Upgrade FTD HA Managed by FDM

Contents

Introduction
Prerequisites
Requirements
Components Used
Overview
Background Information
Configure
Step 1. Upload Upgrade Package
Step 2. Check Readiness
Step 3. Upgrade FTD in HA
Step 4. Switch Active Peer (Optional)
Step 5. Final Deploy
Validate

Introduction

This document describes the upgrade process for a Cisco Secure Firewall Threat Defense in High Availability managed by a Firepower Device Manager.

Prerequisites

Requirements

Cisco recommends you have knowledge of these topics:

- High Availability (HA) concepts and configuration
- Cisco Secure Firepower Device Manager (FDM) configuration
- Cisco Secure Firewall Threat Defense (FTD) configuration

Components Used

The information in this document is based on Virtual Cisco FTD, version 7.2.8.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

The way the FDM works is to upgrade one peer at a time. First the Standby, then the Active, doing a failover before the Active upgrade gets started.

Background Information

The upgrade package must be downloaded from **software.cisco.com** before the upgrade.

On CLI clish, run the**show high-availability config**command in the Active FTD in order to check the status of the HA.

> show high-availability config Failover On Failover unit Primary Failover LAN Interface: failover-link GigabitEthernet0/2 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 3 of 311 maximum MAC Address Move Notification Interval not set failover replication http Version: Ours 9.18(3)53, Mate 9.18(3)53 Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C Last Failover at: 11:57:26 UTC Oct 8 2024 This host: Primary - Active Active time: 507441 (sec) slot 0: ASAv hw/sw rev (/9.18(3)53) status (Up Sys) Interface diagnostic (0.0.0.0): Normal (Waiting) Interface inside (192.168.45.1): Normal (Waiting) Interface outside (192.168.1.10): Normal (Waiting) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up) Other host: Secondary - Standby Ready Active time: 8 (sec) Interface diagnostic (0.0.0.0): Normal (Waiting) Interface inside (0.0.0.0): Normal (Waiting)

```
Interface outside (0.0.0.0): Normal (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
```

If no errors are visible, then proceed with the upgrade.

Configure

Step 1. Upload Upgrade Package

• Upload the FTD upgrade package on the FDM using the GUI.

This has to be previously downloaded from the Cisco Software site based on the FTD model and desired version. Navigate to **Device > Updates > System Upgrade**.



Updates

• Browse for the previously downloaded image, then chooseUpload.



Note: Upload the image on both active and standby nodes.

0	Important
	This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see link 🖸
The	re are no software ungrades available on the system
Unlo	ad an upgrade file to install.

Run Readiness Check

Step 2. Check Readiness

Readiness checks confirm if appliances are ready to proceed with the upgrade.

• Choose Run Upgrade Readiness Check.

System Upgrade Current version 7.2.5-2	208
Important This device is a p precise order. For	eer in a high availability configuration. You must install upgrades in a r details, see link 🗷
File	Cisco_FTD_Upgrade-7.2.8-25.sh.REL Replace file 14 Oct 2024 05:06 PM
Upgrade to	7.2.8-25
Readiness Check	Not Performed Yet Run Upgrade Readiness Check
UPGRADE NOW	Reboot required

Current version 7.2.5	-208
Important This device is a precise order. F	peer in a high availability configuration. You must install upgrades in a for details, see link 🗷
File	Cisco_FTD_Upgrade-7.2.8-25.sh.REL a Replace file 14 Oct 2024 05:06 PM
Upgrade to	7.2.8-25
Readiness Check	Not Performed Yet Run Upgrade Readiness Check
UPGRADE NOW	Reboot required

Run Readiness check

i Important This device is a pr precise order. For	eer in a high availability configuration. You must install upgrades in a details, see link 🖸
File	Cisco_FTD_Upgrade-7.2.8-25.sh.REL Replace file 14 Oct 2024 05:06 PM
Upgrade to	7.2.8-25
Readiness Check	Please Wait
UPGRADE NOW	i Reboot required

Run Readiness Check

The progress can be checked by navigating to **System > Upgrade**.

System Upgrade Current version 7.2.5	e 5-208
 Important This device is a precise order. F 	peer in a high availability configuration. You must install upgrades in a For details, see link 🖸
File	Cisco_FTD_Upgrade-7.2.8-25.sh.REL 14 Oct 2024 05:06 PM
Upgrade to	7.2.8-25
Readiness Check	Precheck Success Run Upgrade Readiness Check 14 Oct 2024 05:51 PM
UPGRADE NOW	Reboot required

Run Readiness Check

The upgrade can be done when the readiness check is completed in both FTD and the result is Success.

