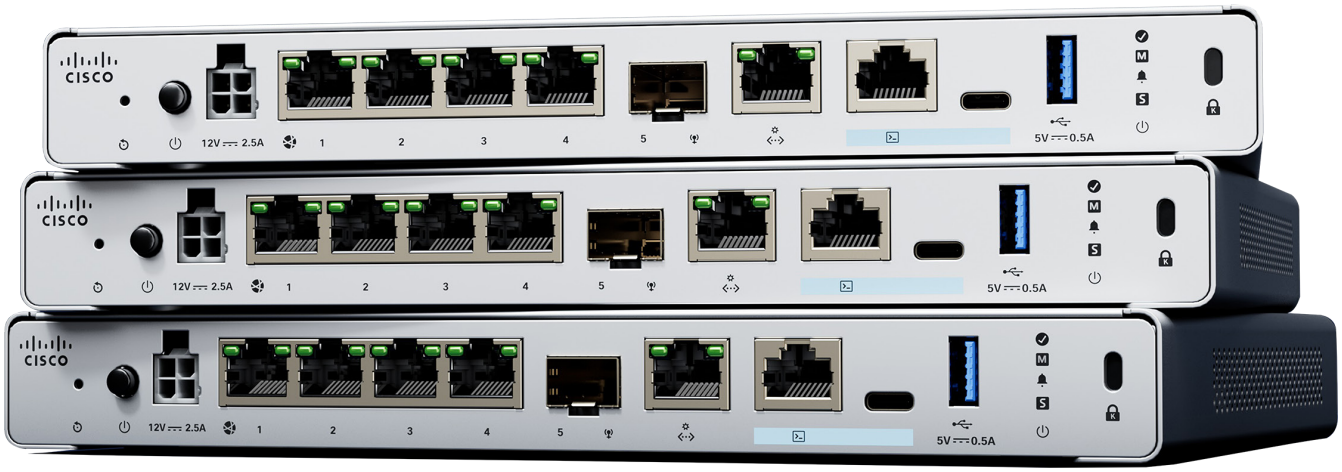
Cisco Secure Firewall 220

200 Series



Contents

Introduction

The Cisco® Secure Firewall 200 Series offers next-generation firewall capabilities specifically designed for distributed enterprises and small branch locations. It provides robust, cost-effective security and simplified management within a compact form factor, ensuring secure and optimized connectivity at the network edge. The 200 Series extends Cisco's Hybrid Mesh Firewall architecture to branch edges, providing AI-powered inspection and consistent security policies. It integrates SD-WAN capabilities for enhanced application performance and reliable user access. Additionally, the 200 Series delivers application and user control, efficient segmentation, and advanced security features tailored for cost-sensitive environments. Cisco Secure Firewall 220 is the first model in the 200 series.

Table 1. Key capabilities of the Cisco Secure Firewall 220

Cisco Secure Firewall 220 with Cisco Firewall Threat Defense Software	
Robust connectivity • Achieve up to 1.5 Gbps throughput from a fanless desktop firewall when next-generation firewall capabilities are enabled. Enable the high-availability feature for continuous uptime. • Connect branch offices to the hybrid mesh firewall architecture using the 1G Small Form-factor Pluggable (SFP) port. Network and cryptographic operations are accelerated inline by leveraging the System on a Chip (SoC).	**Superior visibility** • Leverage the AI-powered Encrypted Visibility Engine (EVE) to gain insights into and control over encrypted traffic, including Transport Layer Security (TLS) 1.3, thereby eliminating the need to decrypt traffic. • Protect networks against zero-day vulnerabilities with SnortML—a machine learning-based exploit detection technology integrated into the industry-leading Snort 3 Intrusion Prevention System (IPS).
Simplified management • Scale effortlessly: Manage up to 1,500 firewalls now, scaling to 2,000, via Security Cloud Control Firewall, Manager optimized for Hybrid Mesh Firewall and MSSP environments. Use prebuilt templates and streamlined migration tools for fast, consistent global deployment without extra overhead. • Unified management, smarter security: A single intuitive console unifies logging and event viewing. Integrated AIOps converts telemetry into actionable insights and automated policy recommendations, enabling faster resolution, less alert fatigue, and proactive threat response.	**Seamless integration** • Achieve comprehensive, end-to-end protection through native integration with Cisco Umbrella®, Cisco Secure Access, and Cisco Endpoint Security. • Optimize application performance and user experience through seamlessly integrated SD-WAN capabilities, accelerated by Zero-Touch Provisioning (ZTP).

