Contents

[1. Purpose and Scope 1](#_Toc116713147)

[2. Physical Topologies 1](#_Toc116713148)

[3. Procedures 3](#_Toc116713149)

[3.1.1. Implementation Preparation 3](#_Toc116713150)

[3.1.2. Physical Installation 3](#_Toc116713151)

[3.1.3. Initial Setup 4](#_Toc116713152)

[3.1.4. FXOS Configuration 5](#_Toc116713153)

[3.1.5. FCM Configuration 9](#_Toc116713154)

[3.1.6. Upgrade System Software 10](#_Toc116713155)

[3.1.7. ASA Migration 11](#_Toc116713156)

[3.1.7.1. ASA Logical Device 11](#_Toc116713157)

[3.1.7.2. Base Firewall Migration 13](#_Toc116713158)

[4. Rollback Plan 17](#_Toc116713159)

[5. Acronyms 18](#_Toc116713160)

Tables and Figures

[Table 1. Installation Procedure 3](#_Toc116713206)

[Table 2. Setup Wizard 4](#_Toc116713207)

[Table 3. Firepower CLI 6](#_Toc116713208)

[Table 4. Firepower Chassis Manager 9](#_Toc116713209)

[Table 5. Software Upgrade using Chassis Manager 10](#_Toc116713210)

[Table 6. Logical ASA 11](#_Toc116713211)

[Table 7. Migration Procedure 13](#_Toc116713212)

[Table 12. Rollback Procedure 17](#_Toc116713213)

[Figure 1: Topology #1 Cisco ASA 5585-X Current Integration 2](#_Toc116713198)

[Figure 2: Topology #2 Cisco Firepower 9300 Tested Integration 2](#_Toc116713199)

[Figure 3: Rack Rails 4](#_Toc116713200)

[Figure 4: Putty 5](#_Toc116713201)

[Figure 5: NTP Validation 8](#_Toc116713202)

[Figure 6: Interface Configuration 10](#_Toc116713203)

[Figure 8: Management Interface 13](#_Toc116713204)

[Figure 9: Adding Device from Network 17](#_Toc116713205)

# Purpose and Scope

The purpose of this guide is to provide instruction on how to successfully migrate the current Firewalls from two(2) physical Cisco Adaptive Security Appliances (ASA) located in one 5585-X chassis to one (1) Firepower 9300 chassis with (2) SM security module installed in each chassis**.**

The FP9300 uses Firepower eXtensible Operating System (FXOS) console and command line configuration. Alternatively, Firepower Chassis Manager (FCM) provides a GUI-based management of the FP9300. This document assumes license and procurement of required software (ASA version 9.8(4)29 and FXOS version 2.3(1.58). This software will need to be loaded on the Firepower chassis via the FCM prior to configuration.

Once basic configuration and licensing is configured on the FirePower Chassis via FXOS/FCM the administrator can begin configuration of the Security Modules. The FP9300 has the ability to run either ASA or FirePower Threat Defense (FTD) software as a logical device on each of its Security Modules (SM). Due to tenant requirements the Security Modules (SM) will be running ASA code configured in multiple context mode for this migration. The ASA software can be managed by either:

* ASA Security Device Manager (ASDM)
* Cisco Security Manager (CSM)
* Command Line Interface (CLI)

This guide will cover how to configure the ASA with both the CLI and CSM concurrently. Two ASA logical devices with be installed on each FP9300 Security Module. Only one (1) ASA instance per Security Module is supported.

# Physical Topologies

****

Figure : Topology #1 Cisco ASA 5585-X Current Integration



Figure : Topology #2 Cisco Firepower 9300 Tested Integration

# Procedures

**Note:** In this guide, ignore the use of angled brackets <xyz> and only type the information provided within, i.e. xyz. In addition, **boldface** indicates syntax that are typed exactly as shown. *Italic* indicates menu options or graphical buttons.

