

# Cisco Firepower



**Team Swords**  
**CIS 8080**



# Table of Contents

About.....	2
Purpose.....	2
Features.....	3
System Requirements.....	5
How do we fare against the competition?.....	6
Compliance with ISO Standards.....	8
ISO 20005.....	8
ISO 27006.....	11
ISO 27002.....	14

---

**Fun Fact: Cisco NGFW was the winner of the 2017 Global Frost & Sullivan Award for Market Leadership for capturing the top spot on the firewall market leader board**

---



## About

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.

## Purpose

**Stop more threats** - Contain known and unknown malware with leading Cisco® Advanced Malware Protection (AMP) and sandboxing.



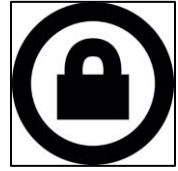
**Gain more insight** - Gain superior visibility into your environment with CiscoFirepower next-gen IPS. Automated risk rankings and impact flags identify priorities for your team.



**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.



## Target Customers

Enterprise companies seeking a comprehensive firewall solution will find Cisco Firepower to be the perfect product for their needs.

## Features

**Multi-Service Security Platform** - Multiple Cisco Security services in one box

**A Threat Focused Approach** - Access controls will not save you, threat focused approach will secure your systems. Identify assets and possible threats to those assets before placing access controls.

**A Correlated View** - Network to Endpoint - Automatically identifies correlation between network events and endpoint events.

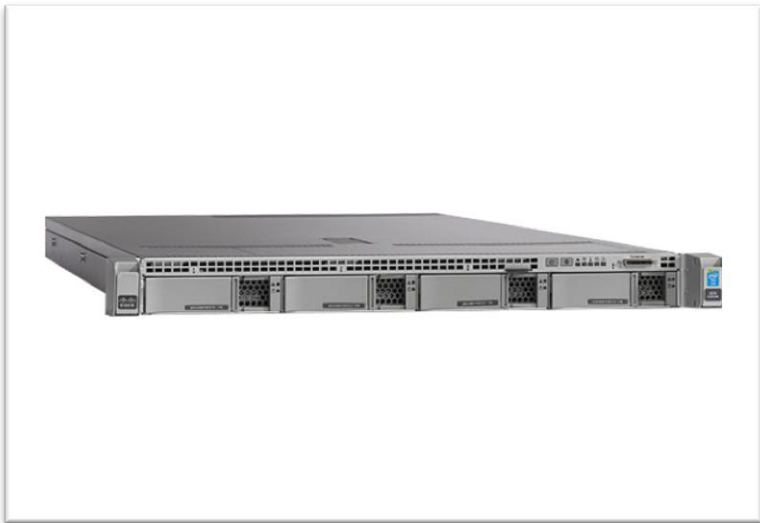
**Value Across The Entire Attack Continuum** - Before, during, and after. Set up policies and access controls in case of malware so that fail safes are in place (nothing is 100%), correct your own mistakes by tweaking access controls and policies proactively.

**A Unified, Single Management Interface** - Single interface and code for management of firewall or IPS or both.

**Integration with Existing Security Systems** - Share contextual data, event data and security intelligence not only with other Cisco systems but also 3rd party systems. Integrates with all databases in the security ecosystem. Block something at one place and it is blocked through the ecosystem.

## System Requirements

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)



*Pictured above is the Cisco Firepower Management Center*

# How do we fare against the competition?

	Cisco	Palo Alto Networks	Fortinet	Check Point Software Technologies
Close all				
^ Security Features				
Continuous analysis and retrospective detection	✓	Limited	Limited	Limited
Network file trajectory	Continuous	✗	✗	✗
Impact assessment	✓	Limited	Limited	Limited
Security automation and adaptive threat management	✓	Limited	Limited	Limited
Behavioral indicators of compromise (IoCs)	✓	Limited	Limited	Limited
User, network, and endpoint awareness	✓	Limited	Limited	Limited
NGIPS	Next-gen	Signature-based	Signature-based	Signature-based
Integrated advanced threat protection	✓	Limited	Limited	Limited
Malware remediation	✓	Limited	Limited	Limited

Fun Fact: Cisco NGFW won the **Best of Interop 2016 Award for Security**. The Best of Interop Awards recognize exhibitors that have made significant technological advancements in specific areas.

