Cisco Firepower Next-Generation Firewall (NGFW)

Prevent breaches, get deep visibility to detect and stop threats fast, and automate your network and security operations to save time and work smarter.

| Prevent breaches | Need to prevent breaches automatically to keep your business moving forward? Talos, our team of 250+ threat researchers, analyze millions of threats daily and create security protections that the Cisco NGFW uses to protect you against the next big breach. WannaCry? NotPetya? VPNFilter? Talos stopped these mega-breaches (and others) before they hit, and Cisco firewall customers were automatically protected. Not a bad track record. |
| See more to detect and stop threats fast | Worried that your firewall isn’t showing you the full picture? Cisco NGFWs go beyond prevention and access control to give you deep visibility to see and stop threats fast. Use built-in advanced security features like next-generation IPS, advanced malware protection, and sandboxing to see across users, hosts, networks and infrastructure. They continuously monitor for suspicious activity and automatically stop it the instant it is seen. Our advanced security capabilities help you see more so you can stop more. |
| Automate to save time and work smart | Are your products working you instead of working for you? Cisco NGFW automates your networking and security operations to save you time and reduce complexity so you can focus on high priority tasks. Threat alerts are prioritized so you can stop playing whack-a-mole and focus on what matters most. Cisco NGFWs work together with the rest of Cisco’s integrated security tools to give you visibility across multiple attack vectors, from edge to endpoint. When this system of tools sees a threat in one place, it will automatically be blocked everywhere. |

Model Overview

Cisco Firepower 2100 Series

The industry’s first midrange NGFWs delivering sustainable performance when threat inspection is enabled

Cisco Firepower 4100 Series:
The industry’s first 1RU NGFWs with 40-Gbps interfaces

Cisco Firepower 9300:
Ultra-high-performance NGFW, expandable as your needs grow
Cisco ASA 5500-X Series:
Models for branch offices, industrial applications, and the Internet edge

Firepower NGFW:
The NGFW for virtual and cloud environments

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 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.

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 (formerly FireSIGHT) 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 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.
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.

Cisco Firepower 2100 Series Appliances
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.

Cisco Firepower 4100 Series Appliances
The Cisco Firepower 4100 Series is a family of four threat-focused NGFW security platforms. Their throughput range addresses data center and internet edge use cases. They deliver superior threat defense, at faster speeds, with a smaller footprint. Cisco Firepower 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 Firepower 4120 platform.

Cisco Firepower 9300 Security Appliance
The Cisco Firepower 9300 is a scalable (beyond 1 Tbps when clustered), carrier-grade, modular platform designed for service providers, high-performance computing centers, large 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.

Cisco ASA 5500-FTD-X Series Appliances
The Cisco ASA 5500-FTD-X Series is a family of eight threat-focused NGFW security platforms. Their throughput range addresses use cases from the small or branch office to the Internet edge. They deliver superior threat defense in a cost-effective footprint.

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.
Performance Testing Methodologies
Cisco uses a variety of testing methodologies in a lab environment to ensure the performance specifications we report are as close to real world as possible. Firewall performance is affected by many factors including network environment, packet sizes, packet type, TLS encryption, and more.

Two modes of firewall testing exist: static or real world. Static testing leverages performance and security testing tools in a simulated environment. Real-world testing uses samples of live traffic on a production or side-car network. While static testing does not completely mimic performance in a real-world networking environment, we review and modify the static methodology to ensure the results are as close to real-world as possible.

The following are test methodologies used for measurements listed in Table 1. Change in performance vs change in packet size is not linear, so extrapolation from a single test is not possible for the almost unlimited variety of network environments. Testing security efficacy or security service performance under loaded conditions adds even more complexity. For these reasons we rely on the 1024B HTTP Test.

1024B HTTP Test (256KB Object)
This number is to compare with other vendors at a 256KB object size. It uses a larger and commonly tested packet size for every simulated session. With the protocol overhead, the average frame size is around 1024 bytes. This represents typical production conditions for most firewall deployments.

1500B UDP vs 64B UDP
This test uses a transactional UDP profile with either 1500B or 64B frames. Due to the stateless nature of UDP, it creates very little impact on a stateful NGFW. Many vendors use this profile to measure maximum firewall performance, however it is only practical as a comparison point. This test does not represent real-world conditions, therefore Cisco only uses it as a legacy metric for ASA performance. For NGFW products, various UDP packet size should only be used to test latency and not overall performance.

Performance Specifications and Feature Highlights
Table 1 summarizes the capabilities of the Cisco Firepower NGFWv, Firepower 2100 Series, and 4100 Series and 9300 appliances as well as the Cisco ASA 5500-FTD-X appliances when running the Cisco Firepower Threat Defense image. All numbers are derived with two-way traffic evaluation to replicate the best security posture.