### Implementation Preparation

In preparation for replacement of the current base firewall with Cisco Firepower 9300, your review of the following Cisco articles is recommended:

* Cisco Firepower 9300 Getting Started Guide
	+ <https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp9300/firepower-9300-gsg.html?dtid=osscdc000283>
* Chassis Authentication/Authorization for remote management with ISE using TACACS+
	+ <https://www.cisco.com/c/en/us/support/docs/security/firepower-9000-series/212688-firepower-extensible-operating-system-f.html>
* User Guide for Cisco Security Manager
	+ <https://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/419/user/guide/CSMUserGuide.html>

### Physical Installation

This procedure entails basic hardware installation of the Firepower 9300 appliance. Ensure using all necessary precautions to prevent electrostatic discharge (ESD) from occurring. The following equipment (included with packaging) was needed to rack and install the Firepower 9300 but is not limited to:

* 2 mounting rails adjustable to 24 to 36 inches
* 1 ground lug and screw
* 2 C19 power cords
* 4 Retention/Cage nuts and screws (optional)
* Serial (console) cable

The Firepower 9300 has a 3 RU form factor and is rack mounted front facing cold aisle and rear facing hot aisle to ensure proper air flow.

Table . Installation Procedure

| **Step** | **Procedure** |
| --- | --- |
|  | Have proper grounding in place to avoid electrical damage from power surge. |
|  | Wear grounding wrist strap or utilize some other method to prevent ESD. |
|  | Install both mounting rails referencing the left/right markings for proper location. |
|  | Secure rails to rack using 4 screws including in packaging. (Figure 3) |
|  | Set the rear of the Firepower 9300 appliance carefully onto the mounting rails. |
|  | Level and push the appliance onto the rails until the ears are flush with the rack posts. |
|  | Ground the appliance. |
|  | Connect power cables to the rear of the chassis and to the power distribution unit (PDU). |
|  | Toggle the power switch on the rear of the chassis to the on position.  |
|  | Observe the SYS LED on the front of the Firepower 9300 chassis. |
|  | Once the SYS LED turns solid green the Firepower 9300 appliance has successfully booted. |



Figure : Rack Rails

### Initial Setup

Ensure the Firepower 9300 appliance has factory configuration loaded. If it does not, run the erase configuration command detailed below. Then proceed the initial configuration.

Table . Setup Wizard

| **Application** | **Procedure** |
| --- | --- |
| CONSOLE | Connect a management laptop to the console port on the front on the chassis using a serial cable. |
| CONSOLE | Open terminal emulator on the management laptop. (Figure 4) |
| CONSOLE | From the laptop’s terminal window, login with username and password. <admin><cisco123> |
| CONSOLE | To erase any previous configuration and run the setup wizard type **connect local-mgmt**command. |
| CONSOLE | Then type **erase configuration**and then type **yes.** |
| CONSOLE | Login with the default username and password <admin><cisco123> |
| CONSOLE | Then step through basic configuration* Admin password
* Hostname
* IP Address
* SSH Subnet
* HTTP Subnet
* DNS Server
* Domain name
 |
| CONSOLE | Once completed, type **yes** then press enter. |
| CONSOLE | Disconnect console cable. |



Figure : Putty

### FXOS Configuration

The FXOS CLI supervisor level is annotated by [hostname] #, e.g. Firepower# and the application console is identified by [module] >, e.g. Firepowermodule1>.