	Cisco	Palo Alto Networks	Fortinet	Check Point Software Technologies
^ Threat Intelligence (Talos)				
Unique malware samples per day	1.5 million	10s of thousands	10s of thousands	10s of thousands
Threats blocked per day	19.7 billion*	Not reported	Not reported	Not reported
Email messages scanned per day	600 billion	Not reported	6 million	Not reported
Web requests monitored per day	16 billion	Not reported	35 million	Not reported
Automated intelligence feeds	✓	✓	✓	✓
	Cisco	Palo Alto Networks	Fortinet	Check Point Software Technologies
^ Operational Capabilities				
Scanning architecture	OptiFlow™	Single pass	ASIC	Multipass
Software-defined segmentation	✓	✗	✗	✗
Automatic threat containment	✓	✗	✗	✗
Operations and management	Excellent	Limited	Limited	Excellent
Deployment models	Typical	Typical	Typical	Typical
eStreamer API	✓	✗	✗	✗
Remediation API	✓	✗	✗	✗
Host API	✓	✗	✗	✗



	Cisco	Palo Alto Networks	Fortinet	Check Point Software Technologies
^ Critical Infrastructure (ICS/SCADA)				
✓ Hardened and ruggedized versions available	✓	✗	✓	✓
✓ Base feature set	NGFW, AMP, NGIPS, threat intelligence	NGFW only	NGFW only	NGFW only
✓ SCADA rules	~250	~100	~300	~180
✓ Modbus, DNP, CIP pre-processors	✓	✓	✓	✓
^ Service Provider				
✓ Carrier-class certification	✓	✗	✓	✓
✓ Carrier-class features	✓	✗	✓	✓
✓ Third-party services stitching	✓	✗	✗	✗
✓ True DDoS	✓	✗	Limited	Limited

## Compliance with ISO Standards

### 27005 - Information Security Risk Management

#### 1. How well does this product deliver business value to its customer?

The Firepower is an integrated platform, with firewall, NGIPS, AMP, URL Filtering, and behavioral DDoS mitigation capability. Cisco Firepower NGFW blocks more threats, and it contains those threats that get in faster.

- Provides a next-generation intrusion prevention system (NGIPS) to deliver industry-leading threat protection
- Includes a fully integrated advanced malware protection (AMP) solution that addresses both known and unknown threats, along with an integrated sandbox
- Gives you the ability to track and contain malware infections
  - Automatically correlates threat events with your network's vulnerabilities so you can focus your resources on the threats that matter most
- Analyzes your network's weaknesses and recommends the best security policies to put in place
- Integrates with a number of Cisco® network security products to take advantage of your previous investments and provide stronger security

Reference:

<https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/datasheet-c78-736661.html>






## 2. What kinds of organizations are vulnerable to these risks?

SMBs, service providers, enterprise Internet edge, distributed enterprise/branch office deployments, industrial control environments, campus, data centers (traditional and micro-segmented), and carrier security gateway and Gi/SGi firewalling.

Reference:

<https://www.esecurityplanet.com/products/cisco-firepower-ngfw.html>

### 3. How effective is the product in its treatment of these risks?

	Stop more threats	Contain known and unknown malware with leading Cisco <sup>®</sup> 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.

Reference:

<https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/datasheet-c78-736661.html>

### 4. How difficult is it to acquire? What is the installation and training burden?

We provide installation instructions of all Firepower series in 3 languages(English, Korean, Chinese). We will send out our Firepower specialist to support your network team.

Reference:

<https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html>

### 5. Does the product enable monitoring and review of its effectiveness?

Yes. We provide management console to generate reports and dashboards to visualize the network activities.



