Cisco FXOS Compatibility

First Published: July 16, 2015
Last Revised: December 11, 2017

This document lists software and hardware compatibility information for the Firepower eXtensible Operating System (FXOS), Cisco Firepower 9300 and Cisco Firepower 4100 series security appliances, and supported logical devices.

Firepower Software and Hardware Compatibility

The following table lists the supported FXOS versions and Firepower models.

Note: Firepower 2100 series appliances utilize FXOS only as an underlying operating system that is included in the ASA and Firepower Threat Defense unified image bundles. Refer to the ASA Compatibility and Firepower Threat Defense Compatibility guides for information about 2100 series compatibility.

Table 1 FXOS Compatibility

FXOS Release	Firepower 9300	Firepower 4110	Firepower 4120	Firepower 4140	Firepower 4150
1.1.1	**YES**	**NO**	**NO**	**NO**	**NO**
1.1.2	**YES**	**NO**	**NO**	**NO**	**NO**
1.1.3	**YES**	**NO**	**NO**	**NO**	**NO**
1.1.4	**YES**	**YES**	**YES**	**YES**	**NO**
2.0.1	**YES**	**YES**	**YES**	**YES**	**YES** Note: Requires ASA 9.6(2) or FTD 6.1
2.1.1	**YES**	**YES**	**YES**	**YES**	**YES**
2.2.1	**YES**	**YES**	**YES**	**YES**	**YES**
2.2.2	**YES**	**YES**	**YES**	**YES**	**YES**
2.3.1	**YES**	**YES**	**YES**	**YES**	**YES**

Logical Device Compatibility

The following table lists the supported logical devices for each FXOS version. See table 1 to determine which FXOS versions your security appliance is compatible with.

The application versions in bold are companion releases to the FXOS version. For a given FXOS version, use the application version listed in bold. Use older compatible versions of applications only in the context of upgrades.

The FXOS versions with (EOL) appended have reached their end of life (EOL), or end of support.

Table 2 Logical Device Compatibility

FXOS	ASA OS	Firepower Threat Defense
1.1(1.147) (EOL)	**9.4(1)**	Not supported
1.1(1.160) (EOL)	**9.4(1)**	
1.1(2.51)	9.4(1) **9.4(2)**	
1.1(2.178)	9.4(1) **9.4(2)**	
1.1(3.84)	9.4(2) **9.5(2)** **9.5(3)**	
1.1(3.86)	9.4(2) **9.5(2)** **9.5(3)**	
1.1(3.97)	9.4(2) **9.5(2)** **9.5(3)**	
1.1(4.95)	9.5(2) 9.5(3) **9.6(1)**	**6.0.1.x**
1.1(4.117)	9.5(2) 9.5(3) **9.6(1)**	**6.0.1.x**
1.1(4.140)	9.5(2) 9.5(3) **9.6(1)**	**6.0.1.x**
1.1(4.169)	9.5(2) 9.5(3) **9.6(1)**	**6.0.1.x**
1.1(4.175)	9.5(2) 9.5(3) **9.6(1)**	**6.0.1.x**

Table 2 Logical Device Compatibility

FXOS	ASA OS	Firepower Threat Defense
1.1(4.178)	9.5(2) 9.5(3) **9.6(1)**	**6.0.1.x**
1.1(4.179)	9.5(2) 9.5(3) **9.6(1)**	**6.0.1.x**
2.0(1.37)	9.6(1) **9.6(2)** **9.6(3)**	6.0.1.x **6.1**
2.0(1.68)	9.6(1) **9.6(2)** **9.6(3)**	6.0.1.x **6.1**
2.0(1.86)	9.6(1) **9.6(2)** **9.6(3)**	6.0.1.x **6.1**
2.0(1.129)	9.6(1) **9.6(2)** **9.6(3)**	6.0.1.x **6.1**
2.0(1.135)	9.6(1) **9.6(2)** **9.6(3)**	6.0.1.x **6.1**
2.0(1.141)	9.6(1) **9.6(2)** **9.6(3)**	6.0.1.x **6.1**
2.0(1.144)	9.6(1) **9.6(2)** **9.6(3)**	6.0.1.x **6.1**
2.0(1.148)	9.6(1) **9.6(2)** **9.6(3)**	6.0.1.x **6.1**
2.0(1.149)	9.6(1) **9.6(2)** **9.6(3)**	6.0.1.x **6.1**
2.0(1.153)	9.6(1) **9.6(2)** **9.6(3)**	6.0.1.x **6.1**