<table>
<thead>
<tr>
<th>Features</th>
<th>Cisco Firepower Model</th>
<th>Cisco ASA 5500-FTD-X Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NGFWv</td>
<td>2110</td>
</tr>
<tr>
<td>Throughput: FW + AVC 1024B</td>
<td>1.9 Gbps</td>
<td>2.0 Gbps</td>
</tr>
<tr>
<td>Throughput: FW + AVC + IPS 1024B</td>
<td>1.9 Gbps</td>
<td>2.0 Gbps</td>
</tr>
</tbody>
</table>

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.
<table>
<thead>
<tr>
<th>Features</th>
<th>Cisco Firepower Model</th>
<th>Cisco ASA 5500-FTD-X Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MSP/PS</td>
<td>20/10</td>
</tr>
<tr>
<td>Maximum concurrent sessions, with AVC</td>
<td>100K</td>
<td>1M</td>
</tr>
<tr>
<td>Maximum new connections per second, with AVC</td>
<td>10K</td>
<td>12K</td>
</tr>
<tr>
<td>IPSec VPN Throughput (1524B TCP w/Fastpath)</td>
<td>-</td>
<td>750</td>
</tr>
<tr>
<td>Maximum VPN Peers</td>
<td>-</td>
<td>1500</td>
</tr>
<tr>
<td>Cisco Firepower Device Manager (local management)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Centralized management</td>
<td>Centralized configuration, logging, monitoring, and reporting are performed by the Management Center or alternatively in the cloud with Cisco Defense Orchestrator</td>
<td></td>
</tr>
<tr>
<td>Application Visibility and Control (AVC)</td>
<td>Standard, supporting more than 4000 applications, as well as geolocations, users, and websites</td>
<td></td>
</tr>
<tr>
<td>AVC: OpenAppID support for custom, open source, application detectors</td>
<td>Standard</td>
<td></td>
</tr>
<tr>
<td>Cisco Security Intelligence</td>
<td>Standard, with IP, URL, and DNS threat intelligence</td>
<td></td>
</tr>
<tr>
<td>Cisco Firepower NGIPS</td>
<td>Available; can passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence</td>
<td></td>
</tr>
<tr>
<td>Cisco AMP for Networks</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>Cisco AMP Threat Grid sandboxing</td>
<td>Available</td>
<td></td>
</tr>
<tr>
<td>URL Filtering: number of categories</td>
<td>More than 60</td>
<td></td>
</tr>
<tr>
<td>URL Filtering: number of URLs categorized</td>
<td>More than 280 million</td>
<td></td>
</tr>
</tbody>
</table>
Feed, and IPS Signature Updates

Third-party and open-source ecosystem

High availability and clustering

VLANs maximum

Cisco Trust Anchor Technologies

**Note:** Throughput assumes HTTP sessions.

Performance will vary depending on features activated, and network traffic protocol mix, packet size characteristics and hypervisor employed (NGFWv). Performance is subject to change with new software releases. Consult your Cisco representative for detailed sizing guidance.

Table 2 summarizes the performance and capabilities of the Cisco Firepower 2100, 4100 Series and 9300 appliances when running the ASA image. For Cisco ASA 5500-X Series performance specifications with the ASA image, please visit the [Cisco ASA with FirePOWER Services data sheet](#).

### Table 2. ASA Performance and Capabilities on Firepower Appliances

<table>
<thead>
<tr>
<th>Features</th>
<th>Cisco Firepower Appliance Model</th>
<th>Cisco ASA 5500-FTD-X Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2110</td>
<td>2120</td>
</tr>
<tr>
<td>Stateful inspection firewall throughput¹</td>
<td>3 Gbps</td>
<td>6 Gbps</td>
</tr>
<tr>
<td>Stateful inspection firewall throughput (multiprotocol)²</td>
<td>1.5 Gbps</td>
<td>3 Gbps</td>
</tr>
<tr>
<td>Concurrent firewall connections</td>
<td>1 million</td>
<td>1.5 million</td>
</tr>
<tr>
<td>Firewall latency (UDP 64B microsecond s)</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
### Table 3. Operating Requirements for Firepower NGFWv Virtual Appliances

<table>
<thead>
<tr>
<th>Features</th>
<th>Cisco Firepower Appliance Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2110</td>
</tr>
<tr>
<td>New connections per second</td>
<td>18000</td>
</tr>
<tr>
<td>IPsec VPN throughput (450B UDP L2L test)</td>
<td>500 Mbps</td>
</tr>
<tr>
<td>IPsec/Cisco AnyConnect/ Apex site-to-site VPN peers</td>
<td>1500</td>
</tr>
<tr>
<td>Maximum number of VLANs</td>
<td>400</td>
</tr>
<tr>
<td>High availability</td>
<td>Active/active and active/standby</td>
</tr>
<tr>
<td>Clustering</td>
<td>-</td>
</tr>
<tr>
<td>Scalability</td>
<td>VPN Load Balancing</td>
</tr>
<tr>
<td>Centralized management</td>
<td>Centralized configuration, logging, monitoring, and reporting are performed by Cisco Security Manager or alternatively in the cloud with Cisco Defense Orchestrator</td>
</tr>
<tr>
<td>Adaptive Security Device Manager</td>
<td>Web-based, local management for small-scale deployments</td>
</tr>
</tbody>
</table>

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.

