Cisco Secure Firewall 4100 Series

Enterprise Firewall

Next Generation Firewall

Next Generation IPS

Contents

Cisco Secure Firewall 4100 Series appliances

The Cisco Secure Firewall 4100 Series is a family of four threat-focused NGFW security platforms. Their throughput range addresses internet edge, data center and service provider use cases. They deliver superior threat defense, at faster speeds, with a smaller footprint. Cisco Secure Firewall 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 Secure Firewall 4125 platform. The 4100 Series platforms can run either the Cisco Secure Firewall ASA or Cisco Secure Firewall Threat Defense (FTD) software.

Model overview

Cisco Secure Firewall 4100 Series summary:

Model	Firewall	NGFW	IPS	Interfaces	Optional Interfaces
FPR-4112	40G	19G	19G	8 x SFP+ on-chassis	2 x NM's: 1/10/40/100G, FTW
FPR-4115	80G	33G	33G	8 x SFP+ on-chassis	2 x NM's: 1/10/40/100G, FTW
FPR-4125	80G	45G	45G	8 x SFP+ on-chassis	2 x NM's: 1/10/40/100G, FTW
FPR-4145	80G	53G	55G	8 x SFP+ on-chassis	2 x NM's: 1/10/40/100G, FTW

Detailed performance specifications and feature highlights

Table 1. Performance specifications and feature highlights for Cisco Secure Firewall 4100 with the Cisco Secure Firewall Threat Defense (TD) image

Features	4112	4115	4125	4145
Throughput: FW + AVC (1024B)	19 Gbps	33 Gbps	45 Gbps	53 Gbps
Throughput: FW + AVC + IPS (1024B)	19 Gbps	33 Gbps	45 Gbps	53 Gbps
Maximum concurrent sessions, with AVC	10 million	15 million	25 million	30 million
Maximum new connections per second, with AVC	98K	210K	269K	365K
TLS (Hardware Decryption)[1]	4.5 Gbps	6.5 Gbps	8.5 Gbps	10 Gbps
Throughput: NGIPS (1024B)	19 Gbps	33 Gbps	45 Gbps	55 Gbps

Features	4112	4115	4125	4145
IPSec VPN Throughput (1024B TCP w/Fastpath)	8.5 Gbps	12.5 Gbps	19 Gbps	24 Gbps
Maximum VPN Peers	10,000	15,000	20,000	20,000
Multi-Instance Capable	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 6000 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 Secure 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	Cisco Secure Firewall 4100 Series with Firepower Threat Defense in HA configuration supports Active/Standby setup. This is available at the appliance level or logical instances defined on two different appliances. Please check latest High Availability Configuration Guide chapter for guidelines and best practices.			
Clustering	Cisco Secure Firewall 4100 Series with Firepower Threat Defense allows clustering of up to 16 appliances, or up to 16 instances across different appliances running Multi Instance feature. Clustering allows to increase overall performance and scale. Please check latest Clustering Configuration Guide chapter for guidelines and best practices.			
Cisco Trust Anchor Technologies	Cisco Secure Firewall 4100 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] Throughput measured with 50% TLS 1.2 traffic with AES256-SHA with RSA 2048B keys.

Table 2. ASA Performance and capabilities on Cisco Secure Firewall 4100 appliances

Features	4112	4115	4125	4145
Stateful inspection firewall throughput[1]	40 Gbps	80 Gbps	80 Gbps	80 Gbps
Stateful inspection firewall throughput (multiprotocol)[2]	30 Gbps	40 Gbps	45 Gbps	50 Gbps
Concurrent firewall connections	10 million	15 million	25 million	40 million
Firewall latency (UDP 64B microseconds)	3.5	3.5	3.5	3.5
New connections per second	400,000	848K	1.1 million	1.5 million
IPsec VPN throughput (450B UDP L2L test)	9 Gbps	15 Gbps	19 Gbps	23 Gbps
Maximum VPN Peers	10,000	15,000	20,000	20,000
Security contexts (included; maximum)	10; 250	10; 250	10; 250	10; 250
High availability	Active/active or active/standby. Active/active is only available with multiple contexts configured. Please check latest Failover for High Availability Configuration Guide chapter for guidelines and best practices.			
Clustering	Up to 16 appliances. Please check latest High Availability and Scalability Configuration Guide chapter for guidelines and best practices.			
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.

[3] In unclustered configuration.

Hardware specifications

Table 3. Cisco Secure Firewall 4100 Series hardware specifications

Features		4112	4115	4125	4145
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			
Supervisor		Cisco Secure Firewall 4000 Supervisor with 8 x 10 Gigabit Ethernet ports and 2 Network Module (NM) slots for I/O expansion			
Network modules		• 2 x 100 Gigabit Ethernet QSFP28 Network Module • 8 x 10 Gigabit Ethernet Enhanced Small Form-Factor Pluggable (SFP+) network modules ◦ 8 x 1 Gbps Fiber or 4 x 1Gbps Copper SFP Network Module • 4 x 40 Gigabit Ethernet Quad SFP+ network modules • 8-port 1Gbps copper, FTW (fail to wire) Network Module ◦ Ports that are not configured as FTW can be used as regular 1 Gb copper ports • 6-port 1 Gbps SX Fiber FTW (fail to wire) Network Module • 6-port 10Gbps SR Fiber FTW (fail to wire) Network Module • 6-port 10Gbps LR Fiber FTW (fail to wire) Network Module • 2-port 40G SR FTW (fail to wire) Network Module • 2-port 100Gbps Network Module			
Maximum number of interfaces		Up to 4 x 100 Gigabit Ethernet (QSFP28) interfaces, 24 x 10 Gigabit Ethernet (SFP+) interfaces; up to 8 x 40 Gigabit Ethernet (QSFP+) interfaces with 2 network modules; up to 24 x 1 Gigabit Ethernet ports(SFP) with network modules and fixed ports			
Integrated network management ports		1 Gigabit Ethernet SFP port Supports 1Gbps fiber or copper optical modules			
Serial port		1 x RJ-45 console			
USB		1 x USB 2.0			
Storage		400 GB	400 GB	800 GB	800 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, 2]	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			

Features		4112	4115	4125	4145
	DC input voltage	-40V to -60VDC			
	DC maximum input current	27A			
	DC maximum output power	950W			
	DC efficiency	>92.5% at 50% load			
	Redundancy	1+1			
Fans		6 hot-swappable fans			
Noise		Typical 63 dBA, max is 74 dBA			
Rack mountable		Yes, mount rails included (4-post EIA-310-D rack)			
Weight		4112/4115/4125/4145: 39.4 lb (17.87 kg) 2 x power supplies, 2 x NMs, 6 x fans; 31.4 lb (14.24 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)	32 to 104° F (0 to 40° C) or NEBS operation (see below)	32 to 104° F (0 to 40° 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)	10,000 ft (max)	10,000 ft (max)
Altitude: nonoperating		40,000 ft (max)			
NEBS operation (FPR 4125 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 4. Cisco Secure Firewall 4100 Series NEBS, Regulatory, Safety, and EMC Compliance

Specification	Description
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.

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 USA C78-742474-06 09/23