Hardware overview

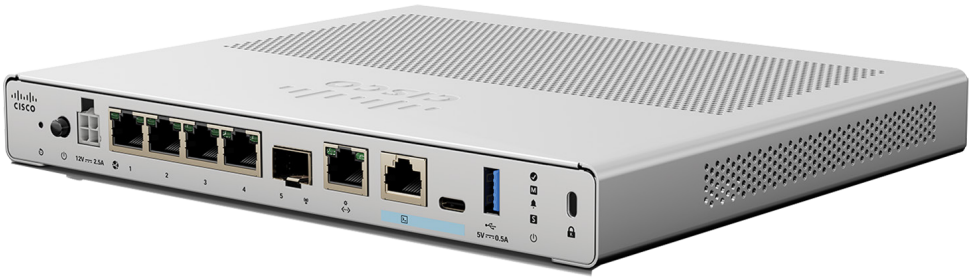


Figure 1. 3D view of the Cisco Secure Firewall 220 model

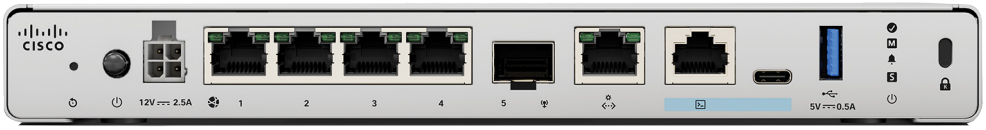


Figure 2. Front panel of the Cisco Secure Firewall 220 model

Figure 3. Back panel of the Cisco Secure Firewall 220 model

Performance

The Cisco Secure Firewall 220 supports both Cisco Firewall Threat Defense (FTD) and Cisco Adaptive Security Appliance (ASA) software. While the FTD software offers all the advanced next-generation security capabilities, ASA software delivers higher throughput for stateful inspection.

Table 2. Cisco Secure Firewall 220 performance with Cisco Secure Firepower Threat Defense (FTD) software

Metric	220
Throughput: Firewall + Application Visibility and Control (AVC) (1024B)	1.5 Gbps
Throughput: AVC + Intrusion Prevention System (IPS) (1024B)	1.5 Gbps
NGFW Throughput: FW + AVC + IPS (1024B)	1.5 Gbps
IPSec VPN Throughput (1024B TCP w/Fastpath)	1.2 Gbps
TLS Decryption[1]	0.7 Gbps
Application Visibility and Control (AVC)	Standard, supporting more than 8100 applications, as well as geolocations, users, and websites

Table 3. Cisco Secure Firewall 220 performance with the Cisco Adaptive Security Appliance (ASA) software

Metric	220
Stateful inspection firewall throughput (1500 B UDP)[2]	2 Gbps
Stateful inspection firewall throughput (HTTP 1024 Byte)	2 Gbps
IPsec VPN throughput (450B UDP L2L test)	1.8 Gbps

Note: Performance will vary depending on features activated, 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.

[1.] Throughput measured with 50% TLS 1.2 traffic with AES256-SHA with RSA 2048B keys.

[2.] Throughput measured with 1500B User Datagram Protocol (UDP) traffic measured under ideal test conditions.

Scalability

Table 4. Cisco Secure Firewall 220 scalability with the Cisco Secure Firewall Threat Defense (FTD) software

Metric	220
Maximum concurrent sessions, with AVC	30K
Maximum new connections per second, with AVC	6K
Maximum VPN peers	50
Maximum virtual router instances (VRF)	5
High availability	Active/Standby
Instances (multi-instance)	Not supported
Clustering	Not supported

Table 5. Cisco Secure Firewall 220 scalability with the Cisco Adaptive Security Appliance (ASA) software

Metric	220
New connections per second	80K
Concurrent firewall connections	100K
Maximum VPN Peers	50
High availability	Active/Standby
Security contexts	Not supported
Clustering	Not supported