### Platform Support

<table>
<thead>
<tr>
<th>VMware, KVM, AWS, Azure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum systems requirements: VMware</strong></td>
</tr>
<tr>
<td><strong>Minimum systems requirements: KVM</strong></td>
</tr>
<tr>
<td><strong>Supported AWS instances</strong></td>
</tr>
<tr>
<td><strong>Supported Azure instances</strong></td>
</tr>
<tr>
<td><strong>Management options</strong></td>
</tr>
</tbody>
</table>
## Hardware Specifications

Tables 4, 5, and 6 summarize the hardware specifications for the 2100 Series, 4100 Series, and 9300 Series, respectively. Table 7 summarizes regulatory standards compliance. For Cisco ASA 5500-X Series hardware specifications, please visit the [Cisco ASA with FirePOWER Services data sheet](#).

### Table 4. Cisco Firepower 2100 Series Hardware Specifications

<table>
<thead>
<tr>
<th>Features</th>
<th>Cisco Firepower Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2110</td>
</tr>
<tr>
<td></td>
<td>2120</td>
</tr>
<tr>
<td></td>
<td>2130</td>
</tr>
<tr>
<td></td>
<td>2140</td>
</tr>
<tr>
<td>Dimensions (H x W x D)</td>
<td>1.73 x 16.90 x 19.76 in. (4.4 x 42.9 x 50.2 cm)</td>
</tr>
<tr>
<td>Form factor (rack units)</td>
<td>1RU</td>
</tr>
<tr>
<td>Security module slots</td>
<td>-</td>
</tr>
<tr>
<td>I/O module slots</td>
<td>0</td>
</tr>
<tr>
<td>Integrated I/O</td>
<td>12 x 10M/100M/10BASE-T Ethernet interfaces (RJ-45), 4 x 1 Gigabit (SFP) Ethernet interfaces</td>
</tr>
<tr>
<td>Network modules</td>
<td>None</td>
</tr>
<tr>
<td>Integrated network management ports</td>
<td>1 x 10M/100M/10BASE-T Ethernet port (RJ-45)</td>
</tr>
<tr>
<td>Serial port</td>
<td>1 x RJ-45 console</td>
</tr>
<tr>
<td>USB</td>
<td>1 x USB 2.0 Type-A (500mA)</td>
</tr>
<tr>
<td>Storage</td>
<td>1x 100 GB, 1x spare slot (for MSP)</td>
</tr>
<tr>
<td></td>
<td>1x 100 GB, 1x spare slot (for MSP)</td>
</tr>
<tr>
<td></td>
<td>1x 200 GB, 1x spare slot (for MSP)</td>
</tr>
<tr>
<td></td>
<td>1x 200 GB, 1x spare slot (for MSP)</td>
</tr>
<tr>
<td>Power supplies</td>
<td>Configuration</td>
</tr>
<tr>
<td>AC input voltage</td>
<td>Single integrated 250W AC power supply.</td>
</tr>
<tr>
<td>AC maximum input current</td>
<td>Single 400W AC, Dual 400W AC optional Single/Dual 350W DC optional^1</td>
</tr>
<tr>
<td>AC maximum output power</td>
<td>Dual 400W AC, Single/Dual 350W DC optional^1</td>
</tr>
<tr>
<td>AC frequency</td>
<td>100 to 240V AC</td>
</tr>
<tr>
<td>DC input voltage</td>
<td>&lt; 2.7A at 100V</td>
</tr>
<tr>
<td>DC maximum input current</td>
<td>&lt; 6A at 100V</td>
</tr>
<tr>
<td>DC maximum output power</td>
<td>250W</td>
</tr>
<tr>
<td>DC efficiency</td>
<td>&gt;88% at 50% load</td>
</tr>
<tr>
<td>Redundancy</td>
<td>None</td>
</tr>
<tr>
<td>1+1 AC or DC with dual supplies</td>
<td></td>
</tr>
<tr>
<td>Fans</td>
<td>4 integrated (2 internal, 2 exhaust) fans^2</td>
</tr>
<tr>
<td>Noise</td>
<td>56 dBA @ 25C</td>
</tr>
<tr>
<td></td>
<td>74 dBA at highest system performance.</td>
</tr>
</tbody>
</table>

^1 AC power supply options depend on the model.

