Cisco Firepower 9300 Series

Enterprise Firewall

Security Gateway

Next-Generation Firewall

Next-Generation IPS

Contents

Cisco Firepower 9300 Series appliances

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. The 9300 Series platforms can run either the Cisco® Adaptive Security Appliance (ASA) Firewall or Cisco Firepower Threat Defense (FTD).

Model overview

Cisco Firepower 9300 Series summary

Model	Firewall	NGFW	Next-Generation Intrusion Prevention System (NGIPS)	Interfaces	Optional interfaces
SM-24	75G	21G	30G	8 x SFP+ on-chassis	2 x NM's: 1/10/40/100G, FTW
SM-36	80G	29G	37G	8 x SFP+ on-chassis	2 x NM's: 1/10/40/100G, FTW
SM-40(New)	80G	48G	57G	8 x SFP+ on-chassis	2 x NMs: 1/10/40/100G, FTW
SM-44	80G	43G	57G	8 x SFP+ on-chassis	2 x NM's: 1/10/40/100G, FTW
SM-44 x 3	234G	132G	148G	8 x SFP+ on-chassis	2 x NM's: 1/10/40/100G, FTW
SM-48(New)	80G	55G	65G	8 x SFP+ on-chassis	2 x NMs: 1/10/40/100G, FTW
SM-56(New)	80G	64G	73G	8 x SFP+ on-chassis	2 x NMs: 1/10/40/100G, FTW
SM-56 x 3	235G	153G	175G	8 x SFP+ on-chassis	2 x NMs: 1/10/40/100G, FTW

Detailed performance specifications and feature highlights

Table 1. Performance specifications and feature highlights for Cisco Firepower 9300 with the Cisco Firepower Threat Defense image

Features	SM-24	SM-36	SM-40	SM-44	3 x SM-44	SM-48	SM-56	3 x SM-56
Throughput: Firewall (FW) + Application Visibility and	25 Gbps	34 Gbps	54 Gbps	50 Gbps	148 Gbps	64 Gbps	70 Gbps	168 Gbps

Features	SM-24	SM-36	SM-40	SM-44	3 x SM-44	SM-48	SM-56	3 x SM-56
Control (AVC) (1024B)								
Throughput: FW + AVC + Intrusion Prevention System (IPS (1024B)	21 Gbps	29 Gbps	48 Gbps	43 Gbps	132 Gbps	55 Gbps	64 Gbps	153 Gbps
Maximum concurrent sessions, with AVC	30 million	30 million	35 million	30 million	63 million	35 million	35 million	60 million
Maximum new connections per second, with AVC	130K	185K	380K	295K	850K	450K	490K	1.1M
TLS (Hardware Decryption)[2]	7.5 Gbps	8.5 Gbps	10 Gbps	10 Gbps	25 Gbps	11 Gbps	12 Gbps	28 Gbps
Throughput: NGIPS (1024B)	30 Gbps	37 Gbps	57 Gbps	57 Gbps	148 Gbps	66 Gbps	73 Gbps	175 Gbps
IPSec VPN throughput (1024B TCP w/Fastpath)	13.5 Gbps	16 Gbps	20 Gbps	17 Gbps	51 Gbps	25 Gbps	27 Gbps	81 Gbps[1]
Maximum VPN Peers	20,000	20,000	20,000	20,000	60,000	20,000	20,000	60,000
Centralized management	Centralized configuration, logging, monitoring, and reporting are performed by the Management Center or alternatively in the cloud with Cisco Defense Orchestrator							
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 Advanced Malware Protection (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							

Features	SM-24	SM-36	SM-40	SM-44	3 x SM-44	SM-48	SM-56	3 x SM-56
URL filtering: number of categories	More than 80							
URL filtering: number of URLs categorized	More than 280 million							
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 Cisco Firepower 9300 intrachassis clustering of up to 5 chassis is allowed							
Cisco Trust Anchor Technologies	Cisco Firepower 9300 Series platforms include Trust Anchor Technologies for supply chain and software image assurance.							

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

[1] In unclustered configuration.

[2] Throughput measured with 50% TLS 1.2 traffic with AES256-SHA with RSA 2048B keys.

