Cisco Secure Firewall

Integrate Network and Security

World-class security controls

Consistent policy and visibility

Turn your entire network into an extension of your security architecture

As our business-critical applications are a blend of cloud and on-premise based and users need secure access to resources from everywhere, the traditional firewall approach no longer works. Our single network perimeter has evolved to multiple micro-perimeters. For many organizations the application is the new perimeter, and 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. The challenges of how to maintain consistent visibility, policy enforcement, and uniform threat visibility without opening vulnerabilities that expose the organization to risk.

At Cisco, we're building a network security vision, NetWORK, that enables a more agile, automated, and integrated approach for harmonizing policies and enforcement across modern dynamic applications and increasingly heterogenous networks. 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.

Benefits

- Real-time, unified, workload and network security for integrated control across dynamic application environments
- Platform approach to network security, leveraging and sharing intelligence from key sources for faster detection, response, and remediation
- Safeguard remote workers with highly secure enterprise access anytime, anywhere, from any device, with powerful threat prevention capabilities that protect the organization, users and critical applications
- SecureX entitlement included with every Cisco Secure Firewall, for a tightly integrated approach to security that enables threat correlation across the Cisco Secure portfolio and accelerates incident response

© 2021 Cisco and/or its affiliates. All rights reserved.

Why Cisco?

The Cisco Secure Firewall portfolio delivers greater protections for your network against an increasingly evolving and complex set of threats. With Cisco, you're investing in a foundation for security that is both agile and integrated- leading to the strongest security posture available today and tomorrow.

From your data center, branch offices, cloud environments, and everywhere in between, you can leverage the power of Cisco to turn your existing network infrastructure into an extension of your firewall solution, resulting in world class security controls everywhere you need them.

Investing in a Secure Firewall appliance 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.

World-class security controls

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 these 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. They offer a dramatic 3x performance boost over the previous generation of appliances, in addition to unique hardware-based capabilities for inspecting encrypted traffic at scale. As well, the human-readable rules of Snort 3 IPS help simplify security. eDynamic 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.

Customer story | Demo

Consistent policy and visibility

With the Secure Firewall portfolio, you gain a stronger security posture, equipped with future-ready, flexible management. Cisco offers a variety of management options tailored to meet your technology and business needs including: Firewall Device Manager (FDM), Cisco Secure Firewall Management Center (FMC), Cisco Defense Orchestrator (CDO), and Cisco Security Analytics and Logging.

Cisco FDM is an on-device management solution for locally managing small-scale deployments. Cisco Secure FMC is an on-premises solution for large deployments to centrally manage security events and policies with rich reporting and local logging. CDO is a cloud-based security manager that streamlines security policies and device management across your extended network. Cisco Security Analytics and Logging provides scalable log management with behavioral analysis.

Customer story | Demo

© 2021 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Firewall advanced capabilities:

Advanced Capability	Details
Cisco Secure Workload integration	· Cisco Secure Workload (Tetration) integration enables comprehensive visibility and policy enforcement for modern distributed and dynamic applications across the network and workload for consistent enforcement in a scalable manner.
Cisco 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.
Dynamic policies 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.
Snort 3 Next-Generation Intrusion Prevention System	· The next step in threat protection with industry leading open-source Snort 3 helps improve detection, simplify customization, and enhance performance.
Transport Layer Security (TLS) Server Identity and Discovery	· Enables you to maintain Layer 7 policies on encrypted TLS 1.3 traffic. Main visibility and control in an encrypted world where it's not realistic that you can decrypt and inspect every single traffic flow. Competing firewalls break your Layer 7 policies with encrypted TLS 1.3 traffic.
Secure Firewall Management Center (FMC)	· Provides unified management of firewalls, application control, intrusion prevention, URL filtering, and malware defense policies. · Integration with Cisco Secure Workload (formerly Tetration) enables consistent visibility and policy enforcement for dynamic applications across the network and workload.
Cisco Defense Orchestrator CDO	· Cloud-based firewall management that helps you consistently and easily manage policies across your Cisco Secure firewalls.
Cisco Security Analytics and Logging (SAL)	· Highly scalable on-premise and cloud based firewall log management with behavioral analysis for real-time threat detection, for faster response times. Plus continuous analysis to further refine your security posture to better defend against future attempts. · Meet your compliance needs with log aggregation across all Cisco Secure Firewalls. · Tight integration with firewall managers for extended logging and analysis, as well as aggregating firewall log data in a single intuitive view.
SecureX platform	· Leverage the SecureX platform to accelerate threat detection and remediation. Every Secure Firewall includes entitlement for Cisco SecureX. The new SecureX ribbon in Firewall Management Center enables SecOps to instantly pivot to SecureX's open platform, speeding incident response.
Advanced threat intelligence (Talos)	· Cisco Talos Intelligence Group is one of the largest commercial threat intelligence teams in the world. They create accurate, rapid and actionable threat intelligence for Cisco customers, products and services. Talos maintains the official rulesets of Snort.org, ClamAV, and SpamCop.

Next steps

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

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

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C45-736624-04 05/21