^2 Fans are hot-swappable, and the exhaust fans are equipped with a fan cage that supports up to two fans.

Note: The 2100 Series appliances may also be deployed as dedicated threat sensors with fail-to-wire network modules. Please contact your Cisco representative for details.
<table>
<thead>
<tr>
<th>Features</th>
<th>Cisco Firepower Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2110</td>
</tr>
<tr>
<td>Rack mountable</td>
<td>Yes, Fixed mount brackets included (2-post). Mount rails optional (4-post EIA-310-D rack)</td>
</tr>
<tr>
<td>Weight</td>
<td>16.1 lb (7.3 kg): with 2x SSDs</td>
</tr>
<tr>
<td>Temperature: operating</td>
<td>32 to 104°F (0 to 40°C)</td>
</tr>
<tr>
<td>Temperature: nonoperating</td>
<td>-4 to 149°F (-20 to 65°C)</td>
</tr>
<tr>
<td>Humidity: operating</td>
<td></td>
</tr>
<tr>
<td>Humidity: nonoperating</td>
<td></td>
</tr>
<tr>
<td>Altitude: operating</td>
<td>10,000 ft (max)</td>
</tr>
<tr>
<td>Altitude: nonoperating</td>
<td>40,000 ft (max)</td>
</tr>
<tr>
<td>NEBS operation (FPR-2130 Only)</td>
<td>Operating altitude: 0 to 13,000 ft (3962 m)</td>
</tr>
</tbody>
</table>

1 Dual power supplies are hot-swappable.
2 Fans operate in a 3+1 redundant configuration where the system will continue to function with only 3 operational fans. The 3 remaining fans will run at full speed.
3 FPR-2130 platform is designed to be NEBS ready. The availability of NEBS certification is pending.

Table 5. Cisco Firepower 4100 Series Hardware Specifications

<table>
<thead>
<tr>
<th>Features</th>
<th>Cisco Firepower Model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4110</td>
</tr>
<tr>
<td>Dimensions (H x W x D)</td>
<td>1.75 x 16.89 x 29.7 in. (4.4 x 42.9 x 75.4 cm)</td>
</tr>
<tr>
<td>Form factor (rack units)</td>
<td>1RU</td>
</tr>
<tr>
<td>Security module slots</td>
<td>-</td>
</tr>
<tr>
<td>I/O module slots</td>
<td>2</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Cisco Firepower 4000 Supervisor with 8 x 10 Gigabit Ethernet ports and 2 Network Module (NM) slots for I/O expansion</td>
</tr>
<tr>
<td>Network modules</td>
<td>- 8 x 10 Gigabit Ethernet Enhanced Small Form-Factor Pluggable (SFP+) network modules - 4 x 40 Gigabit Ethernet Quad SFP+ network modules - 8-port 1Gbps copper. FTW (fail to wire) Network Module</td>
</tr>
<tr>
<td>Note: Firepower 4100 Series appliances may also be deployed as dedicated threat sensors, with fail-to-wire network modules. Please contact your Cisco representative for details.</td>
<td></td>
</tr>
<tr>
<td>Maximum number of interfaces</td>
<td>Up to 24 x 10 Gigabit Ethernet (SFP+) interfaces; up to 8 x 40 Gigabit Ethernet (QSFP+) interfaces with 2 network modules</td>
</tr>
<tr>
<td>Integrated network management ports</td>
<td>1 x Gigabit Ethernet copper port</td>
</tr>
<tr>
<td>Serial port</td>
<td>1 x RJ-45 console</td>
</tr>
<tr>
<td>USB</td>
<td>1 x USB 2.0</td>
</tr>
<tr>
<td>Storage</td>
<td>200 GB</td>
</tr>
</tbody>
</table>
### FeaturesCisco Firepower Model

