Data Sheet

Cisco Firepower NGFW

Contents

The Cisco Firepower® NGFW (next-generation firewall) is the industry's first fully integrated, threat-focused next-gen firewall with unified management. It uniquely provides advanced threat protection before, during, and after attacks.

Stop more threats	Contain known and unknown malware with leading Cisco® Advanced Malware Protection (AMP) and sandboxing.
Gain more insight	Gain superior visibility into your environment with Cisco Firepower next-gen IPS. Automated risk rankings and impact flags identify priorities for your team.
Detect earlier, act faster	The Cisco Annual Security Report identifies a 100-day median time from infection to detection, across enterprises. Reduce this time to less than a day.
Reduce complexity	Get unified management and automated threat correlation across tightly integrated security functions, including application firewalling, NGIPS, and AMP.
Get more from your network	Enhance security, and take advantage of your existing investments, with optional integration of other Cisco and third-party networking and security solutions.

Model Overview

Cisco Firepower 2100 Series:
The industry's first midrange NGFWs delivering sustainable performance when threat inspection is enabled

Cisco Firepower 4100 Series:
The industry's first 1RU NGFWs with 40-Gbps interfaces

Cisco Firepower 9300:
Ultra-high-performance NGFW, expandable as your needs grow

Cisco ASA 5500-X Series:
Models for branch offices, industrial applications, and the Internet edge

Firepower NGFWv:
The NGFW for virtual and cloud environments

Platform Image Support

The Cisco Firepower NGFW includes Application Visibility and Control (AVC), optional Next-Gen IPS (NGIPS), Cisco® Advanced Malware Protection (AMP) for Networks, and URL Filtering. The Cisco Firepower 2100 Series, 4100 Series, and 9300 appliances use the Cisco Firepower Threat Defense software image. Alternatively, Cisco Firepower 2100 Series, 4100 Series, and 9300 appliances can support the Cisco Adaptive Security Appliance (ASA) software image.

Management Options

Cisco Firepower NGFWs may be managed in a variety of ways depending on the way you work, your environment, and your needs.

The Cisco Firepower Management Center provides centralized management of the Cisco Firepower NGFW, the Cisco Firepower NGIPS, and Cisco AMP for Networks. It also provides threat correlation for network sensors and Advanced Malware Protection (AMP) for Endpoints.

The Cisco Firepower Device Manager is available for local management of 2100 Series and select 5500-X Series devices running the Cisco Firepower Threat Defense software image.

The Cisco Adaptive Security Device Manager is available for local management of the Cisco Firepower 2100 Series, 4100 Series, Cisco Firepower 9300 Series, and Cisco ASA 5500-X Series devices running the ASA software image.

Cisco Defense Orchestrator cloud-based management is also available for consistent policy management across Cisco security devices running the ASA software image, enabling greater management efficiency for the distributed enterprise.

Firepower DDoS Mitigation

Also available on the Cisco Firepower 4100 Series and 9300 appliances is tightly integrated, comprehensive, behavioral DDoS mitigation for both network and application infrastructure protection. This DDoS mitigation is Radware’s Virtual DefensePro (vDP). It is available from and supported directly by Cisco.

Cisco Firepower 2100 Series Appliances

The Cisco Firepower 2100 Series is a family of four threat-focused NGFW security platforms that deliver business resiliency through superior threat defense. It offers exceptional sustained performance when advanced threat functions are enabled. These platforms uniquely incorporate an innovative dual multicore CPU architecture that optimizes firewall, cryptographic, and threat inspection functions simultaneously. The series' firewall throughput range addresses use cases from the Internet edge to the data center. Network Equipment Building Standards (NEBS)- compliance is supported by the Cisco Firepower 2100 Series platform.

Cisco Firepower 4100 Series Appliances

The Cisco Firepower 4100 Series is a family of four threat-focused NGFW security platforms. Their throughput range addresses data center and internet edge use cases. They deliver superior threat defense, at faster speeds, with a smaller footprint. Cisco Firepower 4100 Series supports flow-offloading, programmatic orchestration, and the management of security services with RESTful APIs. Network Equipment Building Standards (NEBS)-compliance is supported by the Cisco Firepower 4120 platform.

Cisco Firepower 9300 Security Appliance

The Cisco Firepower 9300 is a scalable (beyond 1 Tbps when clustered), carrier-grade, modular platform designed for service providers, high-performance computing centers, large data centers, campuses, high-frequency trading environments, and other environments that require low (less than 5-microsecond offload) latency and exceptional throughput. Cisco Firepower 9300 supports flow-offloading, programmatic orchestration, and the management of security services with RESTful APIs. It is also available in Network Equipment Building Standards (NEBS)-compliant configurations.

Cisco ASA 5500-FTD-X Series Appliances

The Cisco ASA 5500-FTD-X Series is a family of eight threat-focused NGFW security platforms. Their throughput range addresses use cases from the small or branch office to the Internet edge. They deliver superior threat defense in a cost-effective footprint.

Cisco Firepower NGFW Virtual (NGFWv) Appliances

Cisco Firepower NGFWv is available on VMware, KVM, and the Amazon Web Services (AWS) and Microsoft Azure environments for virtual, public, private, and hybrid cloud environments. Organizations employing SDN can rapidly provision and orchestrate flexible network protection with Firepower NGFWv. As well, organizations using NFV can further lower costs utilizing Firepower NGFWv.

Performance Testing Methodologies

Cisco uses a variety of testing methodologies in a lab environment to ensure the performance specifications we report are as close to real world as possible. Firewall performance is affected by many factors including network environment, packet sizes, packet type, TLS encryption, and more.

Two modes of firewall testing exist: static or real world. Static testing leverages performance and security testing tools in a simulated environment. Real-world testing uses samples of live traffic on a production or side-car network. While static testing does not completely mimic performance in a real-world networking environment, we review and modify the static methodology to ensure the results are as close to real-world as possible.

