Cisco Firepower 9300 Series

Enterprise Firewall | Security Gateway | Dedicated IPS

Contents

Cisco Firepower 9300 Series appliances

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 point in network requiring low (less than 5-microsecond offload) latency and exceptional throughput. Firepower 9300 supports flow-offloading, programmatic orchestration, and the management of security services with RESTful APIs. The appliance uses AI/ML to detect anomalies, remediate threats, and optimize firewall policy for peak performance. NetOps and SecOps operations are streamlined using the multi-threaded Snort 3 engine, while admins benefit from natural language interactions using the AI chatbot for guidance, troubleshooting, and policy configuration. The appliance is SD-WAN capable and allows for simplified site-to-site communication using on-demand tunnels and dynamic application path selection across multiple WAN interfaces. Firepower 9300 is also available in Network Equipment Building Standards (NEBS)-compliant configurations. The 9300 Series runs either the Cisco Secure Firewall ASA or Threat Defense (FTD) software.

Model overview

Cisco Firepower 9300 Series summary

Model	Firewall	NGFW	Next-Generation Intrusion Prevention System (NGIPS)	Interfaces	Optional interfaces
SM-40	80G	55G	60G	8 x SFP+ on-chassis	2 x NMs: 1/10/40/100G, FTW
SM-48	80G	65G	68G	8 x SFP+ on-chassis	2 x NMs: 1/10/40/100G, FTW
SM-56	80G	68G	73G	8 x SFP+ on-chassis	2 x NMs: 1/10/40/100G, FTW
SM-56 x 3	235G	190G	190G	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 Threat Defense (FTD) image

Features	SM-40	SM-48	SM-56	3 x SM-56
Throughput: Firewall (FW) + Application Visibility and Control (AVC) (1024B)	55 Gbps	65 Gbps	70 Gbps	190 Gbps
Throughput: FW + AVC + Intrusion Prevention **System (IPS (1024B)**	55 Gbps	65 Gbps	68 Gbps	190 Gbps
Maximum concurrent sessions, with AVC	35 million	35 million	35 million	60 million
Maximum new connections per second, with AVC	380K	450K	490K	1.1M
TLS (Hardware Decryption)[2]	10 Gbps	11 Gbps	12 Gbps	28 Gbps
Throughput: NGIPS (1024B)	60 Gbps	68 Gbps	73 Gbps	190 Gbps
IPSec VPN throughput (1024B TCP/Fastpath)	27 Gbps	33 Gbps	36 Gbps	110 Gbps[1]
Maximum VPN Peers	20,000	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			

[1] In unclustered configuration.

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

Features	SM-40	SM-48	SM-56	3 x SM-56
AVC: OpenAppID support for custom, open-source application detectors	Standard			
Cisco Security Intelligence	Standard, with IP, URL, and DNS threat intelligence.			
Cisco IPS License	Available; can passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence.			
Cisco Malware Defense 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 Secure Endpoint is also optionally available.			
Cisco Malware Analytics (sandboxing)	Available			
URL filtering: number of categories	More than 120			
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/active (with clustering) and Active/standby; up to 6 modules across up to 6 different Firepower 9300 chassis.			
Cisco Trust Anchor Technologies	Cisco Firepower 9300 Series platforms include Trust Anchor Technologies for supply chain and software image assurance.			

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

Table 2.   ASA software performance and capabilities on Cisco Firepower 9300

Features	SM-40	SM-48	SM-56	3 x SM-56
Stateful inspection firewall throughput[1]	80 Gbps	80 Gbps	80 Gbps	235 Gbps
Stateful inspection firewall throughput (multiprotocol)[2]	55 Gbps	60 Gbps	64 Gbps	172 Gbps
Concurrent firewall connections	55 million	60 million	60million	195 million
Firewall latency (UDP 64B microseconds)	3.5	3.5	3.5	3.5
New connections per second	1.6 million	1.8 million	2 million	4.75 million
IPsec VPN throughput (450B UDP L2L test)	25 Gbps	27 Gbps	30 Gbps	74 Gbps
Maximum VPN Peers	20,000	20,000	20,000	60,000
Security contexts (included; maximum)	10; 250			
High availability	Active/active and active/standby			
Clustering	Up to 16 security modules across up to 16 different Firepower 9300 chassis			
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.

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 • 2 x 100 Gigabit Ethernet Quad SFP28 network modules • 4 x 100 Gigabit Ethernet Quad SFP28 network modules • 6-port 10Gbps SR Fiber FTW (fail to wire) Network Module • 6-port 10Gbps LR Fiber FTW (fail to wire) Network Module • 2-port 40Gbps SR FTW (fail to wire) Network Module **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.

Specification	Description			
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; up to 24 x 1 Gigabit Ethernet ports (SFP) with network modules and fixed ports.			
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	2,500W	2,500W	2,500W
	Frequency	50 to 60 Hz	-	-
	Efficiency (at 50% load)	92%	92%	92% (at 50% load)
	Redundancy	1+1		
Fans	4 hot-swappable fans			

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

Specification	Description
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-40 module 32 to 104°F (0 to 40°C) for SM-48 module at sea level. Altitude adjustment notes: For SM-56, 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:** Firepower 9300 NEBS compliance applies only to SM-40 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-40, SM-48: 0 to 13,000 ft (3962 m) SM-56: 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)

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

Specification	Description
NEBS	Cisco Firepower 9300 is NEBS compliant with SM-40 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**.