<table>
<thead>
<tr>
<th>Power supplies</th>
<th>4110</th>
<th>4120</th>
<th>4140</th>
<th>4150</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Single 1100W AC, dual optional. Single/dual 950W DC optional(^1)</td>
<td>Single 1100W AC, dual optional. Single/dual 950W DC optional(^1)</td>
<td>Dual 1100W AC(^1)</td>
<td>Dual 1100W AC(^1)</td>
</tr>
<tr>
<td>AC input voltage</td>
<td>100 to 240V AC</td>
<td>100 to 240V AC</td>
<td>100 to 240V AC</td>
<td>100 to 240V AC</td>
</tr>
<tr>
<td>AC maximum input current</td>
<td>13A</td>
<td>13A</td>
<td>13A</td>
<td>13A</td>
</tr>
<tr>
<td>AC maximum output power</td>
<td>1100W</td>
<td>1100W</td>
<td>1100W</td>
<td>1100W</td>
</tr>
<tr>
<td>AC frequency</td>
<td>50 to 60 Hz</td>
<td>50 to 60 Hz</td>
<td>50 to 60 Hz</td>
<td>50 to 60 Hz</td>
</tr>
<tr>
<td>AC efficiency</td>
<td>&gt;92% at 50% load</td>
<td>&gt;92% at 50% load</td>
<td>&gt;92% at 50% load</td>
<td>&gt;92% at 50% load</td>
</tr>
<tr>
<td>DC input voltage</td>
<td>-40V to -60VDC</td>
<td>-40V to -60VDC</td>
<td>-40V to -60VDC</td>
<td>-40V to -60VDC</td>
</tr>
<tr>
<td>DC maximum input current</td>
<td>27A</td>
<td>27A</td>
<td>27A</td>
<td>27A</td>
</tr>
<tr>
<td>DC maximum output power</td>
<td>950W</td>
<td>950W</td>
<td>950W</td>
<td>950W</td>
</tr>
<tr>
<td>DC efficiency</td>
<td>&gt;92.5% at 50% load</td>
<td>&gt;92.5% at 50% load</td>
<td>&gt;92.5% at 50% load</td>
<td>&gt;92.5% at 50% load</td>
</tr>
<tr>
<td>Redundancy</td>
<td>1+1</td>
<td>1+1</td>
<td>1+1</td>
<td>1+1</td>
</tr>
</tbody>
</table>

### Fans
6 hot-swappable fans

### Noise
78 dBA

### Rack mountable
Yes, mount rails included (4-post EIA-310-D rack)

### Weight
36 lb (16 kg): 2 x power supplies, 2 x NMs, 6x fans; 30 lb (13.6 kg): no power supplies, no NMs, no fans

### Temperature: operating
32 to 104°F (0 to 40°C)

### 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)

### Altitude: nonoperating
40,000 ft (max)

### NEBS operation (FPR 4120 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 6Cisco Firepower 9300 Hardware Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions (H x W x D)</td>
<td>5.25 x 17.5 x 32 in. (13.3 x 44.5 x 81.3 cm)</td>
</tr>
<tr>
<td>Form factor</td>
<td>3 Rack Units (3RU), fits standard 19-in. (48.3-cm) square-hole rack</td>
</tr>
<tr>
<td>Security module slots</td>
<td>3</td>
</tr>
<tr>
<td>Network module slots</td>
<td>2 (within supervisor)</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Cisco Firepower 9000 Supervisor with 8 x 10 Gigabit Ethernet ports and 2 network module slots for I/O expansion</td>
</tr>
</tbody>
</table>
| Security modules | ● Cisco Firepower 9000 Security Module 24 with 2 x SSDs in RAID-1 configuration  
● Cisco Firepower 9000 Security Module 36 with 2 x SSDs in RAID-1 configuration |
<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
</table>
| Network modules            | ● 8 x 10 Gigabit Ethernet Enhanced Small Form-Factor Pluggable (SFP+) network modules  
|                            | ● 4 x 40 Gigabit Ethernet Quad SFP+ network modules  
|                            | ● 2 x 100 Gigabit Ethernet Quad SFP28 network modules (double-wide, occupies both network module bays)  
| Note:                     | Firepower 9300 may also be deployed as a dedicated threat sensor, with fail-to-wire network modules. Please contact your Cisco representative for details. |
| Maximum number of interfaces | Up to 24 x 10 Gigabit Ethernet (SFP+) interfaces; up to 8 x 40 Gigabit Ethernet (QSFP+) interfaces with 2 network modules |
| Integrated network management ports | 1 x Gigabit Ethernet copper port (on supervisor) |
| Serial port                | 1 x RJ-45 console                                                                                                                                  |
| USB                        | 1 x USB 2.0                                                                                                                                         |
| Storage                    | Up to 2.4 TB per chassis (800 GB per security module in RAID-1 configuration)                                                                         |
| Power supplies             | **AC power supply**  
|                            | 200 to 240V AC  
|                            | -40V to -60V DC  
|                            | 240 to 380V DC  
|                            | **-48V DC power supply**  
|                            | 69A to 42A  
|                            | <14A at 200V  
|                            | **HVDC power supply**  
|                            | 2500W  
|                            | 2500W  
|                            | 2500W  
|                            | **Input voltage**  
|                            | 15.5A to 12.9A  
|                            | 50 to 60 Hz  
|                            | **Maximum output power**  
|                            | 92%  
|                            | 92%  
|                            | 92% (at 50% load)  
|                            | **Maximum input current**  
|                            | Efficiency (at 50% load)  
|                            | 1+1  
|                            | **Frequency**  
|                            | **Redundancy**  
|                            | 4 hot-swappable fans                                                                                                                                   |
| Noise                      | 75.5 dBA at maximum fan speed                                                                                                                           |
| Rack mountable             | Yes, mount rails included (4-post EIA-310-D rack)                                                                                                     |
| Weight                     | 105 lb (47.7 kg) with one security module; 135 lb (61.2 kg) fully configured                                                                             |
| Temperature: standard operating | Up to 10,000 ft (3000 M); 32 to 104°F (0 to 40°C) for SM-24 module  
|                            | 32 to 88°F (0 to 35°C) for SM-36 module at sea-level                                                                                                    |
| Temperature: NEBS operating |  
|                            | Altitude adjustment notes:  
|                            | For SM-36, maximum temp is 35°C, for every 1000 feet above sea level subtract 1° C                                                                     |
| Temperature: nonoperating |  
| Humidity: operating        | 5 to 95% noncondensing                                                                                                                                  |
| Humidity: nonoperating     | 5 to 95% noncondensing                                                                                                                                  |
| Altitude: operating        | SM-24: 0 to 13,000 ft (3962 m)  
|                            | SM-36: 0 to 10,000 ft (3048 m); please see above Operating Temperature section for temperature adjustment notes                                             |
| Altitude: nonoperating     | 40,000 ft (12,192 m)                                                                                                                                   |