The following are test methodologies used for measurements listed in Table 1. Small packet size tests will reflect additional inspection overhead thus results in reduced firewall throughput. The reduction is not linear, so extrapolation from a single test is not possible for the almost unlimited variety of network environments. Testing security efficacy or security service performance under loaded conditions adds even more complexity. For these reasons we rely on the 1024B HTTP Test.

1024B HTTP Test (256KB Object)

This number is to compare with other vendors at a 256KB object size. It uses a larger and commonly tested packet size for every simulated session. With the protocol overhead, the average frame size is around 1024 bytes. This represents typical production conditions for most firewall deployments.

1500B UDP

This test uses a transactional UDP profile with 1500-byte frames. Due to the stateless nature of UDP, it creates very little impact on a stateful NGFW. Many vendors use this profile to measure maximum firewall performance, but it is only practical as a comparison point and does not represent world conditions.

TLS

This test follows the 1024B HTTP test conditions with 50% of sessions encapsulated into TLS (HTTPS) and fully decrypted for inspection in hardware. Client TLS sessions use AES256-SHA cipher with 2048-bit RSA keys, and the server is assumed to reside behind the NGFW for Known Key decryption. These test results can be linearly extrapolated for other percentages of TLS traffic; for example, the NGFW throughput will be approximately twice as high with 25% of HTTPS connections in the overall traffic mix.

Performance Specifications and Feature Highlights

Table 1 summarizes the capabilities of the Cisco Firepower NGFWv, Firepower 2100 Series, and 4100 Series and 9300 appliances as well as the Cisco ASA 5500-FTD-X appliances when running the Cisco Firepower Threat Defense image.

Table 1. Performance Specifications and Feature Highlights for Physical and Virtual Appliances with the Cisco Firepower Threat Defense Image

Features	Cisco Firepower Model														Cisco ASA 5500-FTD-X Model						
	NGFWv	2110	2120	2130	2140	4110	4120	4140	4150	9300 with 1 SM-24 Module	9300 with 1 SM-36 Module	9300 with 1 SM-44 Module	9300 with 3 SM-44 Modules	5506-FTD-X	5506W-FTD-X	5506H-FTD-X	5508-FTD-X	5516-FTD-X	5525-FTD-X	5545-FTD-X	5555-FTD-X
Throughput: FW + AVC 1024B	1.2 Gbps	2.0 Gbps	3 Gbps	4.75 Gbps	8.5 Gbps	12 Gbps	20 Gbps	25 Gbps	30 Gbps	25 Gbps	35 Gbps	50 Gbps	118 Gbps	250 Mbps	250 Mbps	250 Mbps	450 Mbps	850 Mbps	1100 Mbps	1500 Mbps	1750 Mbps
Throughput: FW + AVC + IPS (1024B)	1.1 Gbps	2.0 Gbps	3 Gbps	4.75 Gbps	8.5 Gbps	10 Gbps	15 Gbps	20 Gbps	24 Gbps	20 Gbps	30 Gbps	45 Gbps	117 Gbps	125 Mbps	125 Mbps	125 Mbps	250 Mbps	450 Mbps	650 Mbps	1000 Mbps	1250 Mbps
Maximum concurrent sessions, with AVC	100,000	1 million	1.2 million	2 million	3.0 million	9 million	15 million	25 million	30 million	30 million	30 million	30 million	60 million	20,000	20,000	20,000	100,000	250,000	500,000	750,000	1,000,000

Features	Cisco Firepower Model														Cisco ASA 5500-FTD-X Model						
	NGFWv	2110	2120	2130	2140	4110	4120	4140	4150	9300 with 1 SM-24 Module	9300 with 1 SM-36 Module	9300 with 1 SM-44 Module	9300 with 3 SM-44 Modules	5506-FTD-X	5506W-FTD-X	5506H-FTD-X	5508-FTD-X	5516-FTD-X	5525-FTD-X	5545-FTD-X	5555-FTD-X
Maximum new connections per second, with AVC	10,000	12,000	16,000	24,000	40,000	68,000	120,000	160,000	200,000	120,000	160,000	300,000	900,000	3,000	3,000	3,000	7,000	8,000	10,000	15,000	20,000
TLS (Hardware Decryption)	-	350 Mbps	450 Mbps	700 Mbps	1.2 Gbps	4.5 Gbps	7.1 Gbps	7.3 Gbps	7.5 Gbps	7.5 Gbps	8.5 Gbps	10 Gbps	25.5 Gbps	-	-	-	-	-	-	-	-
IPSec VPN Throughput (1024B TCP w/Fastpath)	-	750 Mbps	1 Gbps	1.5 Gbps	3 Gbps	6 Gbps	10 Gbps	13 Gbps	14 Gbps	13.5 Gbps	16 Gbps	17 Gbps	51 Gbps	100 Mbps	100 Mbps	100 Mbps	175 Mbps	250 Mbps	300 Mbps	400 Mbps	700 Mbps
Maximum VPN Peers	-	1500	3500	7500	10000	10000	15000	20000	20000	20000	20000	20000	60000	50	50	50	100	300	300	400	700
Cisco Firepower Device Manager (local management)	Yes (VMware only)	Yes	Yes	Yes	Yes	-	-	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Centralized management	Centralized configuration, logging, monitoring, and reporting are performed by the Management Center or alternatively in the cloud with Cisco Defense Orchestrator																				
Application Visibility and Control (AVC)	Standard, supporting more than 4000 applications, as well as geolocations, users, and websites																				
AVC: OpenAppID support for custom, open source, application detectors	Standard																				
Cisco Security Intelligence	Standard, with IP, URL, and DNS threat intelligence																				
Cisco Firepower NGIPS	Available; can passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence																				
Cisco AMP for Networks	Available; enables detection, blocking, tracking, analysis, and containment of targeted and persistent malware, addressing the attack continuum both during and after attacks. Integrated threat correlation with Cisco AMP for Endpoints is also optionally available																				
Cisco AMP Threat Grid sandboxing	Available																				
URL Filtering: number of categories	More than 80																				
URL Filtering: number of URLs categorized	More than 280 million																				

