Cisco Firepower NGIPS

Contents

Integrated network threat appliances

Cisco Firepower NGIPS delivers deep visibility, preeminent security intelligence and superior advanced threat protection to secure today's complex IT environments.

Product overview

Cisco Firepower Next-Generation IPS (NGIPS) threat appliances provide network visibility, security intelligence, automation and advanced threat protection. It uses industry-leading intrusion prevention capabilities and multiple techniques to detect even the most sophisticated network attacks and protect you against them. Cisco Firepower NGIPS threat appliances all offer the ability to operate in-line via Fail-To-Wire/Bypass network modules.

Cisco Firepower NGIPS continuously discovers information about your network environment, including data about operating systems, mobile devices, files, applications and users. It then uses this information to build network maps and host profiles. This gives you the contextual information you need to make better decisions about intrusion events. And this information is also used as input to better enable the automation of key threat protection features.

Cisco's TALOS Security Intelligence and Research Group collects and correlates threats in real time using the largest threat detection network in the world. Their efforts result in vulnerability-focused IPS rules and embedded IP-, URL-, and DNS-based security intelligence for Firepower NGIPS.

Security automation correlates intrusion events with your network's vulnerabilities so you can focus on the threats that matter most. It also analyzes your network's weaknesses and recommends the appropriate security policies to put in place.

Cisco Firepower NGIPS threat appliances provide industry leading threat effectiveness against both known and unknown threats. Features include:

- IPS rules that identify and block attack traffic that target vulnerabilities in your network
- Tightly integrated defense against advanced malware incorporating advanced analysis of network and endpoint activity
- Sandboxing technology that uses hundreds of behavioral indicators to identify zero-day and evasive attacks

Features and benefits

Feature	Benefit
Superior effectiveness	Stop more threats, both known and unknown, with industry-leading threat protection. Speeds time to detection of malware to reduce its damage and spread
Contextual awareness	With real-time visibility, gain more insight into and control over the users, applications, devices, threats, and vulnerabilities in your network
Advanced threat protection and rapid remediation	Rapidly detect, block, contain and remediate advanced threats through tightly integrated AMP and sandboxing solutions. Patch vulnerabilities "virtually" and instantaneously before new software or signatures become available

Feature	Benefit
Security automation	Automatically correlate threat events, contextual awareness information, and vulnerability data to better focus your staff, implement better security and speed forensic investigations
Granular application visibility and control	Reduce threats to your network through precise control over more than 4000 commercial applications, with support for custom applications
Global threat intelligence from Cisco's Talos Security Intelligence and Research Group	Benefit from worldwide threat visibility and analysis that produces over 35,000 IPS rules and embedded IP-, URL- and DNS-based security intelligence for up-to-the-minute threat protection

Prominent feature/differentiator/capability

Next-generation intrusion prevention capabilities

Cisco Firepower NGIPS sets a new standard for network threat protection. It integrates real-time contextual awareness, security automation, advanced malware protection, and superior threat intelligence with industry-leading network intrusion prevention. No other solution offers the visibility, simplicity, openness, and effectiveness required to protect today's dynamic environments against increasingly sophisticated threats.

Cisco Firepower NGIPS stands apart from other intrusion prevention solutions by including the following features and capabilities:

Superior threat protection

- Cisco Firepower NGIPS is built on the core open technology of Snort, the world's most popular intrusion prevention software. It uses vulnerability and anomaly-based inspection methods to alert you to malicious hosts, network malware attacks, file movement, and zero-day threats.
- The Cisco Talos Security Intelligence and Research Group analyzes 600 billion emails, more than 1 billion web queries, and nearly 1.5 million malware samples daily to identify the latest threats and vulnerabilities.
- Independent NSS Labs breach detection system testing found that Firepower NGIPS was 99.7% effective in stopping threats and 100% effective in identifying evasion techniques that are used to hide attacks.

Real-time contextual awareness

- Collected and analyzed data includes information about applications, users, devices, operating systems, vulnerabilities, mobile devices, client-side applications, services, processes, network behaviors, files, and threats.
- Contextual data can also be used in your IPS rules to provide an extraordinarily high level of granular protection.