* Minimum turn-on voltage is -44V DC
Table 7. Cisco Firepower 2100 Series, 4100 Series and Cisco Firepower 9300 NEBS, Regulatory, Safety, and EMC Compliance

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NEBS</strong></td>
<td>Cisco Firepower 9300 is NEBS compliant with SM-24 Security Modules. Cisco Firepower 4120 is NEBS compliant.</td>
</tr>
<tr>
<td><strong>Regulatory compliance</strong></td>
<td>Products comply with CE markings per directives 2004/108/EC and 2006/108/EC</td>
</tr>
</tbody>
</table>
| **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  
                 ● TCVN 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  
                 ● EN-61000-4-11 |

**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**

Firepower DDoS Mitigation is provided by Radware Virtual DefensePro (vDP), available and supported directly from Cisco on the following Cisco Firepower 9300 and 4100 series appliances:

<table>
<thead>
<tr>
<th>Cisco Firepower Model</th>
<th>ASA Image</th>
<th>FTD Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>9300 – SM-44</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>9300 – SM-36</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>9300 – SM-24</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>4150</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>4140</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>4120</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>4110</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

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 Table 8 apply to all Cisco Firepower 4100 series models.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum mitigation capacity/throughput</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>Maximum legitimate concurrent sessions</td>
<td>209,000 Connections Per Second (CPS)</td>
</tr>
<tr>
<td>Maximum DDoS flood attack prevention rate</td>
<td>1,800,000 Packets Per Second (PPS)</td>
</tr>
</tbody>
</table>

The performance figures in Table 9 are for Cisco Firepower 9300 with 1 to 3 Security Modules irrespective of Security Module type (SM-24, SM-36 or SM-44).
Table 9. Key DDoS Performance Metrics for Cisco Firepower 9300 with 1, 2, or 3 Security Modules.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Firepower 9300 with 1 Security Module</th>
<th>Firepower 9300 with 2 Security Modules</th>
<th>Firepower 9300 with 3 Security Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum mitigation capacity/throughput</td>
<td>10 Gbps</td>
<td>20 Gbps</td>
<td>30 Gbps</td>
</tr>
<tr>
<td>Maximum legitimate concurrent sessions</td>
<td>209,000 Connections Per Second (CPS)</td>
<td>418,000 Connections Per Second (CPS)</td>
<td>627,000 Connections Per Second (CPS)</td>
</tr>
<tr>
<td>Maximum DDoS flood attack prevention rate</td>
<td>1,800,000 Packets Per Second (PPS)</td>
<td>3,600,000 Packets Per Second (PPS)</td>
<td>5,400,000 Packets Per Second (PPS)</td>
</tr>
</tbody>
</table>

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](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](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](https://www.cisco.com/c/en/us/services/portfolio/product-technical-support/smart-net-total-care.html).
Select Part Numbers

Tables 10, 11, and 12 provide details on part numbers for Cisco Firepower NGFW solutions. Please consult the Ordering Guide for additional configuration options and accessories.

