Cisco Secure Firewall

Today's enterprise IT requires more than traditional security. Legacy solutions can't protect next-gen data centers, campus, branch, or IoT networks. Cisco's Hybrid Mesh Firewall delivers AI-ready, pervasive firewalling—integrated across switches, clouds, containers, and workloads for dynamic threat protection.

As infrastructures evolve for AI, Cisco's solution weaves protection into every layer, with unified cloud management, flexible licensing, and zero trust segmentation. It empowers modernization while ensuring security.

Cisco Secure Firewall, part of the Hybrid Mesh Firewall solution, provides advanced threat protection and operational excellence across all environments. Its advanced AI and machine learning enable smarter threat detection, while AIOps and real-time malware lookups simplify management and performance.

Secure Firewall has been put to the test

Secure Firewall is the first enterprise firewall to earn SE Labs' AAA rating in the Advanced Performance test, proving it adapts to demanding environments and protects against emerging threats.

Cisco Secure Firewall: A leader in enterprise firewalls[1, 2]

- 3x better price-performance than competitors[3].
- Identify and block threats in encrypted traffic without decrypting.
- Recognize zero-day attack patterns in-line and block emerging threats using ML.
- Global threat intelligence by Talos for advanced attack protection.
- Centralized management with AI-driven insights across Cisco security solutions.
- Universal Zero Trust Network Access (UZTNA) from one interface.
- Surface critical security insights and accelerate threat response with Splunk.

Footnote:

1 IDC MarketScape: Worldwide Enterprise Hybrid Firewall 2025 Vendor Assessment.

2 The Forrester Wave™: Enterprise Firewall Solutions, Q4 2024.

3 Secure Firewall outperformed competitive firewalls in throughput for similar use cases.

Hardware that outperforms competitors

Consistently showing 3x better price-for-performance in competitive analysis[4].

Data Center

- Inspect encrypted traffic at scale with cryptographic acceleration.
- Superior efficiency and scalability with highest throughput per Rack Unit (RU).
- High availability clustering for up to 16 devices.
- Terabit-speed encrypted traffic for high volumes of IPSec connections.

Campus and Branch

- Faster branch security with secure routing templates, zero-touch provisioning, and SD-WAN integration.
- 3x better price-performance for branch security.
- Built-in SD-WAN provides seamless connectivity into Universal ZTNA architecture.

4 Performance gain is based on the throughput of competitive firewalls for similar use cases.

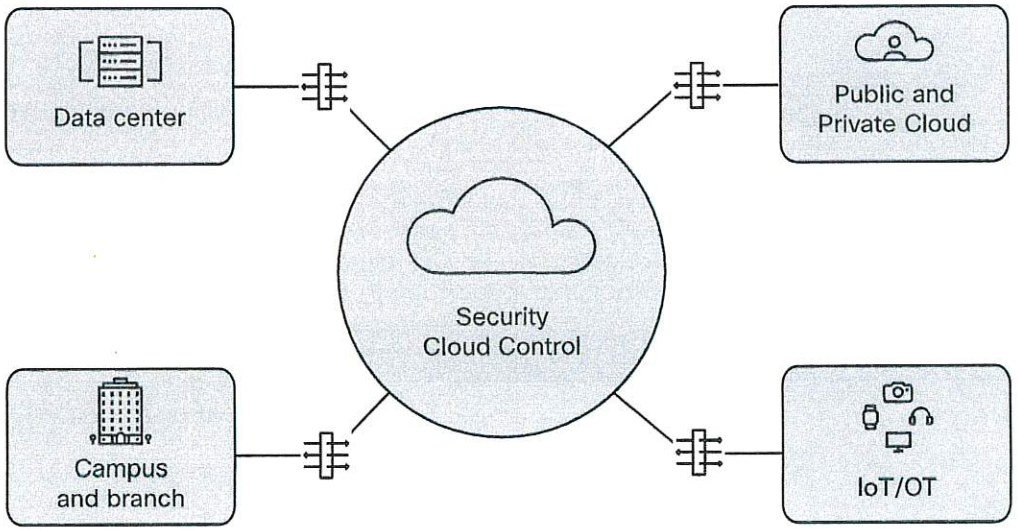
Deploy anywhere, manage in one interface

Manage firewalls centrally across on-premises hardware and virtual environments with Cisco Security Cloud Control, enhancing resilience through cloud-delivered AI-driven insights without disrupting existing workflows.

AI/ML capabilities:

- **Talos** analyzes 900B security events daily using AI/ML for threat protection services.
- **Cisco AI Assistant** helps with configuration, best practices, and workflow automation.
- **AIOps** automates and simplifies firewall management and threat response.
- **Encrypted Visibility Engine (EVE)** uses AI/ML to identify and block threats without decrypting.
- **SnortML** blocks emerging zero-day threats by analyzing live traffic for vulnerabilities.

A unified management experience wherever you have firewalls



See, Try, Buy

Learn more about Cisco Secure Firewall and try out the advanced threat protection demo at cisco.com/go/firewall.

Build the security solution that is right for you and scale as your business needs grow. Experience buying flexibility through customized buying options, price protection, and license simplification. Learn more at cisco.com/c/en/us/buy.

C45-5379301-00 09/25

Cisco Secure Firewall features

Your use case	What Cisco Secure Firewall offers
Unified firewall management	Security Cloud Control transforms security operations with its cloud-native design and AI-driven features, enabling adaptation, optimization, and intent-based policy automation across multi-vendor firewalls from a single interface.
Streamline advanced threat protection	Intrusion detection and prevention (IPS) powered by Snort 3, Secure Firewall's inspection engine, delivers high detection efficacy, resource efficiency, and manageability, with integrated malware protection and URL filtering.
Comprehensive application identification	Gain visibility into 6,500+ applications for accurate identification and control, enabling precise security policies, current threat detection, and better protection of network resources.
Maintain visibility and control where it's not realistic to decrypt	Supplement traditional decryption by providing early visibility into a server's TLS certificate for TLS 1.2 and 1.3 traffic, offering essential insight for application and URL filtering even when decryption is restricted.
Inspect QUIC connections	Deep packet inspection and policy enforcement on inbound and outbound QUIC traffic, with optimized memory allocation for efficient processing.
Implement Universal Zero Trust Network Access (UZTNA)	Users get seamless access to any app, while admins manage policies for SSE and firewall from one platform—no network changes needed. Direct app access maintains business continuity if the cloud is unavailable.
Secure IoT/OT environments	Protect critical OT assets by controlling traffic, blocking unauthorized access, and mitigating OT-specific cyber threats. Secure Firewall integrates OT protocols and ensures visibility and control across IT/OT networks.
Track and analyze firewall activity	Cisco Secure Network Analytics (SNA) and Splunk Enterprise Security (ES) offer a unified solution, compressing raw network telemetry and delivering it to Splunk for high-fidelity security insights.