*Sample dashboard pictured above*

Reference:

<https://www.cisco.com/c/en/us/products/security/firewalls/index.html>

## 27006 - Requirements for bodies providing audit and certification of information security management systems

6. Does the operation of this product require new/additional competencies in the organization or its auditors?

The addition of Firepower would require the auditors to consider the complexity of the system to the site as stated under 9.1.5.1.2 b) 5).

Under section 9.1.6.2 - the ISMS audit team will need to determine if the audit reporting provided by the Firepower Management Center is in compliance with the audit standards such that the ISMS audit team may use the results provided by the management center for sampling purposes.

Under section 9.3.1.2.2 – the ISMS audit team will need to evaluate the effectiveness of Firepower for information security performance against the information security objectives.

Under section 7.1.2 & A.3.1 Typical knowledge related to ISMS: with the addition of Firepower, the audit team should have knowledge and understanding of – management systems; information security; processes applicable to ISMS; communications security, including network security management and information transfer; information security incident management; regulation of cryptographic controls; electronic evidence collection.

Reference:

ISO/IEC 27006, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems. Third edition 2015-10-01.

## 7. Does the product support certification of its performance (or security/privacy performance)?

Yes, the Firepower Management Center supports compliance with security certification standards for:

- **Common Criteria (CC)** : a global standard established by the international Common Criteria Recognition Arrangement, defining properties for security products.”
  - **Unified Capabilities Approved Products List (UCAPL)** : a list of products meeting the security requirements established by the U.S. Defense Information Systems Agency (DISA).
  - **Federal Information Processing Standards (FIPS) 140** : a requirements specification for encryption modules.
- Some highlighted features are:

**Audit Logs** – Managed devices log read-only auditing information for user activity, allowing for the view, sort and filter of audit log messages based on any item in view; detailed reporting and audit log streaming.

**System Logs (syslog)** – Provides local system log information for the appliance and displays each message generated by the system.

**Custom HTTPS Certificates** – Secure Sockets Layer (SSL) certificates enable Firepower Management Centers to establish an encrypted channel between the system and a web browser.

Reference:

Firepower Management Center Configuration Guide,  
Version 6.2.2,  
[www.cisco.com/c/en/us/ed/docs/security/firepower/622](http://www.cisco.com/c/en/us/ed/docs/security/firepower/622),  
February 18, 2018.

## 27002 - Code of practice for information security management - Categories of information security and privacy controls

8. Does the product treat the best ISO/IEC 27002 categories of information security and privacy controls for the situation?

**a. Security Policy** - You can configure general security settings for the device using the General page and the Timeouts page under Platform > Security. You can enable anti-spoofing on interfaces, configure IP fragment settings, and configure a variety of timeout values for the device.

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/security\\_management/cisco\\_security\\_manager/security\\_manager/4-7/user/guide/CSMUserGuide/pxsecuritypolicies.pdf](https://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-7/user/guide/CSMUserGuide/pxsecuritypolicies.pdf)

**b. Organization of Information Security** - Cisco Firepower's Identity Technology associates users on your network with a realm and an authentication method to collect authoritative user data.

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60\\_chapter\\_01100000.pdf](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01100000.pdf)

**c. Human Resources Security** - The system automatically enables file event, malware event, and captured file

logging for active file policies. When a file policy generates a file or malware event, or captures a file, the system also automatically logs the end of the associated connection to the Firepower Management Center database.

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference\\_a\\_wrapper\\_Chapter\\_topic\\_here.pdf](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.pdf)

**d. Asset Management** - You can use Firepower intrusion rule recommendations to associate the operating systems, servers, and client application protocols detected on your network with rules specifically written to protect those assets. This allows you to tailor your intrusion policy to the specific needs of your monitored network.

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Tailoring\\_Intrusion\\_Protection\\_to\\_Your\\_Network\\_Assets.pdf](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Tailoring_Intrusion_Protection_to_Your_Network_Assets.pdf)

**e. Access Control** - An access control policy determines how the system handles traffic on your network. Each ASA FirePOWER module can have one currently applied policy.