Features	Cisco Firepower Model														Cisco ASA 5500-FTD-X Model						
	NGFWv	2110	2120	2130	2140	4110	4120	4140	4150	9300 with 1 SM-24 Module	9300 with 1 SM-36 Module	9300 with 1 SM-44 Module	9300 with 3 SM-44 Modules	5506-FTD-X	5506W-FTD-X	5506H-FTD-X	5508-FTD-X	5516-FTD-X	5525-FTD-X	5545-FTD-X	5555-FTD-X
Automated threat feed and IPS signature updates	Yes: class-leading Collective Security Intelligence (CSI) from the Cisco Talos Group (https://www.cisco.com/c/en/us/products/security/talos.html)																				
Third-party and open-source ecosystem	Open API for integrations with third-party products; Snort® and OpenAppID community resources for new and specific threats																				
High availability and clustering	Active/Standby for ESXi and KVM	Active/standby; for Cisco Firepower 9300 intrachassis clustering of up to 5 chassis is allowed; Cisco Firepower 4100 Series allows clustering of up to 6 chassis																			
VLANs maximum	-	1024																			
Cisco Trust Anchor Technologies	-	ASA 5506-X, 5508-X, and 5516-X appliances, Firepower 2100 Series and Firepower 4100 Series and 9300 platforms include Trust Anchor Technologies for supply chain and software image assurance. Please see the section below for additional details																			

Note: Throughput assumes HTTP sessions with an average packet size of 1024 bytes. TLS numbers measured with AVC only policies and 50% TLS traffic with AES256-SHA cipher and RSA 2048-bit keys.

Performance will vary depending on features activated, and network traffic protocol mix, packet size characteristics and hypervisor employed (NGFWv). Performance is subject to change with new software releases. Consult your Cisco representative for detailed sizing guidance.

Table 2 summarizes the performance and capabilities of the Cisco Firepower 2100, 4100 Series and 9300 appliances when running the ASA image. For Cisco ASA 5500-X Series performance specifications with the ASA image, please visit the [Cisco ASA with FirePOWER Services data sheet](https://www.cisco.com/).

Table 2. ASA Performance and Capabilities on Firepower Appliances

Features	Cisco Firepower Appliance Model										
	2110	2120	2130	2140	4110	4120	4140	4150	9300 with 1 SM-24 Module	9300 with 1 SM-36 Module	9300 with 1 SM-44 Module	9300 with 3 SM-44 Modules
Stateful inspection firewall throughput[1]	3 Gbps	6 Gbps	10 Gbps	20 Gbps	35 Gbps	60 Gbps	70 Gbps	75 Gbps	75 Gbps	80 Gbps	80 Gbps	234 Gbps

Features	Cisco Firepower Appliance Model											
	2110	2120	2130	2140	4110	4120	4140	4150	9300 with 1 SM-24 Module	9300 with 1 SM-36 Module	9300 with 1 SM-44 Module	9300 with 3 SM-44 Modules
Stateful inspection firewall throughput (multiprotocol)[2]	1.5 Gbps	3 Gbps	5 Gbps	10 Gbps	15 Gbps	30 Gbps	40 Gbps	50 Gbps	50 Gbps	60 Gbps	60 Gbps	130 Gbps
Concurrent firewall connections	1 million	1.5 million	2 million	3 million	10 million	15 million	25 million	35 million	55 million	60 million	60 million	70 million
Firewall latency (UDP 64B microseconds)	-	-	-	-	3.5	3.5	3.5	3.5	3.5	3.5	3.5	3.5
New connections per second	18000	28000	40000	75000	150,000	250,000	350,000	800,000	800,000	1.2 million	1.8 million	4 million
IPsec VPN throughput (450B UDP L2L test)	500 Mbps	700 Mbps	1 Gbps	2 Gbps	8 Gbps	10 Gbps	14 Gbps	15 Gbps	15 Gbps	18 Gbps	20 Gbps	60 Gbps[3] / 40 Gbps
IPsec/Cisco AnyConnect/Apex site-to-site VPN peers	1500	3500	7500	10000	10,000	15,000	20,000	20,000	20,000	20,000	20,000	60,000[3] / 20,000
Maximum number of VLANs	400	600	750	1024	1024	1024	1024	1024	1024	1024	1024	1024
Security contexts (included; maximum)	2; 25	2; 25	2; 30	2; 40	10; 250	10; 250	10; 250	10; 250	10; 250	10; 250	10; 250	10; 250
High availability	Active/active and active/standby	Active/active and active/standby	Active/active and active/standby	Active/active and active/standby	Active/active and active/standby	Active/active and active/standby	Active/active and active/standby	Active/active and active/standby	Active/active and active/standby	Active/active and active/standby	Active/active and active/standby	Active/active and active/standby
Clustering	-	-	-	-	Up to 16 appliances	Up to 16 appliances	Up to 16 appliances	Up to 16 appliances	Up to 5 appliances with 3 security modules each	Up to 5 appliances with three security modules each	Up to 5 appliances with three security modules each	Up to 5 appliances with 3 security modules each
Scalability	VPN Load Balancing				VPN Load Balancing, Firewall Clustering							
Centralized management	Centralized configuration, logging, monitoring, and reporting are performed by Cisco Security Manager or alternatively in the cloud with Cisco Defense Orchestrator											
Adaptive Security Device Manager	Web-based, local management for small-scale deployments											

[1] Throughput measured with 1500B User Datagram Protocol (UDP) traffic measured under ideal test conditions.