Intelligent security automation

- Intrusion events are automatically correlated with your network's vulnerabilities. You are alerted to attacks that might be successful and your analysts can focus on those threats that matter most.
- Your network's weaknesses are analyzed and automatically generate recommended security policies to put in place to address your vulnerabilities. This process helps analysts deal with ever changing networks and provides protection that is custom fitted to your environment.
- Indications of Compromise (IoCs) provide another method of threat detection for unknown threats. Hosts that might be potentially compromised are identified by correlating specific events from multiple sources (IPS, security intelligence, network and endpoint malware protection, etc.). A prioritized dashboard and quick links to inspect activity help analysts investigate and remediate these compromised hosts.
- Specific users are associated with their IPS events through captive portal technology and through integration with Active Directory and other LDAP technology. This capability facilitates better monitoring and analysis and speeds forensic investigations.

Protection against advanced threats

- A fully integrated Advanced Malware Protection (AMP) solution addresses evasive and sophisticated file-related threats, and provides the ability to rapidly track, contain, analyze and remediate successful attacks.
- Key features provide early detection into evasive and emerging malware threats, delivering an industry-leading 13-hour median time to detection (Source: Cisco Annual Security Report, January 2016).
- File sandboxing (in the cloud or on premise), threat scoring, and malware behavior analysis to address unknown and zero-day attacks.
- Organizations are immediately alerted to newly identified malicious content in their environment even after the initial analysis allowed the file or malware in.

Management, integration and deployment options

- The Cisco Firepower Management Center provides a single point of event collection and policy management for all deployments of Cisco Firepower NGIPS, Cisco Firepower Threat Defense for ISR, and Cisco Firepower NGFW. You gain a comprehensive enterprise-wide view of security posture, consistent security at all points in your network, and less management complexity.
- Integration with many Cisco network security products provides greater threat effectiveness with less complexity and lower cost. For example, Cisco Firepower NGIPS detections can drive automated remediation actions (quarantine, block, etc.) to take place in Cisco's Identity Services Engine (ISE) for rapid threat containment.
- Available as both physical and virtual NGIPS platforms, this provides a great means to segment portions of your network where other methods are impractical.
- Cisco Firepower Threat Defense for ISR delivers Firepower NGIPS threat capabilities on Cisco Integrated Services Routers. The security concerns of branch offices and other remote locations are addressed without increasing the security infrastructure footprint.

Application control and URL filtering

- Application Visibility and Control provides granular control of application usage and user access to more than 4000 commercial applications.
- With OpenAppID, an open source application identification standard led by Cisco, you can define custom, localized, and cloud applications so that they can be controlled in the same manner as commercial applications.
- URL filtering option improves both security and compliance. It provides access control to over 80 categories of websites and covers more than 200 million individual URLs. Preventing access to known risky or malicious sites reduces the risk of web-borne malware.

Platform support

Cisco Firepower NGIPS includes Application Visibility and Control (AVC) as part of the base product. Optional licenses are available for Cisco Advanced Malware Protection (AMP) for Networks, and URL Filtering. The Cisco Firepower 2100 Series, 4100 Series and 9300 Series appliances use the Cisco Firepower Threat Defense software image.

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.

The Cisco Firepower 4100 Series is a family of four threat-focused NGIPS security platforms. Their maximum throughput ranges from 12 to 24 Gbps, addressing use cases from the Internet edge to the data center. They deliver superior threat defense, at faster speeds, with a smaller footprint.

The Cisco Firepower 9300 is a scalable, carrier-grade, modular platform designed for service providers, high-performance computing centers, 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.

Licensing

The Cisco Firepower NGIPS is sold with Cisco Smart Licensing. Cisco understands that purchasing, deploying, managing, and tracking software licenses can be extremely 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 saving 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 and 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.

Our award-winning Cisco Smart Net Total Care™ 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 need 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 that 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, the Cisco Smart Net Total Care Onsite Service provides a field engineer to install replacement parts at your location and help ensure that your network operates at the highest levels.

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.

Product specifications

Performance Specifications and Feature Highlights

Table 1 summarizes the capabilities of the Cisco Firepower 2100, 4100, and 9300 Series appliances when running the Cisco Firepower NGIPS.