Table . Firepower CLI

| **Application** | **Procedure** |
| --- | --- |
| CLI | Open an SSH connection to the A side Cisco Firepower 9300 management IP address. |
| CLI | Login with the username and password created during setup. |
| CLI | From the supervisor level, run the following commands:1) Firepower # **scope system**2) Firepower/system # **scope services**3) Firepower/system/services # **create ntp-server** {ip-address}4) Firepower/system/services/ntp-server\* # **set ntp-sha1-key-id** {ID}5) Firepower/system/services/ntp-server\* # **set ntp-sha1-key-string**Enter NTP SHA-1 key string6) Firepower/system/services/ntp-server\* # **commit-buffer**7) Firepower/system/services/ntp-server # **exit** |
| CLI | Repeat steps 3-5 for each NTP server. (Figure 5) |
| CLI | Verify with the **show ntp-server** command. |
|  | Next configure TACACS with the following:1) Firepower # **scope security**2) Firepower /security # **scope default-auth**3) Firepower /security/default-auth # **set realm tacacs**4) Firepower /security/default-auth # **top**5) Firepower # **scope security**6) Firepower /security # **scope tacacs**7) Firepower /security/tacacs # **enter server 10.99.99.99**8) Type the tacacs key then hit enter9) Firepower/system/services/ntp-server\* # **commit-buffer** |
| CLI | Next configure SNMPv3 with the following:1) Firepower/system/services# **scope monitoring**2) Firepower/monitoring# **enable snmp**3) Firepower/ monitoring # **create snmp-user** {v3username}Password: *Then enter password*\*\*\*passwords cannot contain (?)question mark ($)dollar sign or (=)equal sign \*\*\*4) Firepower/ monitoring/snmp-user\* # **set aes-128 yes**5) Firepower/ monitoring/snmp-user\* # **set priv-password**Enter a password: *Then enter password*Confirm the password: *Re-enter password*\*\*\*passwords cannot contain (?)question mark ($)dollar sign or (=)equal sign \*\*\*6) Firepower/ monitoring/snmp-user\* # **commit-buffer**7) Firepower/ monitoring/snmp-user # **exit**8) Firepower/ monitoring # **create snmp-trap** {ip-address}9) Firepower/ monitoring/snmp-trap\* # **set version v3**10) Firepower/ monitoring/snmp-trap\* # **set version v3** 11) Firepower/ monitoring/snmp-trap\* # **set notification {traps | informs**}12) Firepower/ monitoring/snmp-trap\* # **set v3privilege priv**13) Firepower/ monitoring/snmp-trap\* # **set community**Community: *Enter community string*14) Firepower/ monitoring/ snmp-trap\* # **commit-buffer** |

FP-9300-B-A /system/services # show

Name: ssh

 Admin State: Enabled

 Port: 22

Kex Algo: Diffie Hellman Group1 Sha1,Diffie Hellman Group14 Sha1

Mac Algo: Hmac Sha1,Hmac Sha1 96,Hmac Sha2 512,Hmac Sha2 256

Encrypt Algo: Aes256 Cbc,Aes128 Cbc,Aes192 Cbc,Aes256 Ctr,Aes128 Ctr,Aes192 Ctr

Auth Algo: Rsa

 Host Key Size: 1024

Volume: None Time: None

Name: telnet

 Admin State: Disabled

 Port: 23

Name: https

 Admin State: Enabled

 Port: 443

 Operational port: 443

 Key Ring: default

 Cipher suite mode: Medium Strength

 Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIU M:+EXP:+eNULL

 Https authentication type: Cred Auth

 Crl mode: Relaxed

NTP Servers:

 Name: 10.99.99.99

 Name: 10.10.99.99

 Name: 10.20.99.99

Figure : NTP Validation

### FCM Configuration

Ensure the Firepower 9300 has a connection from the management interface located on the front of the chassis to the management switch for access to the FCM. The FP9300 has one management interface for FCM or CLI and one interface configured as a shared management interface for 2 ASA logical devices. Each logical device will have its own management IP.

**Note:** Disconnecting Eth1/8 will disconnect management to both ASA logical devices but not the Firepower Chassis Manager / (FXOS). All licensing and upgrades of both the chassis and the ASA security modules occur via the FCM/FXOS.

Table . Firepower Chassis Manager

| **Application** | **Procedure** |
| --- | --- |
| GUI | Open a web browser session to the A side FP9300 management IP address, e.g.:**https://192.168.xxx.xxx**where *192.168.xxx.xxx* is the A side Firepower Chassis Manager IP address |
| GUI | Login with the username and password created during setup. |
| GUI | Click “Interfaces>All Interfaces” |
| GUI | Set interfaces 1/1-1/8 as data:1) Click the edit icon next to Ethernet1/1.2) Check the *Enable* check-box. (see Figure 6)3) Click the *OK* button.4) Repeat steps 1-3 for each data interface. |
| GUI | Set interfaces 3/1 as a shared management interface:1) Click the edit icon next to Ethernet3/1.2) Check the *Enable* check-box.3) Select “mgmt” from the Type: drop-down.4) Select “1gbps” from the Admin Speed: drop-down.5) Select “Full Duplex” from the Admin Duplex: drop-down.6) Click the *OK* button. |
| GUI | Set Syslog servers:1) Click “Platform Settings > Syslog > Remote Destinations.”2) Check the *Enable* check-box for *Server 1.*3) Select *information*. from the *Level*: drop-down.4) Type syslog server IP in the *Hostname/IP Address* field5) Select *local6*. from the *Facility*: drop-down.6) Repeat steps 3-5 for Server 2 and 3.7) Click the *Save* button. |



Figure : Interface Configuration

### Upgrade System Software

This section walks through the steps and procedure to upload/install ASA software as well as FXOS images. Ensure operability by checking Cisco’s ASA Compatibility Matrix. The ASA software that runs on the ASA 5585 is not the same as the ASA software that runs on the FP9300.