[2] "Multiprotocol" refers to a traffic profile consisting primarily of TCP-based protocols and applications like HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.

[3] In unclustered configuration.

Table 3. Operating Requirements for Firepower NGFWv Virtual Appliances

Platform Support	VMware, KVM, AWS, Azure
Minimum systems requirements: VMware	4 vCPU 8-GB memory 50-GB disk
Minimum systems requirements: KVM	4 vCPU 8-GB memory 50-GB disk
Supported AWS instances	c3.xlarge
Supported Azure instances	Standard_D3
Management options	Firepower Management Center Cisco Defense Orchestrator Firepower Device Manager (VMware)

Hardware Specifications

Tables 4, 5, and 6 summarize the hardware specifications for the 2100 Series, 4100 Series, and 9300 Series, respectively. Table 7 summarizes regulatory standards compliance. For Cisco ASA 5500-X Series hardware specifications, please visit the Cisco ASA with FirePOWER Services data sheet.

Table 4. Cisco Firepower 2100 Series Hardware Specifications

Features	Cisco Firepower Model			
	2110	2120	2130	2140
Dimensions (H x W x D)	1.73 x 16.90 x 19.76 in. (4.4 x 42.9 x 50.2 cm)			
Form factor (rack units)	1RU			
Security module slots	-			
I/O module slots	0		1 NM slot	
Integrated I/O	12 x 10M/100M/1GBASE-T Ethernet interfaces (RJ-45), 4 x 1 Gigabit (SFP) Ethernet interfaces		12 x 10M/100M/1GBASE-T Ethernet interfaces (RJ-45), 4 x 10 Gigabit (SFP+) Ethernet interfaces	
Network modules	None		(FPR-NM-8X10G) 8 x 10 Gigabit Ethernet Enhanced Small Form-Factor Pluggable (SFP+) network module	
	Note: The 2100 Series appliances may also be deployed as dedicated threat sensors with fail-to-wire network modules. Please contact your Cisco representative for details.			
Maximum number of interfaces	Up to 16 total Ethernet ports (12x1G RJ-45, 4x1G SFP)		Up to 24 total Ethernet ports (12x1G RJ-45, 4x10G SFP+, and network module with 8x10G SFP+)	

Features		Cisco Firepower Model			
		2110	2120	2130	2140
Integrated network management ports		1 x 10M/100M/1GBASE-T Ethernet port (RJ-45)			
Serial port		1 x RJ-45 console			
USB		1 x USB 2.0 Type-A (500mA)			
Storage		1x 100 GB, 1x spare slot (for MSP)	1x 100 GB, 1x spare slot (for MSP)	1x 200 GB, 1x spare slot (for MSP)	1x 200 GB, 1x spare slot (for MSP)
Power supplies	Configuration	Single integrated 250W AC power supply.		Single 400W AC, Dual 400W AC optional. Single/Dual 350W DC optional[1]	Dual 400W AC. Single/dual 350W DC optional[1]
	AC input voltage	100 to 240V AC		100 to 240V AC	
	AC maximum input current	< 2.7A at 100V		< 6A at 100V	
	AC maximum output power	250W		400W	
	AC frequency	50 to 60 Hz		50 to 60 Hz	
	AC efficiency	>88% at 50% load		>89% at 50% load	
	DC input voltage	-		-48V to -60VDC	
	DC maximum input current	-		< 12.5A at -48V	
	DC maximum output power	-		350W	
	DC efficiency	-		>88% at 50% load	
	Redundancy	None		1+1 AC or DC with dual supplies	
Fans		4 integrated (2 internal, 2 exhaust) fans[2]		1 hot-swappable fan module (with 4 fans)[2]	
Noise		56 dBA @ 25C 74 dBA at highest system performance.		56 dBA @ 25C 77 dBA at highest system performance.	
Rack mountable		Yes. Fixed mount brackets included (2-post). Mount rails optional (4-post EIA-310-D rack)		Yes. Mount rails included (4-post EIA-310-D rack)	
Weight		16.1 lb (7.3 kg): with 2x SSDs		19.4 lb (8.8 kg) 1 x power supplies, 1 x NM, 1 x fan module, 2x SSDs	21 lb (9.53 kg) 2 x power supplies, 1 x NM, 1 x fan module, 2x SSDs
Temperature: operating		32 to 104°F (0 to 40°C)		32 to 104°F (0 to 40°C) or NEBS operation (see below)[3]	32 to 104°F (0 to 40°C)

Features	Cisco Firepower Model			
	2110	2120	2130	2140
Temperature: nonoperating	-4 to 149°F (-20 to 65°C)			
Humidity: operating	10 to 85% noncondensing			
Humidity: nonoperating	5 to 95% noncondensing			
Altitude: operating	10,000 ft (max)		10,000 ft (max) or NEBS operation (see below)[3]	10,000 ft (max)
Altitude: nonoperating	40,000 ft (max)			
NEBS operation (FPR-2130 Only)[3]	Operating altitude: 0 to 13,000 ft (3962 m) Operating temperature: Long term: 0 to 45°C, up to 6,000 ft (1829 m) Long term: 0 to 35°C, 6,000 to 13,000 ft (1829 to 3964 m) Short term: -5 to 55°C, up to 6,000 ft (1829 m)			

[1] Dual power supplies are hot-swappable.

[2] Fans operate in a 3+1 redundant configuration where the system will continue to function with only 3 operational fans. The 3 remaining fans will run at full speed.

[3] FPR-2130 platform is designed to be NEBS ready. The availability of NEBS certification is pending.

