The Cisco Firepower NGFW is unique in the industry because it is the only next-generation firewall that:

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

Cisco Firepower Management Center

FMC1000

Up to 50 sensors managed
30 million maximum events
900 GB event storage
Network map up to 50K hosts, 50K users



FMC2500

Up to 300 sensors managed
60 million maximum events
1.8 TB event storage
Network map up to 150K hosts, 150K users



FMC4500

Up to 750 sensors managed
300 million maximum events
3.2 TB event storage
Network map up to 600K hosts, 600K users

Virtual

Up to 25 sensors managed
10 million maximum events
250 GB event storage
Network map up to 50K hosts, 50K users

NGIPS features and benefits

Visibility

With Firepower Management Center, you can see more contextual data from your network and fine-tune your security. View applications, signs of compromise, host profiles, file trajectory, sandboxing, vulnerability information, and device-level OS visibility. Use these data inputs to optimize security through policy recommendations or Snort customizations.

Efficacy

NGIPS receives new policy rules and signatures every two hours, so your security is always up to date. Cisco Talos leverages the world’s largest threat detection network to bring security effectiveness to every Cisco security product. This industry-leading threat intelligence works as an early-warning system that constantly updates with new threats.

Operational cost

Use NGIPS automation to increase operational efficiency and reduce overhead by separating actionable events from noise. Prioritize threats for your staff and improve your security through policy recommendations based on network vulnerabilities. Stay informed on what rules to activate and deactivate, and filter events pertinent for the devices on your network.

Flexibility

Cisco Firepower NGIPS flexible deployment options meet the needs of the enterprise. It can be deployed at the perimeter, at the data center distribution/core, or behind the firewall to protect mission-critical assets, guest access, and WAN connections. NGIPS can be deployed for inline inspection or passive detection.

Integration

Firepower NGIPS plugs into your network without major hardware changes or significant time to implement. Enable and manage several security applications from a single pane with Firepower Management Center. Seamlessly navigate between NGIPS, NGFW, and AMP to optimize your security and ingest third-party data through Cisco Threat Intelligence Director.

High-performance appliances

Cisco Firepower (4100 Series and 9000 Series) and FirePOWER (7000 Series and 8000 Series) appliances are purpose-built to provide the right throughput, modular design, and carrier-class scalability. They incorporate a low-latency, single-pass design and include fail-to-wire interfaces.

Firepower 4100 Series

* Designed for Internet-edge, high-performance environments
* Threat inspection from 10 to 20 Gbps
* Includes AVC, with AMP and URL options
* Fail-to-wire interfaces available



FirePOWER 7000 Series

* Designed for sales and remote offices
* Threat inspection from 50 Mbps to 1.25 Gbps
* 8-12 monitoring interfaces
* Small Form-Factor Pluggable (SFP): 2 models



Firepower 9000 Series

* Designed for service provider and data center deployments
* Threat inspection up to 90 Gbps
* Includes AVC, with AMP and URL options
* Fail-to-wire interfaces available

NGIPSv for VMware

* Small branch offices and remote locations
* Threat inspection up to 800 Mbps
* East-west data center/PCI critical servers
* Full NGIPS and options functionality



FirePOWER 8000 Series

* Designed for campus and enterprise deployments
* Threat inspection up to 60 Gbps
* Stackable scalability
* Fail-to-wire interfaces available