Table 2 Logical Device Compatibility

FXOS	ASA OS	Firepower Threat Defense
2.0(1.159)	9.6(1) **9.6(2)** **9.6(3)**	6.0.1.x **6.1**
2.1(1.64)	9.6(2) 9.6(3.x) 9.7(1)	6.1.x **6.2.0**
2.1(1.73)	9.6(2) 9.6(3.x) 9.7(1)	6.1.x **6.2.0**
2.1(1.77)	9.6(2) 9.6(3) **9.7(1)**	6.1.x **6.2.0**
2.1(1.83)	9.6(2) 9.6(3) **9.7(1)**	6.1.x **6.2.0**
2.1(1.85)	9.6(2) 9.6(3) **9.7(1)**	6.1.x **6.2.0**
2.1(1.86)	9.6(2) 9.6(3) **9.7(1)**	6.1.x **6.2.0**
2.1(1.97)	9.6(2) 9.6(3) **9.7(1)**	6.1.x **6.2.0**
2.2(1.63)	9.7(1) **9.8(1)** Note: 9.7(1.15) or later is required for flow offload	**6.2.0** Note: 6.2.0.3 or later is required for flow offload
2.2(1.66)	9.7(1) **9.8(1)** Note: 9.7(1.15) or later is required for flow offload	**6.2.0** Note: 6.2.0.3 or later is required for flow offload
2.2(1.70)	9.7(1) **9.8(1)** Note: 9.7(1.15) or later is required for flow offload	**6.2.0** Note: 6.2.0.3 or later is required for flow offload

Table 2 Logical Device Compatibility

FXOS	ASA OS	Firepower Threat Defense
2.2(2.17)	**9.8(1)**	**6.2.0**
	9.8(2)	**6.2.2**
2.2(2.19)	**9.8(1)**	**6.2.0**
	9.8(2)	**6.2.2**
2.2(2.24)	**9.8(1)**	**6.2.0**
	9.8(2)	**6.2.2**
2.2(2.26)	**9.8(1)**	**6.2.0**
	9.8(2)	**6.2.2**
2.3(1.56)	9.6(3)	6.1.0
	9.7(1)	6.2.0
	9.8(1)	**6.2.2**
	9.8(2)	
	9.9(1)	

Link Decorator Compatibility

The following table lists the supported link decorator for each Firepower security appliance and associated logical device.

Table 3 Link Decorator Compatibility

Radware vDP	FXOS	ASA	Firepower Threat Defense	Firepower Model				
				9300	4110	4120	4140	4150
1.1(2.32-3)	1.1(4)	9.6(1)	not supported	YES	NO	NO	NO	NO
8.10.01.16-5	2.0(1)	9.6(2)	not supported	YES	NO	YES	YES	YES
	2.1(1)	9.7(1)						YES
8.10.01.17-2	2.1(1)	9.7(1)	6.2.0	YES	ASA: NO	YES	YES	YES
	2.2(1)	9.8(1)	6.2.2		FTD: YES			
	2.2(2)	9.8(2)						
8.13.01	2.3(1)	9.9(1)	6.2.2	YES	ASA: NO	YES	YES	YES
					FTD: YES			

Network Module Support

The following table lists supported single-wide and double-wide network modules on the Firepower 9300 and Firepower 4100 security appliances.

Table 4 Network Module Support

Network Module	Firepower 9300	Firepower 4100 series
Firepower 8-port 10G Network Module single-wide	FPR9K-NM-8X10G	FPR4K-NM-8X10G
Firepower 4-port 40G Network Module single-wide	FPR9K-NM-4X40G	FPR4K-NM-4X40G
Firepower 2-port 100G Network Module double-wide	FPR9K-DNM-2X100G (FXOS 1.1.4 and later) Note: Requires firmware package 1.0.10 or later	Not supported
Firepower 6-port 1G SX Network Module single-wide, FTW	Not supported	FPR4K-NM-6X1SX-F (FXOS 2.0.1 and later)
Firepower 6-port 10G SR Network Module single-wide, FTW	FPR9K-NM-6X10SR-F (FXOS 2.0.1 and later)	FPR4K-NM-6X10SR-F (FXOS 2.0.1 and later)
Firepower 6-port 10G LR Network Module single-wide, FTW	FPR9K-NM-6X10LR-F (FXOS 2.0.1 and later)	FPR4K-NM-6X10LR-F (FXOS 2.0.1 and later)
Firepower 2-port 40G SR Network Module single-wide, FTW	FPR9K-NM-2X40G-F (FXOS 2.0.1 and later)	FPR4K-NM-2X40G-F (FXOS 2.0.1 and later)
Firepower 8-port 1G Network Module single-wide, FTW	Not supported	FPR-NM-8X1G-F (FXOS 2.1.1 and later; Firepower Threat Defense 6.2 and later)

Note: For instructions on how to verify your firmware package version and to upgrade the firmware if necessary, see "Firmware Upgrade" in the *Cisco FXOS CLI Configuration Guide* or *Cisco FXOS Firepower Chassis Manager Configuration Guide* (http://www.cisco.com/go/firepower9300-config).

Power Supply Support

The following table lists supported power supply modules on the Firepower 9300 and 4100 security appliances.

