned to the Dedicated HA Link Port
 - b. Peer Administration IP Address is assigned to the Peer Administration Port
3. Auxiliary device:
 - a. LAN zone: All administrative services (HTTP, HTTPS, Telnet, SSH) are allowed
 - b. DMZ zone: Only HTTPS and SSH are allowed

Result

All the traffic is processed by the primary device.

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.