Table 10. Cisco Firepower 2100 Series: Select Product Components

<table>
<thead>
<tr>
<th>Part Number (Appliance Master Bundle)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPR2110-BUN</td>
<td>Cisco Firepower 2110 Master Bundle</td>
</tr>
<tr>
<td>FPR2120-BUN</td>
<td>Cisco Firepower 2120 Master Bundle</td>
</tr>
<tr>
<td>FPR2130-BUN</td>
<td>Cisco Firepower 2130 Master Bundle</td>
</tr>
<tr>
<td>FPR2140-BUN</td>
<td>Cisco Firepower 2140 Master Bundle</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part Number (Network Module)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPR2K-NM-8X10G</td>
<td>Spare Cisco Firepower 8-port SFP+ network module</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part Number (Appliances with FTD software)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPR2110-NGFW-K9</td>
<td>Cisco Firepower 2110 NGFW Appliance, 1RU</td>
</tr>
<tr>
<td>FPR2120-NGFW-K9</td>
<td>Cisco Firepower 2120 NGFW Appliance, 1RU</td>
</tr>
<tr>
<td>FPR2130-NGFW-K9</td>
<td>Cisco Firepower 2130 NGFW Appliance, 1RU, 1 x Network Module Bays</td>
</tr>
<tr>
<td>FPR2140-NGFW-K9</td>
<td>Cisco Firepower 2140 NGFW Appliance, 1RU, 1 x Network Module Bays</td>
</tr>
</tbody>
</table>

Cisco Firepower 2100 Series NGFW Select Licenses

<table>
<thead>
<tr>
<th>License Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L-FPR2110T-TMC=</td>
<td>Cisco Firepower 2110 Threat Defense Threat, Malware, and URL License</td>
</tr>
<tr>
<td>L-FPR2120T-TMC=</td>
<td>Cisco Firepower 2120 Threat Defense Threat, Malware, and URL License</td>
</tr>
<tr>
<td>L-FPR2130T-TMC=</td>
<td>Cisco Firepower 2130 Threat Defense Threat, Malware, and URL License</td>
</tr>
<tr>
<td>L-FPR2140T-TMC=</td>
<td>Cisco Firepower 2140 Threat Defense Threat, Malware, and URL License</td>
</tr>
</tbody>
</table>

Note: These optional security services licenses can be ordered with 1-, 3-, or 5-year subscriptions.

<table>
<thead>
<tr>
<th>Part Number (Appliances with ASA Software)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPR2110-ASA-K9</td>
<td>Cisco Firepower 2110 ASA Appliance, 1RU</td>
</tr>
<tr>
<td>FPR2120-ASA-K9</td>
<td>Cisco Firepower 2120 ASA Appliance, 1RU</td>
</tr>
<tr>
<td>FPR2130-ASA-K9</td>
<td>Cisco Firepower 2130 ASA Appliance, 1RU, 1 x Network Module Bays</td>
</tr>
<tr>
<td>FPR2140-ASA-K9</td>
<td>Cisco Firepower 2140 ASA Appliance, 1RU, 1 x Network Module Bays</td>
</tr>
</tbody>
</table>

Optional ASA Software Licenses

<table>
<thead>
<tr>
<th>License Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L-FPR2K-ENC-K9=</td>
<td>License to enable strong encryption for ASA on Cisco Firepower 2100 Series</td>
</tr>
<tr>
<td>L-FPR2K-ASASC-10=</td>
<td>Cisco Firepower 2100 Add-on 10 security context licenses</td>
</tr>
<tr>
<td>L-FPR2K-ASASC-5=</td>
<td>Cisco Firepower 2100 Add-on 5 security context licenses</td>
</tr>
</tbody>
</table>

Hardware Accessories

Please consult the ordering guide for accessories including rack mounts, spare fans, power supplies, and Solid-State Drives (SSDs)
### Table 11. Cisco Firepower 4100 Series: Select Product Components

<table>
<thead>
<tr>
<th>Part Number (Appliance Master Bundle)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPR4110-BUN</td>
<td>Cisco Firepower 4110 Master Bundle, for ASA or Cisco Firepower Threat Defense Image</td>
</tr>
<tr>
<td>FPR4120-BUN</td>
<td>Cisco Firepower 4120 Master Bundle, for ASA or Cisco Firepower Threat Defense Image</td>
</tr>
<tr>
<td>FPR4140-BUN</td>
<td>Cisco Firepower 4140 Master Bundle, for ASA or Cisco Firepower Threat Defense Image</td>
</tr>
<tr>
<td>FPR4150-BUN</td>
<td>Cisco Firepower 4150 Master Bundle, for ASA or Cisco Firepower Threat Defense Image</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part Number (Spare Network Module)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPR4K-NM-8X10G=</td>
<td>Spare Cisco Firepower 8-port SFP+ network module</td>
</tr>
<tr>
<td>FPR4K-NM-4X40G=</td>
<td>Spare Cisco Firepower 4-port QSFP+ network module</td>
</tr>
</tbody>
</table>

**Hardware Accessories**

Please consult the ordering guide for accessories including rack mounts, spare fans, power supplies, and Solid-State Drives (SSDs).