Step 3. Upgrade FTD in HA

• Choose Standby FDM and click Upgrade Now.

Important This device is a precise order. F	peer in a high availability co or details, see link 🕐	nfiguration. You must install upgrades in a
File	Cisco_FTD_Upgrade-7. 14 Oct 2024 05:06 PM	2.8-25.sh.REL 💼 Replace file
Upgrade to	7.2.8-25	
Readiness Check	Precheck Success 14 Oct 2024 05:51 PM	Run Upgrade Readiness Check
UPGRADE NOW	Reboot required	

Upgrade Now

Before starting the upgrade:

- 1. Do not start a system restore at the same time as a system upgrade.
- 2. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during the upgrade, if a reboot is necessary.
- 3. Do not power off the deviceduring the upgrade. Interrupting the upgrade can make the system unusable.

You are logged out of the system when the upgrade begins. After the installation is completed, the device is rebooted.

Confirm System Upgrade	<
 Before starting the upgrade: 1. Do not start a system restore at the same time as a system upgrade. 2. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during upgrade if a reboot is necessary. 3. Do not power off the device during the upgrade. Interrupting the upgrade can leave the system in an unusable state. You will be logged out of the system when the upgrade begins. After the installation completes, the device will be rebooted. UPGRADE OPTIONS Automatically cancel on upgrade failure and roll back to the previous version 	
CANCEL	

Continue



Note: Upgrade takes around 20 min per FTD.

On CLI, progress can be checked in the upgrade folder /ngfw/var/log/sf; move to**expert mode**and enter**root** access.

> expert

admin@firepower:~\$ sudo su

Password:

root@firepower:/home/admin# cd /ngfw/var/log/sf

root@firepower:/ngfw/var/log/sf# ls

Cisco_FTD_Upgrade-7.2.8.

root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# ls -lrt

root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# tail -f status.log

ui: Upgrade in progress: (8% done.22 mins to reboot). Preparing to upgrade... (200_pre/011_check_self. ui: Upgrade in progress: (8% done.22 mins to reboot). Preparing to upgrade... (200_pre/015_verify_rpm. ui: Upgrade in progress: (8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_check_dashb ui: Upgrade in progress: (8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_get_snort_f ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/110_setup_upgra ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/120_generate_au ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/120_generate_au ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/120_generate_au

ui: Upgrade in progress: (79% done. 5 mins to reboot). Finishing the upgrade... (999_finish/999_zz_inst ui: Upgrade in progress: (83% done. 4 mins to reboot). Finishing the upgrade... (999_finish/999_zzz_com ui: Upgrade complete

ui: The system will now reboot.

ui: System will now reboot.

Broadcast message from root@firepower (Mon Oct 14 12:01:26 2024): System will reboot in 5 seconds due to system upgrade.

Broadcast message from root@firepower (Mon Oct 14 12:01:31 2024): System will reboot now due to system upgrade.

Broadcast message from root@firepower (Mon Oct 14 12:01:39 2024): The system is going down for reboot NOW!

Upgrade the second unit.

Switch roles in order to make this device active: Choose **Device> High Availability**, then choose **Switch Mode** from the gear menu. Wait for the status of the unit in order to change to active and confirm that traffic is flowing normally. Then, log out.

Upgrade: Repeat the previous steps in order to log into the new standby, upload the package, upgrade the device, monitor progress, and verify success.



Date/Time

Attaching to Diagnostic CLI \dots Press 'Ctrl+a then d' to detach.

Type help or '?' for a list of available commands.

primary_ha> enable

Password:

primary_ha# show failover state

	State	Last Failure Reason
This host -	Primary	
	Standby Ready	None

Other host - Secondary

Active None

====Configuration State===

Sync Skipped - STANDBY

====Communication State===

Mac set

primary_ha#

Step 4. Switch Active Peer (Optional)



Note: If the Secondary device is Active, it does not have any operational impact.

Having the Primary device as Active and Secondary as Standby is a best practice that helps track any failover that can occur.

In this case, the FTD Active is now Standby, a manual failover can be used to set it back to Active.

• Navigate to **Devices > High Availability**.