Table 1. Performance[2] specifications and feature highlights with the Firepower NGIPS

Features	Cisco Firepower Model								
	2130	2140	4115	4125	4145	9300 with SM-40	9300 with SM-48	9300 with SM-56	9300 with SM-56 x 3
Throughput: NGIPS (1024B)	4.7 Gbps	9 Gbps	27 Gbps	41 Gbps	55 Gbps	57 Gbps	66 Gbps	73 Gbps	175 Gbps
Throughput: NGIPS (450B)	1.5 Gbps	3 Gbps	9 Gbps	15 Gbps	19 Gbps	21 Gbps	23 Gbps	27 Gbps	64 Gbps
Maximum concurrent sessions	2M	3M	15M	25M	30M	35M	35M	35M	60M

Features	Cisco Firepower Model								
Maximum new connections per second	27K	57K	200K	265K	350K	380K	450K	490K	1.1M
Integrated Interfaces	12 x 1GE RJ45, 4 x SFP+	12 x 1GE RJ45, 4 x SFP+	8 x SFP+	8 x SFP+	8 x SFP+	8 x SFP+	8 x SFP+	8 x SFP+	8 x SFP+
Max Fail-to-Wire (FTW) Interfaces	8 x 1GE RJ45 6 x 1GE SX 6 x 10G SR 6 x 10G LR		16 x 1GE RJ45 12 x 1GE SX 12 x 10G SR 12 x 10G LR 4 x 40G SR			12 x 1GE SX 12 x 10G SR 12 x 10G LR 4 x 40G SR			
Cisco Security Intelligence	Standard, with IP-, URL-, and DNS-based threat 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 and URLs categorized	More than 80 categories with more than 280 million individual URLs								
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								
Centralized management	Centralized configuration, logging, monitoring, and reporting is performed by the Firepower Management Center								
High availability and clustering	Active/standby; with Cisco Firepower 9300 intrachassis clustering is also supported								
Cisco Trust Anchor Technologies	Cisco 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								

[2] 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.

Ordering information

Ordering Information for Cisco Firepower NGIPS, available options, and hardware parts can be found in the Cisco Network Security Ordering Guide. What follows are a series of tables listing out specific components related to Firepower NGIPS.

Table 2. Cisco Firepower 2100 Series Threat appliance bundles

Part Number (Appliance primary bundle)	Description
FPR2130-BUN (FRP2140-NGFW-K9)	Cisco Firepower 2130 NGFW Appliance, 1RU, 1 x Network Module Bay
FPR2140-BUN (FPR2140-NGFW-K9)	Cisco Firepower 2140 NGFW Appliance, 1RU, 1 x Network Module Bay

Table 3. Cisco Firepower 4100 Series Threat appliance bundles

Part number (Appliance primary bundle)	Description
FPR4115-BUN (FPR4115-NGIPS-K9)	Cisco Firepower 4115 NGIPS Appliance, 1RU, 2 x Network Module Bays
FPR4125-BUN (FPR4125-NGIPS-K9)	Cisco Firepower 4125 NGIPS Appliance, 1RU, 2 x Network Module Bays
FPR4145-BUN (FRP4145-NGIPS-K9)	Cisco Firepower 4145 NGIPS Appliance, 1RU, 2 x Network Module Bays
Hardware Accessories	
Please consult the ordering guide for accessories including rack mounts, spare fans, power supplies, and Solid-State Drives (SSDs)	

Table 4. Cisco Firepower 9300 Series Threat appliance bundles

Part number (Appliance primary bundle)	Description
FPR9K-SM40-FTD-BUN	Cisco Firepower 9300 SM-40 FTD Bundle
FPR9K-SM48-FTD-BUN	Cisco Firepower 9300 SM-48 FTD Bundle
FPR9K-SM56-FTD-BUN	Cisco Firepower 9300 SM-56 FTD Bundle
Hardware accessories	
Please consult the ordering guide for accessories including rack mounts, spare fans, power supplies, and Solid-State Drives (SSDs)	