Table 2. ASA performance and capabilities on Cisco Firepower 9300

Features	SM-24	SM-36	SM-40	SM-44	3 x SM-44	SM-48	SM-56	3 x SM-56
Stateful inspection firewall throughput[1]	75 Gbps	80 Gbps	80 Gbps	80 Gbps	234 Gbps	80 Gbps	80 Gbps	235 Gbps
Stateful inspection firewall throughput (multiprotocol)[2]	50 Gbps	60 Gbps	55 Gbps	60 Gbps	130 Gbps	60 Gbps	64 Gbps	172 Gbps
Concurrent firewall connections	55 million	60 million	55 million	60 million	70 million	60 million	60 million	195 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	800,000	1.2 million	1.6 million	1.8 million	4 million	1.8 million	2 million	4.75 million

Features	SM-24	SM-36	SM-40	SM-44	3 x SM-44	SM-48	SM-56	3 x SM-56
IPsec VPN throughput (450B UDP L2L test)	15 Gbps	18 Gbps	25 Gbps	20 Gbps	60 Gbps[3]	27 Gbps	30 Gbps	74 Gbps
Maximum VPN Peers	20,000	20,000	20,000	20,000	60,000	20,000	20,000	60,000
Security contexts (included; maximum)	10; 250							
High availability	Active/active and active/standby							
Clustering	Up to 5 appliances with 3 security modules each							
Scalability	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.

Performance testing methodologies LINK

Hardware specifications

Table 3.   Cisco Firepower 9300 Series 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 40 with 2 x SSDs in RAID-1 configuration • Cisco Firepower 9000 Security Module 48 with 2 x SSDs in RAID-1 configuration • Cisco Firepower 9000 Security Module 56 with 2 x SSDs in RAID-1 configuration
Network modules (2 module slots per chassis)	• 8 x 10 Gigabit Ethernet Enhanced Small Form-Factor Pluggable (SFP+) network modules • 4 x 40 Gigabit Ethernet Quad SFP+ network modules

Specification	Description			
	• 2 x 100 Gigabit Ethernet Quad SFP28 network modules • 4 x 100 Gigabit Ethernet Quad SFP28 network modules **Note:** Cisco Firepower 9300 may also be deployed as a dedicated threat sensor, 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; up to 8 x 100 Gigabit Ethernet interfaces with two network modules			
Integrated network management ports	1 x Gigabit Ethernet copper port (on supervisor)			
Serial port	1 x RJ-45 console			
USB	1 x USB 2.0			
Storage	Up to 4.8 TB per chassis (1.6 TB per security module in RAID-1 configuration)			

Power supplies		AC power supply	-48V DC power supply	HVDC power supply
	Input voltage	200 to 240V AC	-40V to -60V DC[*]	240 to 380V DC
	Maximum input current	15.5A to 12.9A	69A to 42A	<14A at 200V
	Maximum output power	2500W	2500W	2500W
	Frequency	50 to 60 Hz	-	-
	Efficiency (at 50% load)	92%	92%	92% (at 50% load)
	Redundancy	1+1		

Specification	Description
Fans	4 hot-swappable fans
Noise	75.5 dBA at maximum fan speed
Rack mountable	Yes, mount rails included (4-post EIA-310-D rack)
Weight	105 lb (47.7 kg) with one security module; 135 lb (61.2 kg) fully configured
Temperature: standard operating	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°C, for every 1000 feet above sea level subtract 1°C
Temperature: NEBS operating	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,SM-40,SM-44 and SM-48 configurations.
Temperature: nonoperating	-40 to 149°F (-40 to 65°C); maximum altitude is 40,000 ft
Humidity: operating	5 to 95% noncondensing
Humidity: nonoperating	5 to 95% noncondensing
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

Specification	Description
	adjustment notes
Altitude: nonoperating	40,000 ft (12,192 m)

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

Table 4.   Cisco Firepower 9300 Series NEBS, regulatory, safety, and EMC compliance

Specification	Description
NEBS	Cisco Firepower 9300 is NEBS compliant with SM-24,SM-40, SM-44 and SM-48 Security Modules
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, EN61000-4-11

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.

Printed in USA

C78-742471-01 08/19