**Note:** When downloading ASA software from the cisco website, be sure to look for the software under the Firepower 9300 not the ASA 5500. The version numbers will be the same, but the file extension will be different.

Table . Software Upgrade using Chassis Manager

| **Application** | **Procedure** |
| --- | --- |
| GUI | Open a web browser session to the A side FP9300 management IP address, e.g.:**https://192.168.xxx.xxx**where *192.168.xxx.xxx* is the A side Firepower Chassis Manager IP address. |
| GUI | Login with the username and password. |
| GUI | Navigate to “System>Updates” menu. |
| GUI | 1) Click the *Upload Image*button.2) Click the *Choose File* button, then select cisco-asa.9.8.4.10.SPA.csp3) Click the *Upload*button.4) When the image finishes uploading, a dialog box will read “Successfully Uploaded”5) Click *OK*button. |
| GUI | Repeat steps 1-5 to upload **fxos-k9.2.3.1.58.SPA** |
| GUI | Click the () icon next the version 2.3(1.58) platform-bundle to upgrade the FXOS software on the FP9300 chassis. |
| GUI | Click *YES*to proceed with the install.  |
| GUI | The system will reboot automatically and return to the login screen. (may take 10-20 minutes for completion) |
| GUI | Verify new version by navigating to “Overview” menu. (see Figure 7) |

### ASA Migration

There are number of caveats to migrate ASA 5585 configuration over to the FP9300. When taking a backup copies of the ASA 5585 running configuration, keep in mind that each context will be edited and pasted individually into the FP9300. However, copying and pasting the configuration without making the following edits will result in syntax errors and possible lock out of the ASA.

### ASA Logical Device

The Firepower’s ASA logical device does not have any management interfaces; therefore, the management IP addresses were configured on Ethernet1/8. Two separate management IP addresses were configured on each FP9300 chassis even though there is only one Eth1/8 interface.

**Note:** Disconnecting Eth1/8 will disconnect management to both ASA logical devices but not the Firepower Chassis Manager / (FXOS).

Table . Logical ASA

| **Application** | **Procedure** |
| --- | --- |
| GUI | Open a web browser session to the A side FP9300 management IP address, e.g.:**https://1.1.1.1**where *1.1.1.1* is the A side Firepower Chassis Manager IP address. |
| GUI | 1. Login with the username and password.
2. Navigate to “Logical Devices” menu.
3. Click *Add Device* button.
4. Enter/Select the following:
* Device Name
* Cisco: Adaptive Security Appliance
* 9.8.4.10
* Standalone
1. Click the *OK* button.
2. Click to highlight interfaces Ethernet1/1, Ethernet1/2 and Ethernet1/3.
3. Click the *ASA- 9.8.4.10 (Click to configure)* button.
4. Click *SM 1- Ok*. (see Figure 8)
5. Select *Ethernet1/8* from the *Management Interface* drop-down
6. Enter the following information:
* Management IP
* Network Mask
* Network Gateway
1. Click the *Settings* Tab
2. Enter password for admin and enable
3. Click the *OK* button.
4. Click the *Save* button.
 |
| GUI | Repeat steps 3-9 selecting interfaces Ethernet1/5, Ethernet1/6 and Ethernet1/7; SM 2-Ok; Ethernet1/8 from the Management Interface drop-down.(Figure 8) |
| GUI | Repeat steps 1-9 for each firewall. |



Figure : Management Interface

### Base Firewall Migration

**Note**: In this guide, ignore the use of angled brackets <xyz> and only type the information provided within, i.e. xyz. In addition, **boldface** indicates syntax that are typed exactly as shown. *Italic* indicates menu options or graphical buttons.

