The bridge to possible

Cisco Secure Firewall

The bridge to possible

Benefits

- **Simplified operations:** With a host of management options, an overhauled workflow interface, and the new AI Assistant for Security, management has never been simpler.
- **World-class security controls:** Backed by Talos threat intelligence and our encrypted visibility engine to recognize encrypted threats without decryption.
- **Budget-friendly:** Reduce vendor sprawl, list pricing and licensing across multiple products with Enterprise Licensing Agreements and flexible payment options.

Simplified operations

Word-class security controls

Budget-friendly

Secure your business with confidence, now and into the future

As the business-critical applications become a blend of cloud and on-prem environments, users need secure access to resources from everywhere. The traditional firewall approach no longer works, as a single network perimeter has evolved to multiple micro-perimeters. In the evolving hybrid work environment, applications are the new perimeter for many organizations. Traditional firewall deployments have evolved to a mixture of physical, virtual, and cloud-native appliances. As a result, organizations are struggling to operationalize support for modern application environments.

At Cisco, we're building a network security vision to enable an agile, automated, and integrated approach to harmonize policy enforcement across modern dynamic applications and increasingly heterogenous networks. Cisco Secure Firewall gives you the deepest set of integrations between core networking functions and network security, delivering the most secure architecture ever. The result is a complete security portfolio that protects your applications and users everywhere – from small and medium businesses to enterprise datacenters to service providers.

The bridge to possible

Why Cisco Secure Firewall?

The Cisco Secure Firewall portfolio delivers greater protection for your network against an increasingly evolving and complex set of threats. You can protect your business with confidence, now and into the future, with superior performance and stronger security that maximize uptime and protect your investment. With Cisco, you're investing in a foundation for security that is both agile and integrated, leading to the strongest security posture available.

Investing in Cisco Secure Firewall today gives you robust protections against even the most sophisticated threats without compromising performance when inspecting encrypted traffic. Further, integrations with other Cisco and 3rd party solutions provides you with a broad and deep portfolio of security products, all working together to correlate previously disconnected events, eliminate noise, and stop threats faster.

Superior visibility and control

Threats have become more sophisticated, and networks have become more complex. Very few, if any, organizations have the resources to dedicate to staying up to date and successfully fend off all the constantly emerging and evolving threats.

As threats and networks become more complex, it is imperative to have the right tools to protect your data, applications, and networks. Cisco Secure Firewalls have the power and flexibility that you need to stay one step ahead of threats. Thanks to its cryptographic acceleration hardware, Secure Firewall can inspect encrypted traffic at scale, or inspect without decryption, allowing you to dramatically boost your firewall performance over the previous generation of appliances. Furthermore, the human-readable rules of multi-threaded Snort 3 inspection engine help simplify security. Dynamic application visibility and control is available through the Cisco Secure Workload integration, for consistent protection for today's modern applications across the network and workload.

Find the ideal firewall for your business

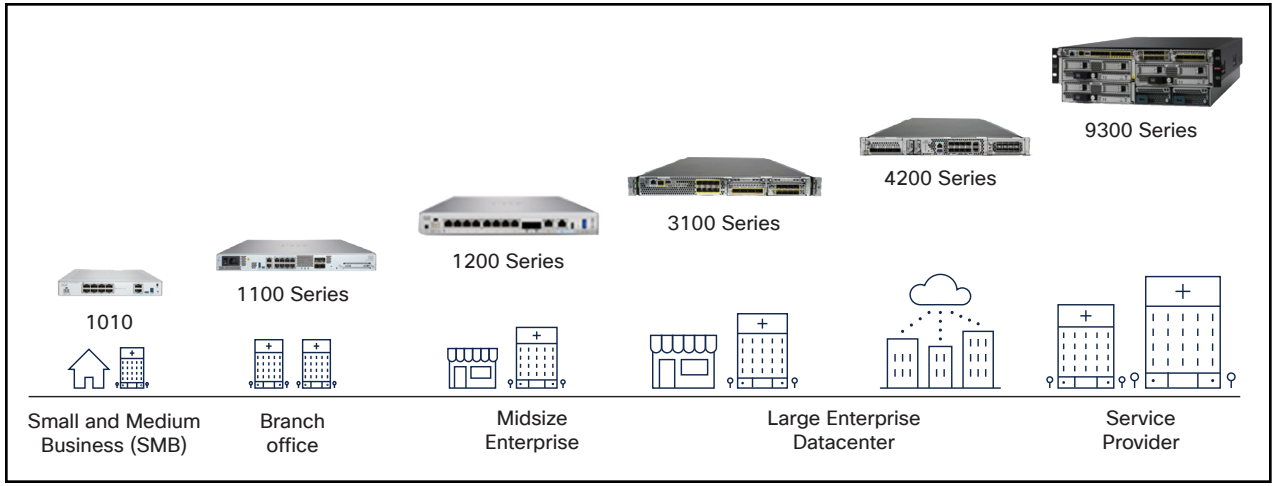

Figure 1. Cisco Secure Firewall hardware portfolio

The bridge to possible

Simplified firewall management

Cisco Secure Firewall portfolio offers flexible management options to comprehensively manage hundreds of firewalls from a central location. Whether you deploy our on-premises hardware, or use any virtual environment of your choice, you can enjoy the same look and feel, increasing your productivity. You can boost your operational efficiency even one step further with our cloud-delivered solution.