Table 5. Cisco Firepower 4100 Series Hardware Specifications

Features		Cisco Firepower Model			
		4110	4120	4140	4150
Dimensions (H x W x D)		1.75 x 16.89 x 29.7 in. (4.4 x 42.9 x 75.4 cm)			
Form factor (rack units)		1RU			
Security module slots		-			
I/O module slots		2			
Supervisor		Cisco Firepower 4000 Supervisor with 8 x 10 Gigabit Ethernet ports and 2 Network Module (NM) slots for I/O expansion			
Network modules		● 8 x 10 Gigabit Ethernet Enhanced Small Form-Factor Pluggable (SFP+) network modules ● 4 x 40 Gigabit Ethernet Quad SFP+ network modules ● 8-port 1Gbps copper, FTW (fail to wire) Network Module **Note:** Firepower 4100 Series appliances may also be deployed as dedicated threat sensors, with fail-to-wire network modules. Please contact your Cisco representative for details.			
Maximum number of interfaces		Up to 24 x 10 Gigabit Ethernet (SFP+) interfaces; up to 8 x 40 Gigabit Ethernet (QSFP+) interfaces with 2 network modules			
Integrated network management ports		1 x Gigabit Ethernet copper port			
Serial port		1 x RJ-45 console			
USB		1 x USB 2.0			
Storage		200 GB	200 GB	400 GB	400 GB
Power supplies	Configuration	Single 1100W AC, dual optional. Single/dual 950W DC optional[1, 2]	Single 1100W AC, dual optional. Single/dual 950W DC optional[1]	Dual 1100W AC[1]	Dual 1100W AC[1]
	AC input voltage	100 to 240V AC			
	AC maximum input current	13A			
	AC maximum output power	1100W			
	AC frequency	50 to 60 Hz			
	AC efficiency	>92% at 50% load			
	DC input voltage	-40V to -60VDC			
	DC maximum input current	27A			
	DC maximum output power	950W			
	DC efficiency	>92.5% at 50% load			

Features	Cisco Firepower Model			
	4110	4120	4140	4150
Redundancy	1+1			
Fans	6 hot-swappable fans			
Noise	78 dBA			
Rack mountable	Yes, mount rails included (4-post EIA-310-D rack)			
Weight	36 lb (16 kg): 2 x power supplies, 2 x NMs, 6x fans; 30 lb (13.6 kg): no power supplies, no NMs, no fans			
Temperature: operating	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C) or NEBS operation (see below)	32 to 95°F (0 to 35°C), at sea level	32 to 95°F (0 to 35°C), at sea level
Temperature: nonoperating	-40 to 149°F (-40 to 65°C)			
Humidity: operating	5 to 95% noncondensing			
Humidity: nonoperating	5 to 95% noncondensing			
Altitude: operating	10,000 ft (max)	10,000 ft (max) or NEBS operation (see below)	10,000 ft (max)	
Altitude: nonoperating	40,000 ft (max)			
NEBS operation (FPR 4120 only)	Operating altitude: 0 to 13,000 ft (3960 m) Operating temperature: Long term: 0 to 45°C, up to 6,000 ft (1829 m) Long term: 0 to 35°C, 6,000 to 13,000 ft (1829 to 3964 m) Short term: -5 to 50°C, up to 6,000 ft (1829 m)			

[1] Dual power supplies are hot-swappable.

Table 6. Cisco Firepower 9300 Hardware Specifications

Specification	Description
Dimensions (H x W x D)	5.25 x 17.5 x 32 in. (13.3 x 44.5 x 81.3 cm)
Form factor	3 Rack Units (3RU), fits standard 19-in. (48.3-cm) square-hole rack
Security module slots	3
Network module slots	2 (within supervisor)
Supervisor	Cisco Firepower 9000 Supervisor with 8 x 10 Gigabit Ethernet ports and 2 network module slots for I/O expansion
Security modules	• Cisco Firepower 9000 Security Module 24 with 2 x SSDs in RAID-1 configuration • Cisco Firepower 9000 Security Module 36 with 2 x SSDs in RAID-1 configuration
Network modules	• 8 x 10 Gigabit Ethernet Enhanced Small Form-Factor Pluggable (SFP+) network modules

<table>
<tr><th>Specification</th><th colspan="4">Description</th></tr>
<tr><td></td><td colspan="4">• 4 x 40 Gigabit Ethernet Quad SFP+ network modules
• 2 x 100 Gigabit Ethernet Quad SFP28 network modules (double-wide, occupies both network module bays)
Note: Firepower 9300 may also be deployed as a dedicated threat sensor, with fail-to-wire network modules. Please contact your Cisco representative for details.</td></tr>
<tr><td>**Maximum number of interfaces**</td><td colspan="4">Up to 24 x 10 Gigabit Ethernet (SFP+) interfaces; up to 8 x 40 Gigabit Ethernet (QSFP+) interfaces with 2 network modules</td></tr>
<tr><td>**Integrated network management ports**</td><td colspan="4">1 x Gigabit Ethernet copper port (on supervisor)</td></tr>
<tr><td>**Serial port**</td><td colspan="4">1 x RJ-45 console</td></tr>
<tr><td>**USB**</td><td colspan="4">1 x USB 2.0</td></tr>
<tr><td>**Storage**</td><td colspan="4">Up to 2.4 TB per chassis (800 GB per security module in RAID-1 configuration)</td></tr>
<tr><td rowspan="7">**Power supplies**</td><td></td><td>**AC power supply**</td><td>**-48V DC power supply**</td><td>**HVDC power supply**</td></tr>
<tr><td>**Input voltage**</td><td>200 to 240V AC</td><td>-40V to -60V DC*</td><td>240 to 380V DC</td></tr>
<tr><td>**Maximum input current**</td><td>15.5A to 12.9A</td><td>69A to 42A</td><td><14A at 200V</td></tr>
<tr><td>**Maximum output power**</td><td>2500W</td><td>2500W</td><td>2500W</td></tr>
<tr><td>**Frequency**</td><td>50 to 60 Hz</td><td>-</td><td>-</td></tr>
<tr><td>**Efficiency (at 50% load)**</td><td>92%</td><td>92%</td><td>92% (at 50% load)</td></tr>
<tr><td>**Redundancy**</td><td colspan="3">1+1</td></tr>
<tr><td>**Fans**</td><td colspan="4">4 hot-swappable fans</td></tr>
<tr><td>**Noise**</td><td colspan="4">75.5 dBA at maximum fan speed</td></tr>
<tr><td>**Rack mountable**</td><td colspan="4">Yes, mount rails included (4-post EIA-310-D rack)</td></tr>
<tr><td>**Weight**</td><td colspan="4">105 lb (47.7 kg) with one security module; 135 lb (61.2 kg) fully configured</td></tr>
<tr><td>**Temperature: standard operating**</td><td colspan="4">Up to 10,000 ft (3000 M): 32 to 104°F (0 to 40°C) for SM-24 module
32 to 88°F (0 to 35°C) for SM-36 module at sea-level
Altitude adjustment notes:
For SM-36, maximum temp is 35^{0}C, for every 1000 feet above sea level subtract 1^{0}C</td></tr>
<tr><td>**Temperature: NEBS operating**</td><td colspan="4">Long term: 0 to 45°C, up to 6,000 ft (1829 m)
Long term: 0 to 35°C, 6,000 to 13,000 ft (1829-3964 m)
Short term: -5 to 55°C, up to 6,000 ft (1829 m)
Note: Cisco Firepower 9300 NEBS compliance applies only to SM-24 configurations.</td></tr>
<tr><td>**Temperature: nonoperating**</td><td colspan="4">-40 to 149°F (-40 to 65°C); maximum altitude is 40,000 ft</td></tr>
<tr><td>**Humidity: operating**</td><td colspan="4">5 to 95% noncondensing</td></tr>
<tr><td>**Humidity: nonoperating**</td><td colspan="4">5 to 95% noncondensing</td></tr>
</table>