Hardware specifications

Table 6. Cisco Secure Firewall 220 hardware specifications

<table>
<tr><th>Specification</th><th>220</th></tr>
<tr><td>Form factor</td><td>Compact (Can be placed on desktop. Rackmount and wall mount accessories are also available)</td></tr>
<tr><td>Fixed ports</td><td>4x 1000BASE-T
1x1G SFP</td></tr>
<tr><td>Management Ethernet</td><td>1000BASE-T port</td></tr>
<tr><td>Network modules</td><td>N/A</td></tr>
<tr><td>Maximum number of interfaces</td><td>
<table>
<tr><th>Interface Speed / Type</th><th>Fixed Ports</th><th>Expansion (2 Slots)</th><th>Total Maximum Ports</th></tr>
<tr><td>1000 BASE-T</td><td>4</td><td>NA</td><td>4</td></tr>
<tr><td>1 Gigabit SFP</td><td>1</td><td>NA</td><td>1</td></tr>
<tr><td>1000 Base-T, Management</td><td>1</td><td>NA</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>Console port</td><td>USB Type-C and RJ-45 (Cisco serial)</td></tr>
<tr><td>USB port</td><td>USB 3 Type A port</td></tr>
<tr><td>Storage</td><td>64GB</td></tr>
<tr><td>Power over Ethernet</td><td>N/A</td></tr>
<tr><td>Transceiver support</td><td>Refer to Cisco Secure Firewall (CSF) 200 Hardware Installation Guide</td></tr>
<tr><td>Mean Time Between Failures (MTBF)</td><td>700,000 Hours</td></tr>
<tr><td>Chassis dimensions (HxWxD)</td><td>1.15” x 9.2” x 7.8”
(2.9 x 23.4 x 19.8 cm)</td></tr>
</table>

Specification	220
Weight	2.6lb (1.17kg)
Cooling	Passive (fanless)
Rack mountable	Yes
Power supply	
Configuration	Single AC External 30W power supply
AC input voltage	100–240V AC
AC input frequency	50–60Hz
AC current draw, maximum	1.0A
Power consumption, typical	12.7 Watts
Power consumption, maximum	19 Watts
Redundancy	N/A
Operating Range	
Temperature: operating	32° to 104°F (0° to 40°C)
Humidity: operating	5% to 85% (noncondensing)
Altitude: operating	up to 10,000 feet (3048 m)
Acoustic noise	0 dBA
Non-operating/storage environment	
Temperature: nonoperating	-13° to 158°F (-25° to 70°C)
Humidity: nonoperating	5% to 95% (noncondensing)
Altitude: nonoperating	0 to 15,000 ft (4570 m)

Compliance

For details on product regulatory compliance in a specific market, consult the Cisco Product Approvals tool.

Table 7. Cisco Secure Firewall 220 Network Equipment-Building System (NEBS), Regulatory, Safety, Environmental and EMC Compliance

Specification	Description
Regulatory compliance	Products comply with CE markings per directives 2004/108/EC and 2006/108/EC
Safety	• UL 60950-1 • UL 62368-1 • CAN/CSA-C22.2 No. 62368-1 • EN 62368-1 • IEC 62368-1 • AS/NZS 62368-1
EMC: Emissions	• 47CFR Part 15 (CFR 47) Class A (FCC Class A) • AS/NZS CISPR 32 Class A • CISPR 32 Class A • EN55032 Class A • ICES003 Class A • VCCI Class A • EN61000-3-2 • EN61000-3-3 • KS C 9832 Class A • CNS15936 Class A • EN300386 • QCVN 118:2018
EMC: Immunity	• EN55035 • CISPR 35 • EN300386 • KS C 9835 • QCVN 18:2022 • EN61000-3-2/-3 • EN61000-4-2/-3/-4/-5/-6/-8/-11

Ordering information

Cisco Secure Firewall 200 Series hardware appliances are listed below. For information on licenses, subscriptions, and other options associated with the product, refer to the Network Security Ordering Guide.

Table 8. Cisco Secure Firewall 200 Series Product IDs

Product ID	Description
CSF220-ASA-K9	Cisco Secure Firewall 220 Appliance, ASA
CSF220-TD-K9	Cisco Secure Firewall 220 Appliance, Threat Defense

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environmental Sustainability" section of Cisco's Corporate Social Responsibility (CSR) report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.