Firewall Device Manager Monitoring Policies	Device: firepower	(b) 🚱 🎯 (?) : admin Administrator
Model Cisco Firepower Threat Defense for VMwa	Software VD8 Intrusion Rule Update 7.2.8-25 353.0 20220511-1540	Cloud Services High Assiability Nick Registered Register Primary Device: Standby c? Peer: Active
		di literat
	Cisco-Firepower Threat Defense for VMware	DNS Server
🔁 Inside Herwork		CONCUL
	2	

High Availability

• ChooseSwitch Mode.

Firewall Device Manager Monitoring Policies Objects Device: Enspower	🔈 🚑 🞯 🕐 🗄 admin Administrator	· dine SECURE
Device Summary High Availability		
Primary Device Current Device Mode: Standby # Peer: Active Eallower History Deployment History		C Resume HA
High Availability Configuration	Failover Criteria	O Suspend HA
Select and configure the near desire based on the following characteristics	INTERFACE FAILURE THRESHOLD	88 Break HA
deservation consigned the previous sector on the rowswing transmissions of a	Failure Criteria	+=* Switch Mode
GENERAL DEVICE INFORMATION	Number of failed interfaces exceeds	1
Model Cisco Firepower Threat Defense for VMware		1-211

Switch Mode

• Choose **OK** in order to confirm the failover.

Make This Device the Active Peer	8	×
Please check whether the active unit is currently running a deployment jo switch modes while a deployment job is in progress, the job will fail and y lose your configuration changes. Are you sure you want to switch modes to make this device the active un	b. If yo /ou will it?	u I
CANCEL	ОК	

Active Peer

Validation of HA status at the end of the upgrade and failover done.

Firewall Device Manager Monitoring Polici	s Objects Device: frepower	(admin admin administrator advalue SECURE
Model Cisco Firepower Threat Defense for VI	Software VDB Intrusion Rule Update wa 7.2.8-25 353.0 20220511-1540	Cloud Services High Availability () Not Registered Register Primary Device: Active 2 Pren: Standby
	<u>_</u>	
	Gisco Firepower Threat Defense for Wilware	Ends Server
🔁 Inside Network		SPYNIAL/Gateway

Devices

Step 5. Final Deploy

• Deploy the policy to devices by clicking **DEPLOY NOW** under the Deployment tab.



Donding	Changes
renuing	Changes

0	\sim
v	\sim

~	Last Deployment Completed Successfully 14 Oct 2024 06:26 PM. See Deployment History		
	Deployed Version (14 Oct 2024 06:26 PM)	Pending Version	LEGEND
Ø	Rule Update Version Edited: 20220511-1540		
	lastSuccessSRUDate: 2024-10-08 06:15:04Z	2024-10-14 12:53:26Z lspVersions[1]: 20220511-1540	
0	VDB Version Edited: 353		
O	Snort Version Added: 3.1.21.800-2		
	-	<pre>snortVersion: 3.1.21.800-2</pre>	
	-	<pre>snortPackage: /ngfw/var/sf/snort-3.1.21.800-2/snor name: 3.1.21.800-2</pre>	
0	Data SSL Cipher Setting Edited: DefaultDataSSLCipherSetting		
Ø	SSL Cipher Edited: DefaultSSLCipher		
	-	<pre>protocolVersions[0]: TLSV1</pre>	
	-	<pre>protocolVersions[1]: DTLSV1 protocolVersions[2]: TLSV1 1</pre>	
		h	
Ø	Intrusion Policy Edited: Security Over Connectivity - Cisco Talos		
0	Intrusion Policy Edited: Maximum Detection - Cisco Talos		
М	ORE ACTIONS V	CANCEL DEPLOY NOW	~

Policy Deployment

Validate

In order to validate that HA status and upgrade are complete, you must confirm the status: Primary: Active Secondary: Standby Ready

Both are under the version that is the recently changed one (7.2.8 in this example).

Firewall Device Manager Monitoring Policies	Device: firepower	S 🖨 Ø ? : admin Administrator
Model Cisco Firepower Threat Defense for VMw	Software VDB Intrusion Bule Update 7.2.8-25 353.0 20220511-1540	Cloud Services High Availability @ Not Registered Register Primary Device: Active 🚯 Peer: Standby
	Cisco Firepower Threat Defense for Villmare	Mont Ends Server
C Inside Network		SP/SEAN/Gateway O NTP Server
	60	

Failover

• Over CLI clish, check the failover state using the commands**show failover state**and**show failover**for more detailed information.