Specification	Description
Altitude: operating	SM-24: 0 to 13,000 ft (3962 m) SM-36: 0 to 10,000 ft (3048 m); please see above Operating Temperature section for temperature adjustment notes
Altitude: nonoperating	40,000 ft (12,192 m)

* Minimum turn-on voltage is -44V DC.

Table 7. Cisco Firepower 2100 Series, 4100 Series and Cisco Firepower 9300 NEBS, Regulatory, Safety, and EMC Compliance

Specification	Description
NEBS	Cisco Firepower 9300 is NEBS compliant with SM-24 Security Modules. Cisco Firepower 4120 is NEBS compliant
Regulatory compliance	Products comply with CE markings per directives 2004/108/EC and 2006/108/EC
Safety	• UL 60950-1 • CAN/CSA-C22.2 No. 60950-1 • EN 60950-1 • IEC 60950-1 • AS/NZS 60950-1 • GB4943
EMC: emissions	• 47CFR Part 15 (CFR 47) Class A (FCC Class A) • AS/NZS CISPR22 Class A • CISPR22 CLASS A • EN55022 Class A • ICES003 Class A • VCCI Class A • EN61000-3-2 • EN61000-3-3 • KN22 Class A • CNS13438 Class A • EN300386 • TCVN7189
EMC: Immunity	• EN55024 • CISPR24 • EN300386 • KN24 • TVCN 7317 • EN-61000-4-2 • EN-61000-4-3 • EN-61000-4-4 • EN-61000-4-5 • EN-61000-4-6 • EN-61000-4-8 • EN-61000-4-11

Cisco Trust Anchor Technologies

Cisco Trust Anchor Technologies provide a highly secure foundation for certain Cisco products. They enable hardware and software authenticity assurance for supply chain trust and strong mitigation against a man-in-the-middle compromise of software and firmware.

Trust Anchor capabilities include:

- **Image signing:** Cryptographically signed images provide assurance that the firmware, BIOS, and other software are authentic and unmodified. As the system boots, the system's software signatures are checked for integrity.
- **Secure Boot:** Secure Boot anchors the boot sequence chain of trust to immutable hardware, mitigating threats against a system's foundational state and the software that is to be loaded, regardless of a user's privilege level. It provides layered protection against the persistence of illicitly modified firmware.
- **Trust Anchor module:** A tamper-resistant, strong-cryptographic, single-chip solution provides hardware authenticity assurance to uniquely identify the product so that its origin can be confirmed to Cisco, providing assurance that the product is genuine.

Firepower DDoS Mitigation

Firepower DDoS Mitigation is provided by Radware Virtual DefensePro (vDP), available and supported directly from Cisco on the following Cisco Firepower 9300 and 4100 series appliances:

Cisco Firepower Model	ASA image	FTD Image
9300 – SM-44	yes	yes
9300 – SM-36	yes	yes
9300 – SM-24	yes	yes
4150	yes	yes
4140	yes	yes
4120	yes	yes
4110	no	yes

Radware vDP is an award-winning, real-time, behavioral DDoS attack mitigation solution that protects organizations against multiple DDoS threats. Firepower DDoS mitigation defends your application infrastructure against network and application degradation and outage.

DDoS Mitigation: Protection Set

Firepower's vDP DDoS mitigation consists of patent-protected, adaptive, behavioral-based real-time signature technology that detects and mitigates zero-day network and application DDoS attacks in real time. It eliminates the need for human intervention and does not block legitimate user traffic when under attack.

The following attacks are detected and mitigated:

- SYN flood attacks
- Network DDoS attacks, including IP floods, ICMP floods, TCP floods, UDP floods, and IGMP floods

- Application DDoS attacks, including HTTP floods and DNS query floods
- Anomalous flood attacks, such as nonstandard and malformed packet attacks

Performance

The performance figures in Table 8 apply to all Cisco Firepower 4100 series models.