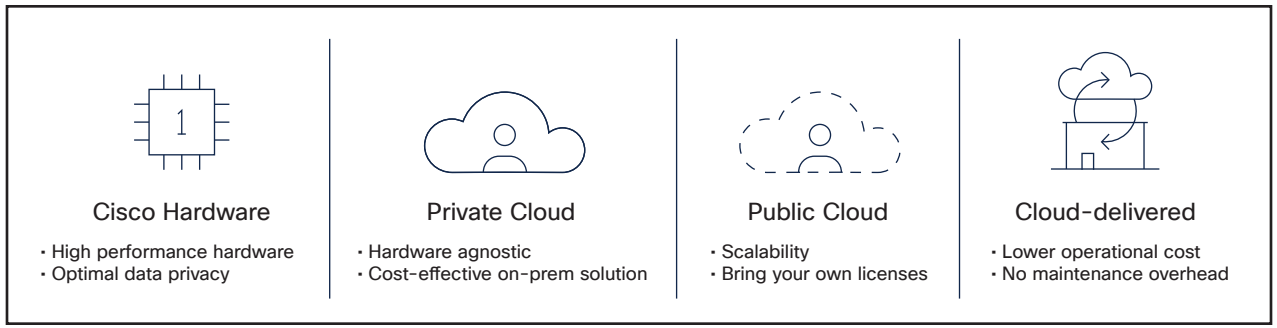

Figure 2. Versatile firewall management supports all form factors to offer unique value for your use case

Cisco also offers Cisco Security Analytics and Logging for scalable log management. It enhances threat detection and meets compliance mandates across the organization with longer retention and behavioral analysis capabilities.

Customer story

Cisco Secure Firewall advanced capabilities

Advanced Capability	Details
Simplified firewall management	• Cisco Secure Firewall Management Center (FMC) provides unified management of firewalls, application control, intrusion prevention, URL filtering, and malware defense policies.
Intrusion prevention system	• Secure Firewall provides faster threat protection with industry leading Snort 3 Intrusion Detection and Prevention System (IDS/IPS).
Threat intelligence update	• Cisco Talos Intelligence Group, one of the largest commercial threat intelligence teams in the world, regularly provides actionable threat intelligence for Cisco customers. • Talos maintains the official rulesets of Snort.org and ClamAV.net.

The bridge to possible

Advanced Capability	Details
Dynamic policy support	▪ Dynamic attributes support VMware, AWS, Azure tags for situations where static IP addresses are not available. ▪ Cisco has been a pioneer in tag-based policies with Security Group Tags (SGTs) and Cisco Identity Services Engine (ISE) attribute support.
Encrypted Visibility Engine (EVE)	▪ Gain control over encrypted traffic without decryption, allowing you to eliminate performance bottlenecks and meet compliance requirements. ▪ Encrypted Visibility Engine uses machine learning and artificial intelligence to block malicious applications in encrypted traffic without decryption.
SnortML	▪ Proactively detect and block common threats, known vulnerabilities, and 0-day exploits using Machine Learning (ML) based exploit detection engine.
AI Assistant for Security	▪ Interact with your firewall – to assist in policy identification and reporting, to augment troubleshooting and threat defense, and to automate the correction of misconfigurations, duplicate, and legacy rules.
TLS server identity and discovery	▪ Enables you to maintain Layer 7 policies on encrypted Transport Layer Security (TLS) 1.3 traffic. ▪ Maintain visibility and control in an encrypted world where it's not realistic to decrypt and inspect every single traffic flow.
Secure Branch Routing capabilities	▪ Consolidate advanced security and networking in distributed branches, and simplify the branch to headquarters security with built-in secure branch routing templates and zero-touch provisioning.
Zero Trust Application Access (ZTAA)	▪ Move beyond traditional "authorize then ignore" ZTNA models by adding complete threat inspection and policy for each individual application.

The bridge to possible

Advanced Capability	Details
Secure Firewall Cloud Native	▪ Built with Kubernetes and first available in AWS, Secure Firewall Native Cloud is a developer-friendly application access solution for building highly elastic, cloud-native infrastructure.
Cloud-delivered management	▪ Cisco Defense Orchestrator, the cloud-delivered firewall management solution, helps you to manage policies consistently with the same look and feel, enabling you to lower operational costs.
Security Analytics and Logging	▪ Highly scalable on-premises and cloud-based firewall log management with behavioral analysis for real-time threat detection and faster response times. ▪ Meet compliance needs with log aggregation across all Cisco firewalls. ▪ Tight integration with firewall managers for extended logging and analysis, as well as aggregation of firewall log data in a single intuitive view.
Secure Workload integration	▪ Cisco Secure Workload (formerly Tetration) integration enables comprehensive visibility and consistent policy enforcement for modern distributed and dynamic applications across the network and workload in a scalable manner.
Cisco XDR	▪ Leverage the Cisco XDR platform to accelerate threat detection and remediation. Firewall Management Center enables SecOps to instantly pivot to Cisco XDR open platform, accelerating incident response.

Next steps

To learn more about Cisco Secure Firewall, visit cisco.com/go/firewall.

To view buying options and speak with a Cisco sales representative, visit cisco.com/c/en/us/buy.

C45-736624-09 06/24