Table . Migration Procedure

| **Application** | **Procedure** |
| --- | --- |
| CLI/NotepadNote: This method is depreciated. Refer to Wiki) | 1. Open an SSH connection to the management IP address of the A side Cisco 5585.
2. Back up all context configurations of the current base firewall.
3. Break each copied configuration (system, admin, and firewall contexts) into separate text files for editing.
4. Edit the system context file first.
5. Delete NTP commands from the configuration file.
6. ntp authentication-key
7. ntp authenticate
8. ntp trusted-key
9. ntp server
10. sed -i '/^ntp/d' system-context.cfg
11. Remove all boot system command(s) from the configuration file
12. boot system disk0:/asa984-10-smp-k8.bin
13. sed -i '/^boot/d' system-context.cfg
14. Rename interface TenGigabitEthernet0/ to interface Ethernet1/
15. sed -i 's/TenGigabitEthernet0/Ethernet1/g' system-context.cfg
16. Delete interface Management commands and unused interface commands
17. Add no shut command to interfaces 0/1-8
18. I have to add changing interface Ethernet1/6 to interface Ethernet1/1; interface Ethernet1/7 to interface Ethernet1/2; and interface Ethernet1/8 to interface Ethernet1/3 for fw-x1. interface Ethernet1/6 to interface Ethernet1/5, interface Ethernet1/7 to interface Ethernet1/5, and interface Ethernet1/8 to interface Ethernet1/7 for fw-x2.
19. There is a script for each firewall.
20. For fw-x1 use script: int-conversion-fw-x1.sh
21. For fw-x2 use script: int-conversion-fw-x2.sh
22. Script int-conversion-fw-x1.sh

#!/bin/shsed -i -e '/^ntp/d' -e '/^boot/d' -e 's/TenGigabitEthernet0/Ethernet1/g' -e 's/Ethernet1\/6/Ethernet1\/1/g' -e 's/Ethernet1\/7/Ethernet1\/2/g' -e 's/Ethernet1\/8/Ethernet1\/3/g' system-context.cfg1. Script int-conversion-fw-x2.sh#!/bin/sh
2. sed -i -e '/^ntp/d' -e '/^boot/d' -e 's/TenGigabitEthernet0/Ethernet1/g' -e 's/Ethernet1\/6/Ethernet1\/5/g' -e 's/Ethernet1\/7/Ethernet1\/6/g' -e 's/Ethernet1\/8/Ethernet1\/7/g' system-context.cfg
3. Note: After creating the file, have to do **chmod u+x *<filename>*** in order to make the file executable.
4. Verify:
5. cat system-context.cfg | grep " TenGigabitEthernet"
6. cat system-context.cfg | grep "Ethernet1/6"
7. cat system-context.cfg | grep "Ethernet1/7"
8. cat system-context.cfg | grep "Ethernet1/8"
9. cat system-context.cfg | grep "Ethernet1/1"
10. cat system-context.cfg | grep "Ethernet1/2"
11. cat system-context.cfg | grep "Ethernet1/3"
12. Save notepad
13. Edit the admin context file.
14. Rename interface Management0/0 to interface Ethernet3/1
15. Rename mgmt to management
16. Replace \*\*\*\*\* in the “key \*\*\*\*\*” command with the actual password.
17. Remove the “engineID <engineID>” from the command:
18. snmp-server user jitc jitc v3 engineID <engineID> encrypted auth sha <encrypted output omitted> priv aes 128 <encrypted output omitted>
19. Remove “aaa authorization…” commands; otherwise copy and paste will fail.
20. Save notepad.
21. Edit the remaining firewall context files.
22. Rename interface TenGigabitEthernet0/ to interface Ethernet1/
23. Replace \*\*\*\*\* in the “key \*\*\*\*\*” command with the actual password
24. Save notepad.
25. Open an SSH connection to the A side FP9300 management IP address.
26. Run the following commands from FXOS:
27. Firepower # **connect module 1 console**
28. Firepower-module1 # **connect asa**
29. asa> **enable**
30. asa # **configure terminal**
31. asa (config) # **mode multiple**
32. Proceed with change mode? [confirm] press *Enter*
33. Convert the system configuration? [confirm] press *Enter*
34. Wait for the firewall to reboot.
35. Login once the firewall has completed its boot sequence.
36. Run the following commands:
37. asa> **enable**
38. asa # **configure terminal**
39. From the asa (config) # prompt paste the contents of the edited base firewall A1 system context configuration file.
40. Run the following commands:
41. asa (config) # **write memory**
42. asa (config) # **changeto context admin**
43. From the asa/admin (config) # prompt paste the contents of edited base firewall A1 admin context configuration file.
44. Repeat steps 11-12 for all remaining context configuration files.
45. Ensure SSH to admin context with TACACS is functioning before saving configuration.
46. From the hostname/admin (config) # prompt paste authorization commands e.g.