Table 5 Power Supply Support

Power Supply	FXOS	Firepower Model				
		9300	4110	4120	4140	4150
AC	1.1.1 and later	YES	YES	YES	YES	YES
DC	1.1.1 and later	YES	YES	YES	YES	YES
HVDC	2.1.1 and later	YES	NO	NO	NO	NO

Note: For more detailed information about the power supply modules in the 4100 series security appliances, see “Power Supply Modules” in the *Cisco Firepower 4100 Series Hardware Installation Guide* (http://www.cisco.com/c/en/us/td/docs/security/firepower/4100/hw/guide/b_install_guide_4100.html). For more detailed information about the power supply modules in your 9300 security appliance, see “Power Supply Modules” in the *Cisco Firepower 9300 Hardware Installation Guide* (http://www.cisco.com/c/en/us/td/docs/security/firepower/9300/hw/guide/b_install_guide_9300.html).

Security Module Compatibility

The following table lists supported security modules on the Firepower 9300 security appliances.

Table 6 Security Module Compatibility

Security Module	Product ID	FXOS Version
24 physical core security module with two SSDs (NEBS-compliant)	FPR9K-SM-24	1.1.1 and later
36 physical core security module with two SSDs	FPR9K-SM-36	1.1.1 and later
44 physical core security module with two SSDs	FPR9K-SM-44	2.0.1 and later Note: Requires ASA 9.6(2) or FTD 6.1

ASA and Firepower Threat Defense Clustering External Hardware Support

Clustering will work with both Cisco and non-Cisco switches from other major switching vendors with no known interoperability issues if they comply with the following requirements and recommendations. For switches that have been verified to work with clustering, see the verified switches table below.

Switch Requirements

- All third party switches must be compliant to the IEEE standard (802.3ad) Link Aggregation Control Protocol.
- EtherChannel bundling must be completed within 45 seconds when connected to Firepower devices and 33 seconds when connected to ASA devices.
- On the cluster control link, the switch must provide fully unimpeded unicast and broadcast connectivity at Layer 2 between all cluster members.
- On the cluster control link, the switch must not impose any limitations on IP addressing or the packet format above Layer 2 headers.
- On the cluster control link, the switch interfaces must support jumbo frames and be configurable for an MTU above 1600.

Switch Recommendations

- The switch should provide uniform traffic distribution over the EtherChannel's individual links.
- The switch should have an EtherChannel load-balancing algorithm that provides traffic symmetry.
- The EtherChannel load balance hash algorithm should be configurable using the 5-tuple, 4-tuple, or 2-tuple to calculate the hash.

Note: Cisco does not support the resolution of bugs found in non-verified switches.

Note: For the Firepower 9300 ASA cluster, intra-chassis clustering can operate with any switch because Firepower 9300-to-switch connections use standard interface types.

Note: Some switches, such as the Nexus series, do not support LACP rate fast when performing in-service software upgrades (ISSUs), so we do not recommend using ISSUs with clustering.

Verified Switches

The following table lists verified Cisco external hardware and software to interoperate with ASA clustering.

Table 7 Verified Switches

External Hardware	External Software
Cisco Firepower 2100, 4100, and 9300 Cisco ASA Series You can connect an ASA cluster directly to one or more Firepower or ASA chassis in standalone or failover mode, running either ASA or Firepower Threat Defense. For example, you might connect an Active/Standby ASA failover pair in multiple context mode to a Firepower Threat Defense cluster with inline sets (NGIPS mode).	Any
Cisco ASR 9000 with RSP 440	Cisco IOS XR 5.3(1)+
Cisco Nexus 3000 Cisco Nexus 6000 Cisco Nexus 7000 Cisco Nexus 9500 Cisco Nexus 9300 **Note:** For the Nexus 7000, you can use F1-series line cards for the cluster control link, but we do not recommend using them for data EtherChannels in Spanned EtherChannel mode due to asymmetric load-balancing, which can cause performance degradation for data throughput on the cluster. **Note:** For the Nexus 3000, we do not recommend using this switch for data EtherChannels in Spanned EtherChannel mode due to asymmetric load-balancing, which can cause performance degradation for data throughput on the cluster. You can use the switch for the cluster control link or for interfaces in Individual Interface mode.	Cisco NX-OS 7.0(2)N1(1)+ APIC 1.0(1)+
Catalyst 3750-X Catalyst 6500 with Supervisor 2T Catalyst 6800 with Supervisor 2T	Cisco IOS 15.1(2)SY5+
Catalyst 6500 with Supervisor 32, 720, and 720-10GE	Cisco IOS 12.2(33)SXI7, SXI8, and SXI9+
Catalyst 4500 with Supervisor 8-E	Cisco IOS XE 3.7(1E)+
Catalyst 3850 Catalyst 4500-X **Note:** We do not recommend using this switch for data EtherChannels in Spanned EtherChannel mode due to asymmetric load-balancing, which can cause performance degradation for data throughput on the cluster. You can use the switch for the cluster control link or for interfaces in Individual Interface mode.	Cisco IOS 3.7(3)+

ASA and Firepower Threat Defense Clustering External Hardware Support