Table 8. Key DDoS Performance Metrics for Cisco Firepower 4100 Series

Parameter	Value
Maximum mitigation capacity/throughput	10 Gbps
Maximum legitimate concurrent sessions	209,000 Connections Per Second (CPS)
Maximum DDoS flood attack prevention rate	1,800,000 Packets Per Second (PPS)

The performance figures in Table 9 are for Cisco Firepower 9300 with 1 to 3 Security Modules irrespective of Security Module type (SM-24, SM-36 or SM-44).

Table 9. Key DDoS Performance Metrics for Cisco Firepower 9300 with 1, 2, or 3 Security Modules.

Parameter	Firepower 9300 with 1 Security Module	Firepower 9300 with 2 Security Modules	Firepower 9300 with 3 Security Modules
Maximum mitigation capacity/throughput	10 Gbps	20 Gbps	30 Gbps
Maximum legitimate concurrent sessions	209,000 Connections Per Second (CPS)	418,000 Connections Per Second (CPS)	627,000 Connections Per Second (CPS)
Maximum DDoS flood attack prevention rate	1,800,000 Packets Per Second (PPS)	3,600,000 Packets Per Second (PPS)	5,400,000 Packets Per Second (PPS)

Ordering Information

Cisco Smart Licensing

The Cisco Firepower NGFW is sold with Cisco Smart Licensing. Cisco understands that purchasing, deploying, managing, and tracking software licenses is complex. As a result, we are introducing Cisco Smart Software Licensing, a standardized licensing platform that helps customers understand how Cisco software is used across their network, thereby reducing administrative overhead and operating expenses.

With Smart Licensing, you have a complete view of software, licenses, and devices from one portal. Licenses are easily registered and activated and can be shifted between like hardware platforms. Additional information is available here: https://www.cisco.com/web/ordering/smart-software-licensing/index.html. Related information, on Smart Licensing Smart Accounts, is available here: https://www.cisco.com/web/ordering/smart-software-manager/smart-accounts.html.

Cisco Smart Net Total Care Support: Move Quickly with Anytime Access to Cisco Expertise and Resources

Cisco Smart Net Total Care™ is an award-winning technical support service that gives your IT staff direct anytime access to Technical Assistance Center (TAC) engineers and Cisco.com resources. You receive the fast, expert response and the dedicated accountability you require to resolve critical network issues.

Smart Net Total Care provides the following device-level support:

- Global access 24 hours a day, 365 days a year to specialized engineers in the Cisco TAC
- Anytime access to the extensive Cisco.com online knowledge base, resources, and tools
- Hardware replacement options include 2-hour, 4-hour, Next-Business-Day (NDB) advance replacement, as well as Return For Repair (RFR)
- Ongoing operating system software updates, including both minor and major releases within your licensed feature set
- Proactive diagnostics and real-time alerts on select devices with Smart Call Home

In addition, with the optional Cisco Smart Net Total Care Onsite Service, a field engineer installs replacement parts at your location and helps ensure that your network operates optimally. For more information on Smart Net Total Care please visit: https://www.cisco.com/c/en/us/services/portfolio/product-technical-support/smart-net-total-care.html.

Select Part Numbers

Tables 10, 11, and 12 provide details on part numbers for Cisco Firepower NGFW solutions. Please consult the Ordering Guide for additional configuration options and accessories.

Table 10. Cisco Firepower 2100 Series: Select Product Components

Part Number (Appliance Master Bundle)	Description
FPR2110-BUN	Cisco Firepower 2110 Master Bundle
FPR2120-BUN	Cisco Firepower 2120 Master Bundle
FPR2130-BUN	Cisco Firepower 2130 Master Bundle
FPR2140-BUN	Cisco Firepower 2140 Master Bundle

Part Number (Appliance Master Bundle)	Description
Part Number (Network Module)	**Description**
FPR2K-NM-8X10G=	Spare Cisco Firepower 8-port SFP+ network module
Part Number (Appliances with FTD software)	
FPR2110-NGFW-K9	Cisco Firepower 2110 NGFW Appliance, 1RU
FPR2120-NGFW-K9	Cisco Firepower 2120 NGFW Appliance, 1RU
FPR2130-NGFW-K9	Cisco Firepower 2130 NGFW Appliance, 1RU, 1 x Network Module Bays
FPR2140-NGFW-K9	Cisco Firepower 2140 NGFW Appliance, 1RU, 1 x Network Module Bays
Cisco Firepower 2100 Series NGFW Select Licenses	
L-FPR2110T-TMC=	Cisco Firepower 2110 Threat Defense Threat, Malware, and URL License
L-FPR2120T-TMC=	Cisco Firepower 2120 Threat Defense Threat, Malware, and URL License
L-FPR2130T-TMC=	Cisco Firepower 2130 Threat Defense Threat, Malware, and URL License
L-FPR2140T-TMC=	Cisco Firepower 2140 Threat Defense Threat, Malware, and URL License
Note: These optional security services licenses can be ordered with 1-, 3-, or 5-year subscriptions.	

Part Number (Appliances with ASA Software)	
FPR2110-ASA-K9	Cisco Firepower 2110 ASA Appliance, 1RU
FPR2120-ASA-K9	Cisco Firepower 2120 ASA Appliance, 1RU
FPR2130-ASA-K9	Cisco Firepower 2130 ASA Appliance, 1RU, 1 x Network Module Bays
FPR2140-ASA-K9	Cisco Firepower 2140 ASA Appliance, 1RU, 1 x Network Module Bays
Optional ASA Software Licenses	**Description**
L-FPR2K-ENC-K9=	License to enable strong encryption for ASA on Cisco Firepower 2100 Series
L-FPR2K-ASASC-10=	Cisco Firepower 2100 Add-on 10 security context licenses
L-FPR2K-ASASC-5=	Cisco Firepower 2100 Add-on 5 security context licenses
Hardware Accessories	
Please consult the ordering guide for accessories including rack mounts, spare fans, power supplies, and Solid-State Drives (SSDs)	