**Optional ASA Software Licenses**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L-F4K-ASA-CAR</td>
</tr>
<tr>
<td>L-FPR4K-ENC R-K9</td>
</tr>
<tr>
<td>L-FPR4K-ASASC-10</td>
</tr>
</tbody>
</table>

### Table 12. Cisco Firepower 9300: Select Product Components

<table>
<thead>
<tr>
<th>Part Number (Chassis)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPR-C9300-AC</td>
<td>Cisco Firepower 9300 AC Chassis - includes 2 power supply units + 4 fans + rack-mount kit (3RU; accommodates up to three security modules)</td>
</tr>
<tr>
<td>FPR-C9300-DC</td>
<td>Cisco Firepower 9300 DC Chassis - includes 2 power supply units + 4 fans + rack-mount kit (3RU; accommodates up to three security modules)</td>
</tr>
<tr>
<td>FPR-C9300-HVDC</td>
<td>Cisco Firepower 9300 high-voltage DC Chassis - includes 2 power supply units + 4 fans + rack-mount kit (3RU; accommodates up to three security modules)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part Number (Security Module)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPR9K-SM-24</td>
<td>24 Physical Core Security Module (NEBS Ready)</td>
</tr>
<tr>
<td>FPR9K-SM-36</td>
<td>36 Physical Core Security Module</td>
</tr>
<tr>
<td>FPR9K-SM-44</td>
<td>44 Physical Core Security Module</td>
</tr>
</tbody>
</table>

**ASA Software Licenses for Cisco Firepower 9300**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L-F9K-ASA-CAR</td>
</tr>
<tr>
<td>L-F9K-ASA-CAR=</td>
</tr>
<tr>
<td>L-F9K-ASA-SC-10</td>
</tr>
<tr>
<td>L-F9K-ASA-SC-10=</td>
</tr>
<tr>
<td>L-F9K-ASA</td>
</tr>
<tr>
<td>L-F9K-ASA=</td>
</tr>
<tr>
<td>L-F9K-ASA-ENC R-K9</td>
</tr>
</tbody>
</table>
Cisco Firepower 9300 NGFW Threat Defense Software Licenses

<table>
<thead>
<tr>
<th>Description</th>
<th>Part Number (Virtual Appliance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Firepower Threat Defense Base License for Cisco Firepower 9300 NGFW</td>
<td>FPR9K-TD-BASE</td>
</tr>
<tr>
<td>Cisco Firepower 9000 SM-24 Threat Defense Threat, Malware, and URL License</td>
<td>L-FPR9K-SM24-TMC</td>
</tr>
<tr>
<td>Cisco Firepower 9000 SM-24 Threat Defense Threat, Malware, and URL 3Yr Svcs</td>
<td>L-FPR9K-SM24-TMC-3Y</td>
</tr>
<tr>
<td>Cisco Firepower 9000 SM-36 Threat Defense Threat, Malware, and URL License</td>
<td>L-FPR9K-SM36-TMC</td>
</tr>
<tr>
<td>Cisco Firepower 9000 SM-36 Threat Defense Threat, Malware, and URL 3Yr Svcs</td>
<td>L-FPR9K-SM36-TMC-3Y</td>
</tr>
<tr>
<td>Cisco Firepower 9000 SM-44 Threat Defense Threat, Malware, and URL License</td>
<td>L-FPR9K-SM44-TMC</td>
</tr>
<tr>
<td>Cisco Firepower 9000 SM-44 Threat Defense Threat, Malware, and URL 3Yr Svcs</td>
<td>L-FPR9K-SM44-TMC-3Y</td>
</tr>
</tbody>
</table>

Note: Firepower 9300 may also be deployed as a dedicated threat sensor, with fail-to-wire network modules. Please contact your Cisco representative for details.

Table 13. Cisco Firepower NGFW Virtual

<table>
<thead>
<tr>
<th>Part Number (Virtual Appliance)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPR9K-TD-V9</td>
<td>Cisco Firepower NGFWv Base License</td>
</tr>
<tr>
<td>L-FPR9K-TD-V9=</td>
<td>Cisco Firepower NGFWv Threat Defense Threat Protection License</td>
</tr>
<tr>
<td>L-FPR9K-TD-V9=</td>
<td>Cisco Firepower NGFWv Threat Defense Threat and Malware Protection License</td>
</tr>
<tr>
<td>L-FPR9K-TD-V9=</td>
<td>Cisco Firepower NGFWv Threat Defense Threat and URL License</td>
</tr>
<tr>
<td>L-FPR9K-TD-V9=</td>
<td>Cisco Firepower NGFWv Threat Defense Threat, Malware, and URL License</td>
</tr>
</tbody>
</table>

Note: These optional security services licenses can be ordered with 1-, 3-, or 5-year subscriptions.

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:

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