Cisco Firepower Extensible Operating System (FX-OS) v2.12.1 (build 73) Cisco Firepower Threat Defense for VMware v7.2.8 (build 25)

> show failover state

	State	Last Failure Reason	Date/Time
This host -	Primary		
	Active	None	
Other host -	Secondary		
	Standby Ready	None	
====Configurat	ion State===		
Sync S	kipped		
====Communicat	ion State===		

Mac set

> show failover

Failover On

Failover unit Primary

Failover LAN Interface: failover-link GigabitEthernet0/2 (up)

Reconnect timeout 0:00:00

Unit Poll frequency 1 seconds, holdtime 15 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 3 of 311 maximum

MAC Address Move Notification Interval not set

failover replication http

Version: Ours 9.18(4)210, Mate 9.18(4)210

Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C

Last Failover at: 14:13:56 UTC Oct 15 2024

This host: Primary - Active

Active time: 580 (sec)

slot 0: ASAv hw/sw rev (/9.18(4)210) status (Up Sys)
Interface diagnostic (0.0.0.0): Normal (Waiting)
Interface inside (192.168.45.1): Normal (Waiting)
Interface outside (192.168.1.10): Normal (Waiting)
slot 1: snort rev (1.0) status (up)

slot 2: diskstatus rev (1.0) status (up)

Other host: Secondary - Standby Ready

Active time: 91512 (sec) Interface diagnostic (0.0.0.0): Normal (Waiting) Interface inside (0.0.0.0): Normal (Waiting) Interface outside (0.0.0.0): Normal (Waiting) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics

Link : failover	-link Gigab	itEthernet()/2 (up)	
Stateful Obj	xmit	xerr	rcv	rerr
General	11797	0	76877	0
sys cmd	11574	0	11484	0

up time	0	0	0	0
RPC services	0	0	0	0
TCP conn	0	0	0	0
UDP conn	176	0	60506	0
ARP tbl	45	0	4561	0
Xlate_Timeout	0	0	0	0
IPv6 ND tbl	0	0	0	0
VPN IKEv1 SA	0	0	0	0
VPN IKEv1 P2	0	0	0	0
VPN IKEv2 SA	0	0	0	0
VPN IKEv2 P2	0	0	0	0
VPN CTCP upd	0	0	0	0
VPN SDI upd	0	0	0	0
VPN DHCP upd	0	0	0	0
SIP Session	0	0	0	0
SIP Tx 0	0	0	0	
SIP Pinhole	0	0	0	0
Route Session	1	0	0	0
Router TD				
Router ib	0	0	0	0
User-Identity	0 0	0	0 30	0 0
User-Identity CTS SGTNAME	0 0 0	0 0 0	0 30 0	0 0 0
User-Identity CTS SGTNAME CTS PAC	0 0 0	0 0 0 0	0 30 0	0 0 0 0
User-Identity CTS SGTNAME CTS PAC TrustSec-SXP	0 0 0 0	0 0 0 0 0	0 30 0 0	0 0 0 0
User-Identity CTS SGTNAME CTS PAC TrustSec-SXP IPv6 Route	0 0 0 0 0	0 0 0 0 0	0 30 0 0 0	0 0 0 0 0
User-Identity CTS SGTNAME CTS PAC TrustSec-SXP IPv6 Route STS Table	0 0 0 0 0 0	0 0 0 0 0 0	0 30 0 0 0 0	0 0 0 0 0
User-Identity CTS SGTNAME CTS PAC TrustSec-SXP IPv6 Route STS Table Umbrella Device	0 0 0 0 0 0 0 -TD 0	0 0 0 0 0 0 0 0 0 0	0 30 0 0 0 0 0 0	0 0 0 0 0
User-Identity CTS SGTNAME CTS PAC TrustSec-SXP IPv6 Route STS Table Umbrella Device Rule DB B-Sync	0 0 0 0 0 0 0 -ID 0	0 0 0 0 0 0 0 0 0 0	0 30 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0
User-Identity CTS SGTNAME CTS PAC TrustSec-SXP IPv6 Route STS Table Umbrella Device Rule DB B-Sync Rule DB P-Sync	0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 30 0 0 0 0 0 0 0 30 266	0 0 0 0 0 0

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	31	123591
Xmit Q:	0	1	12100

If both FTDs are on the same version, and the HA status is healthy, the upgrade is complete.