**aaa authorization command global-tacacs LOCAL**1. Run the following commands:
2. hostname/admin (config) # **changeto system**
3. hostname (config) # **write memory all**
4. hostname (config) # **end**
 |
| CSM | Add base firewall A1 to Cisco Security Manager (CSM) using admin context management IP. (Figure 9) |
| CSM | Use the Copy Policies Wizard in CSM to copy policies from each individual context on the existing A1 firewall to the new Firepower A security module 1 firewall contexts. |
| CLI | Hit Ctrl+A+D to exit the logical device A1 . |
| CLI | Then type **~** press enter. Type **quit** then press enter to return to FXOS. |
| CLI | 1. Run the following commands from FXOS:
2. Firepower # **connect module 2 console**
3. Firepower-module1 # **connect asa**
4. asa> **enable**
5. asa # **configure terminal**
6. asa (config) # **mode multiple**
7. Proceed with change mode? [confirm] press *Enter*
8. Convert the system configuration? [confirm] press *Enter*
9. Wait for the firewall to reboot.
10. Login once the firewall has completed its boot sequence.
11. Run the following commands:
12. asa> **enable**
13. asa # **configure terminal**
14. From the asa (config) # prompt paste the contents of the edited base firewall A2 system context configuration file. (see [Table 7](#_Base_Firewall_Migration))
15. Run the following commands:
16. asa (config) # **write memory**
17. asa (config) # **changeto context admin**
18. From the asa/admin (config) # prompt paste the contents of edited base firewall A2 admin context configuration file.
19. Repeat steps for all remaining context configuration files.
20. Ensure SSH to admin context with TACACS is functioning before saving configuration.
21. From the hostname/admin (config) # prompt paste authorization commands e.g.

**aaa authorization command global-tacacs LOCAL**1. Run the following commands:
2. hostname/admin (config) # **changeto system**
3. hostname (config) # **write memory all**
4. hostname (config) # **end**
5. Save all configurations from the system context, command “write memory all”.
 |
| CSM | Add base firewall A2 to Cisco Security Manager (CSM) using admin context management IP. (Figure 9) |
| CSM | Use the Copy Policies Wizard in CSM to copy policies from each individual context on the existing A2 firewall to the new Firepower A security module 2 firewall contexts. |
|  | Repeat the procedure for base firewall B1 and B2 on Firepower B security module 1 and 2 respectively. |



Figure : Adding Device from Network

# Rollback Plan

Apply the following process if the upgrade fails or has issues.

Table . Rollback Procedure

| **Step** | **Task** |
| --- | --- |
|  | Swap physical cabling back to ASA 5585 |
|  | Delete system, admin and other contexts from CSM |
|  |  |
|  |  |
|  |  |

# Acronyms

**Define any acronyms used in the document.**

| **Acronym** | **Definition** |
| --- | --- |
|  |  |
| ASA | Adaptive Security Appliances |
| ASDM | ASA Security Device Manager |
| CLI | Command Line Interface |
| CSM | Cisco Security Manager |
| ESD | Electrostatic Discharge |
| FCM | Firepower Chassis Manager |
| FP | Firepower |
| FTD | Firepower Threat Defense |
| FXOS | Firepower eXtensible Operating System |
| GUI | Graphical User Interface |
| LACP | Link Aggregation Control Protocol |
| PDU | Power Distribution Unit |
| RU | Rack Unit |
| SSH | Secure Shell |

This is the last page of this document.