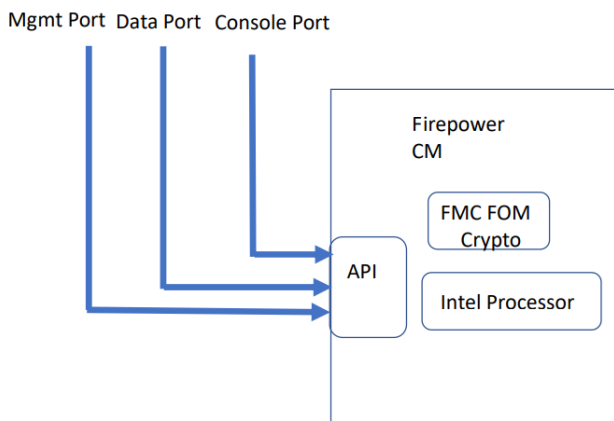
**Table 4-2 Access Control Policy Default Actions**

Default Action	Effect on Traffic	Inspection Type and Policy
Access Control: Block All Traffic	block without further inspection	none
Access Control: Trust All Traffic	trust (allow to its final destination without further inspection)	none
Intrusion Prevention	allow, as long as it is passed by the intrusion policy you specify (requires a Protection license)	intrusion, using the specified intrusion policy and associated variable set

**Reference:**

<https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/AC-Getting-Started.html>

**f. Cryptography** - The Firepower Cryptographic Module is defined as a multiple-chip standalone cryptographic module. Deployed inline, the system can affect the flow of traffic using access control, which allows the ability to specify, in a granular fashion, how to handle the traffic entering, exiting, and traversing a network. The data collected about network traffic and all information gleaned from it can be used to filter and control that traffic.



Reference:

<https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2960.pdf>

**g. Physical And Environmental Security** - Biometrics can be used to provide access to both hardware and software assets

**h. Operations security** - The system can generate logs of the connections its managed devices detect. These logs are called connection events. Settings in rules and policies give you granular control over which connections you log, when you log them, and where you store the data.

Reference:

[https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Connection\\_Logging.pdf](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Connection_Logging.pdf)

**i. Communications Security** - If the Firepower Management Center and its managed devices reside on the same network, you can connect the management interfaces on the devices to the same protected internal network as the Firepower Management Center. This allows you to securely control the devices from the Firepower Management Center. You can also configure multiple management interfaces to allow the Firepower Management Center to manage and isolate traffic from devices on other networks.

**Reference:**

[https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/security\\_internet\\_access\\_and\\_communication\\_ports.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/security_internet_access_and_communication_ports.html))

**j. Information Systems Acquisition, Development, Maintenance** - In maintenance mode, the system administratively takes down all interfaces except for the management interface. After maintenance is completed, you can re-enable the peer to resume normal operation. The Firepower System lets you allocate user privileges based on the user's role. You can also create custom user roles with access privileges tailored to your organization's needs.

**Reference:**

[https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower\\_System\\_User\\_Management.pdf](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Firepower_System_User_Management.pdf)

**k. Supplier Relationships** – See section j

**l. Information Security Incident management** - The FireSIGHT System includes features to support you as you collect and process information that is relevant to your investigation of an incident. You can use these features to gather intrusion events and packet data that may be related to the incident. You can also use the incident as a repository for notes about any activity that you take outside of the FireSIGHT System to mitigate the effects of the attack. For example, if your security policies

require that you quarantine compromised hosts from your network, you can note that in the incident.

Reference:

<https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/Incidents.html>

#### **m. Information Security Aspects of Business Continuity -**

Site-to-site and remote access VPN and advanced clustering provide highly secure, high-performance access and high availability to help ensure business continuity

Reference:

<https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733916.html>

**n. Compliance** - Cisco VMDC Cloud Security 1.0 offers a Unified Compliance Solution Framework with guidelines that facilitate addressing multiple regulatory compliance requirements from one network infrastructure

Reference:

[https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data\\_Center/VMDC/Cloud\\_Security/1-0/DG/ICSecurity/ICSecurity5.html](https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/Cloud_Security/1-0/DG/ICSecurity/ICSecurity5.html)