Table 11. Cisco Firepower 4100 Series: Select Product Components

Part Number (Appliance Master Bundle)	Description
FPR4110-BUN	Cisco Firepower 4110 Master Bundle, for ASA or Cisco Firepower Threat Defense

Part Number (Appliance Master Bundle)	Description
	Image
FPR4120-BUN	Cisco Firepower 4120 Master Bundle, for ASA or Cisco Firepower Threat Defense Image
FPR4140-BUN	Cisco Firepower 4140 Master Bundle, for ASA or Cisco Firepower Threat Defense Image
FPR4150-BUN	Cisco Firepower 4150 Master Bundle, for ASA or Cisco Firepower Threat Defense Image
Part Number (Spare Network Module)	**Description**
FPR4K-NM-8X10G=	Spare Cisco Firepower 8-port SFP+ network module
FPR4K-NM-4X40G=	Spare Cisco Firepower 4-port QSFP+ network module
Hardware Accessories	
Please consult the ordering guide for accessories including rack mounts, spare fans, power supplies, and Solid-State Drives (SSDs)	
Optional ASA Software Licenses	**Description**
L-F4K-ASA-CAR	License to add Carrier Security Features to ASA
L-FPR4K-ENCR-K9	License to enable strong encryption for ASA on Cisco Firepower 4100 Series
L-FPR4K-ASASC-10	Cisco Firepower 4100 Add-on 10 security context licenses
Cisco Firepower 4100 Series NGFW Select Licenses	
L-FPR4110T-TMC=	Cisco Firepower 4110 Threat Defense Threat, Malware, and URL License
L-FPR4120T-TMC=	Cisco Firepower 4120 Threat Defense Threat, Malware, and URL License
L-FPR4140T-TMC=	Cisco Firepower 4140 Threat Defense Threat, Malware, and URL License
L-FPR4150T-TMC=	Cisco Firepower 4150 Threat Defense Threat, Malware, and URL License
Note: These optional security services licenses can be ordered with 1-, 3-, or 5-year subscriptions.	

Table 12. Cisco Firepower 9300: Select Product Components

Part Number (Chassis)	Description
FPR-C9300-AC	Cisco Firepower 9300 AC Chassis - includes 2 power supply units + 4 fans + rack-mount kit (3RU; accommodates up to three security modules)
FPR-C9300-DC	Cisco Firepower 9300 DC Chassis - includes 2 power supply units + 4 fans + rack-mount kit (3RU; accommodates up to three security modules)

Part Number (Chassis)	Description
FPR-C9300-HVDC	Cisco Firepower 9300 high-voltage DC Chassis - includes 2 power supply units + 4 fans + rack-mount kit (3RU; accommodates up to three security modules)
Part Number (Security Module)	**Description**
FPR9K-SM-24	24 Physical Core Security Module (NEBS Ready)
FPR9K-SM-36	36 Physical Core Security Module
FPR9K-SM-44	44 Physical Core Security Module
ASA Software Licenses for Cisco Firepower 9300	**Description**
L-F9K-ASA-CAR	License to add Carrier Security Features to ASA
L-F9K-ASA-CAR=	License to add Carrier Security Features to ASA
L-F9K-ASA-SC-10	License to add 10 Security Contexts to ASA in Cisco Firepower 9000
L-F9K-ASA-SC-10=	License to add 10 Security Contexts to ASA in Cisco Firepower 9000
L-F9K-ASA	License to run Standard ASA on a Cisco Firepower 9300 module
L-F9K-ASA=	License to run Standard ASA on a Cisco Firepower 9300 module
L-F9K-ASA-ENCR-K9	License to enable strong encryption in ASA running on Cisco Firepower 9000
Cisco Firepower 9300 NGFW Threat Defense Software Licenses	**Description**
FPR9K-TD-BASE	Cisco Firepower Threat Defense Base License for Cisco Firepower 9300 NGFW
L-FPR9K-SM24-TMC=	Cisco Firepower 9000 SM-24 Threat Defense Threat, Malware, and URL License
L-FPR9K-SM24-TMC-3Y	Cisco Firepower 9000 SM-24 Threat Defense Threat, Malware, and URL 3Yr Svc
L-FPR9K-SM36-TMC=	Cisco Firepower 9000 SM-36 Threat Defense Threat, Malware, and URL License
L-FPR9K-SM36-TMC-3Y	Cisco Firepower 9000 SM-36 Threat Defense Threat, Malware, and URL 3Yr Svc
L-FPR9K-SM44-TMC=	Cisco Firepower 9000 SM-44 Threat Defense Threat, Malware, and URL License
L-FPR9K-SM44-TMC-3Y	Cisco Firepower 9000 SM-44 Threat Defense Threat, Malware, and URL 3Yr Svc

[*] **Note:** Firepower 9300 may also be deployed as a dedicated threat sensor, with fail-to-wire network modules. Please contact your Cisco representative for details.

Warranty Information

Find warranty information on cisco.com at the Product Warranties page.

Cisco Services

Cisco offers a wide range of service programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco Services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services for security, visit https://www.cisco.com/go/services/security.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

More Information for Service Providers

For information about Cisco Firepower in service provider environments, please visit:

- https://www.cisco.com/c/en/us/solutions/enterprise-networks/service-provider-security-solutions/

More Information about Firepower NGFWs

For further information about Cisco Firepower NGFWs, please visit:

- https://www.cisco.com/go/ngfw

More Information about Cisco Anyconnect

- Cisco AnyConnect Secure Mobility Client

  https://www.cisco.com/go/anyconnect

- Cisco AnyConnect Ordering Guide

  https://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf

Document History

New or Revised Topic	Described In	Date
Added performance testing information, and updated performance table	Table 1	9-Oct-18
Removed explicit software version numbers from Table 5 and referred readers to the current release note pages	Table 5	19-Jul-18

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USAs C78-736661-19 02/19