Table 5. Cisco Firepower 2100 series Fail-to-Wire (FTW) network modules

Part number	Product description
FPR2K-NM-6X10LR-F	Cisco Firepower 6-port 10G LR FTW Network Module
FPR2K-NM-6X10LR-F=	Cisco Firepower 6-port 10G LR FTW Network Module (Spare)
FPR2K-NM-6X10SR-F	Cisco Firepower 6-port 10G SR FTW Network Module

Part number	Product description
FPR2K-NM-6X10SR-F=	Cisco Firepower 6-port 10G SR FTW Network Module (Spare)
FPR2K-NM-6X1SX-F	Cisco Firepower 6-port 1G SX Fiber FTW Network Module
FPR2K-NM-6X1SX-F=	Cisco Firepower 6-port 1G SX Fiber FTW Network Module (Spare)
FPR2K-NM-8X1G-F	Cisco Firepower 8-port 1G Copper FTW Network Module
FPR2K-NM-8X1G-F=	Cisco Firepower 8-port 1G Copper FTW Network Module (Spare)

Table 6. Cisco Firepower 4100 series Fail-to-Wire (FTW) network modules

Part Number	Product Description
FPR4K-NM-2X40G-F	Cisco Firepower 2-port 40G SR FTW Network Module
FPR4K-NM-2X40G-F=	Cisco Firepower 2-port 40G SR FTW Network Module (Spare)
FPR4K-NM-6X10LR-F	Cisco Firepower 6-port 10G LR FTW Network Module
FPR4K-NM-6X10LR-F=	Cisco Firepower 6-port 10G LR FTW Network Module (Spare)
FPR4K-NM-6X10SR-F	Cisco Firepower 6-port 10G SR FTW Network Module
FPR4K-NM-6X10SR-F=	Cisco Firepower 6-port 10G SR FTW Network Module (Spare)
FPR4K-NM-6X1SX-F	Cisco Firepower 6-port 1G SX Fiber FTW Network Module
FPR4K-NM-6X1SX-F=	Cisco Firepower 6-port 1G SX Fiber FTW Network Module (Spare)
FPR4K-NM-8X1G-F	Cisco Firepower 8-port 1G Copper FTW Network Module
FPR4K-NM-8X1G-F=	Cisco Firepower 8-port 1G Copper FTW Network Module (Spare)

Table 7. Cisco Firepower 9300 series Fail-to-Wire (FTW) network modules

Part Number	Product Description
FPR9K-NM-2X40G-F	Cisco Firepower 2-port 40G SR FTW Network Module
FPR9K-NM-2X40G-F=	Cisco Firepower 2-port 40G SR FTW Network Module (Spare)
FPR9K-NM-6X10LR-F	Cisco Firepower 6-port 10G LR FTW Network Module
FPR9K-NM-6X10LR-F=	Cisco Firepower 6-port 10G LR FTW Network Module (Spare)
FPR9K-NM-6X10SR-F	Cisco Firepower 6-port 10G SR FTW Network Module
FPR9K-NM-6X10SR-F=	Cisco Firepower 6-port 10G SR FTW Network Module (Spare)
FPR9K-NM-6X1SX-F	Cisco Firepower 6-port 1G SX Fiber FTW Network Module
FPR9K-NM-6X1SX-F=	Cisco Firepower 6-port 1G SX Fiber FTW Network Module (Spare)

Warranty information

All Cisco hardware and software products are covered by warranty for a minimum of 90 days. Some products have longer warranties. For additional information on product warranty for the Firepower NGIPS product, please visit https://www.cisco.com/c/en/us/products/warranty-listing.html.

Cisco and partner services for Cisco Firepower NGIPS

Cisco offers a wide range of service programs to help customers succeed. 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 our services for Cisco Firepower NGIPS, 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.

Custom call to action

Next steps

To learn more about Cisco Firepower NGIPS threat appliances, please visit https://www.cisco.com/go/ngips.

To learn more about Cisco Advanced Malware Protection, please visit https://www.cisco.com/go/amp.

To learn more about Cisco's Talos Security Intelligence and Research Group, please visit https://www.talosintelligence.com/.

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

C78-742472-00 06/19