Data Sheet

Cisco Firepower Appliances

Next-Generation Firewall

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.

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 1000 Series, 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.

Cisco Firepower 1000 Series Appliances - Detailed Platform Specifications

Cisco Firepower 2100 Series Appliances – Detailed Platform Specifications

Cisco Firepower 4110, 4120, 4140, 4150 - Detailed Platform Specifications

Cisco Firepower 4115, 4125, 4145- Detailed Platform Specifications

Cisco Firepower 9300 SM24, SM36, SM44 - Detailed Platform Specifications

Cisco Firepower 9300 SM40, SM48, SM56 - Detailed Platform Specifications

Cisco ASA 5500-FTD-X Series Appliances - Detailed Platform Specifications

Performance Testing Methodologies – Detailed Performance Testing Information

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.

Table 1. 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)

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 1000 Series, 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.

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

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.

Firepower DDoS Mitigation is provided by 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 Series – All Security Modules	Yes	Yes
4100 Series – All Models	Yes	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 the table below apply to all Cisco Firepower 4100 series models.

Table 2. 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.

Table 3. 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

The tables below provide details on part numbers for Cisco Firepower NGFW solutions. Please consult the Ordering Guide for additional configuration options and accessories.

Table 4. Cisco Firepower Series Bundle PID's

Part number (Appliance master bundle)	Description
FPR1010-BUN	Cisco Firepower 1010 Master Bundle
FPR1120-BUN	Cisco Firepower 1120 Master Bundle
FPR1140-BUN	Cisco Firepower 1140 Master Bundle
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
FPR4110-BUN	Cisco Firepower 4110 Master Bundle
FPR4115-BUN	Cisco Firepower 4115 Master Bundle
FPR4120-BUN	Cisco Firepower 4120 Master Bundle
FPR4125-BUN	Cisco Firepower 4125 Master Bundle
FPR4140-BUN	Cisco Firepower 4140 Master Bundle
FPR4145-BUN	Cisco Firepower 4145 Master Bundle
FPR4150-BUN	Cisco Firepower 4150 Master Bundle
FPR-C9300-AC	Cisco Firepower 9300 Appliance ASA Bundle, AC supplies
FPR-C9300-DC	Cisco Firepower 9300 Appliance ASA Bundle, DC supplies
FPR-C9300-HVDC	Cisco Firepower 9300 Appliance ASA Bundle, HVDC supplies

Part number (Appliance master bundle)	Description
FPR9K-SM24-FTD-BUN	Cisco Firepower 9300 Security Module 24 FTD Bundle
FPR9K-SM36-FTD-BUN	Cisco Firepower 9300 Security Module 36 FTD Bundle
FPR9K-SM44-FTD-BUN	Cisco Firepower 9300 Security Module 44 FTD Bundle
FPR9K-SM40-FTD-BUN	Cisco Firepower 9300 Security Module 40 FTD Bundle
FPR9K-SM48-FTD-BUN	Cisco Firepower 9300 Security Module 48 FTD Bundle
FPR9K-SM56-FTD-BUN	Cisco Firepower 9300 Security Module 56 FTD Bundle

Note: The Bundle PID's offer the ability to choose hardware, hardware options, licenses and subscriptions.

Table 5. Cisco Firepower Network Module PID's

Part Number (Appliance Master Bundle)	Description
FPR2K-NM-8X1G	Cisco Firepower 8 Port SFP 1G Network Module
FPR2K-NM-8X1G-F	Cisco Firepower 8 Port 1G Copper FTW Network Module
FPR2K-NM-6X1SX-F	Cisco Firepower 6 Port 1G Fiber FTW Network Module
FPR2K-NM-8X10G	Cisco Firepower 8 Port SFP+ 10G Network Module
FPR2K-NM-6X10SR-F	Cisco Firepower 6 Port 10G SR FTW Network Module
FPR2K-NM-6X10LR-F	Cisco Firepower 6 Port 10G LR FTW Network Module
FPR4K-NM-8X1G	Cisco Firepower 8 Port SFP 1G Network Module
FPR4K-NM-8X1G-F	Cisco Firepower 8 Port 1G Copper FTW Network Module
FPR4K-NM-6X1SX-F	Cisco Firepower 6 Port 1G Fiber FTW Network Module
FPR4K-NM-8X10G	Cisco Firepower 8 Port SFP+ 10G Network Module
FPR4K-NM-6X10SR-F	Cisco Firepower 6 Port 10G SR FTW Network Module
FPR4K-NM-6X10LR-F	Cisco Firepower 6 Port 10G LR FTW Network Module
FPR4K-NM-4X40G	Cisco Firepower 4 Port 40G QSFP+ Network Module
FPR4K-NM-2X40G-F	Cisco Firepower 4 Port 40G SR FTW Network Module
FPR9K-NM-6X1SX-F	Cisco Firepower 6 Port 1G Fiber FTW Network Module
FPR9K-NM-8X10G	Cisco Firepower 8 Port SFP+ 10G Network Module
FPR9K-NM-6X10SR-F	Cisco Firepower 6 Port 10G SR FTW Network Module
FPR9K-NM-6X10LR-F	Cisco Firepower 6 Port 10G LR FTW Network Module

Part Number (Appliance Master Bundle)	Description
FPR9K-NM-4X40G	Cisco Firepower 4 Port 40G QSFP+ Network Module
FPR9K-NM-2X40G-F	Cisco Firepower 4 Port 40G SR FTW Network Module
FPR9K-NM-2X100G	Cisco Firepower 2 Port 100G Network Module
FPR9K-NM-4X100G	Cisco Firepower 4 Port 100G Network Module
FPR9K-DNM-2X100G	Cisco Firepower 2 Port 100G Network Module, Double Width

Note: The above PID's are used in appliance configurations in CCW. For a standalone/spare version, simply add "=" when searching in CCW.

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

C78-742480-00 06/19