Cisco Firepower Next-Generation Firewall

Turn your entire network into an extension of your security architecture, protect against threats with world class security controls, and gain clarity with consistent policy and visibility.

Modernize your “firewalling” with Cisco NGFW

For over two decades, the firewall has been the cornerstone of an organization’s network security strategy. It was designed based on the notion that internal traffic and users were inherently trustworthy, and external traffic wasn’t, thus creating a trust boundary – or perimeter – between networks. This network perimeter became the logical security control point to protect the entire organization; the network, data, users and devices. All network traffic, whether originating from the headquarters, a data center or remote worker, was funneled through this single control point.

Since then, the way we work changed. Many of our business-critical applications moved from our data centers and premises-based networks to the cloud. Our branch offices are now connecting directly to the internet. And users are accessing resources from their personal devices everywhere. These new developments require that we re-think firewalling and network security with a more holistic approach.

At Cisco, we’re bringing networking leadership and cutting-edge security technology together to deliver the most secure architecture ever. Whether it’s enhancing network security with your existing investments in Cisco Application-Centric Infrastructure (ACI) and Identity Services Engine (ISE), or transforming your router into a firewall, we aren’t going to stop innovating for our customers. Because Cisco NGFW is network security designed for you - from the company that built the network.

Capabilities

Stop more threats:
Contain known and unknown malware with leading Cisco® Advanced Malware Protection (AMP) and sandboxing.

Prioritize threats:
Gain superior visibility into your environment with Cisco Firepower next-generation intrusion prevention system (NGIPS). Automated risk rankings and impact flags identify priorities for your team.

Detect earlier, act faster:
Cisco Talos is an industry-leading threat intelligence research organization that powers the Cisco NGFW portfolio. Talos defends Cisco customers by finding new malware domains, malicious URLs as well as unknown or undisclosed vulnerabilities and writing rules to help mitigate them. These rules are also incorporated into the integrated SNORT IPS of Cisco NGFW to provide enhanced security against even the most sophisticated threats as well as to help comply with regulatory requirements.

World class security controls

It's time to re-think the firewall. To do this, you need a more agile and integrated approach for harmonizing policies and enforcement across increasingly heterogeneous networks. At Cisco, we're building a security platform that does just that – by delivering world-class security controls everywhere you need them, with industry-leading security intelligence and intrusion prevention.

To protect your network against an increasingly complex set of threats you require a complete portfolio of integrated enforcement points deployed everywhere you need them. Cisco is the leader in threat efficacy due to our ability to collate threat data across our security portfolio. Our solutions are informed by Talos, an industry leading threat intelligence organization that helps keep you aware of and protected from the latest threats.

Case Study: Cyprus University of Technology

With Cisco Firewall and Cisco Security, we can secure our network and be sure that students, staff, and visitors are safe so we can focus on what matters here: education.

Andreas Mouskos,

Network Security Engineer, Cyprus University of Technology

Read story

Case Study: Los Rios Community College District

Cisco Defense Orchestrator makes firewall builds, management, visibility, and auditing infinitely easier. Things that take 10 minutes in Cisco Defense Orchestrator take a day or more without it.

Mike Muzinich,

Senior IT Network Administrator, Los Rios Community College District

Read story

Consistent policy and visibility

Security breaches and attacks are becoming more common and more impactful each year. As threats become more advanced, organizations are responding by adding more point security products. The result is complex management, inconsistent policies, and human error that lead to vulnerability.

With the Cisco NGFW portfolio you gain a stronger security posture, equipped with future-ready management. Cisco continues to invest in streamlining security policy harmonization and device management across your extended network. The result is accelerated security operations such as detection, investigation, and remediation.

Capabilities

Maintain consistent policies: With the Cisco NGFW portfolio you gain a stronger security posture, equipped with future-ready, flexible management. Cisco offers a variety of management options tailored to meet your environment and business needs including: Firepower Device Manager (FDM), Cisco Firepower Management Center (FMC), and Cisco Defense Orchestrator (CDO).

Cisco FDM is an on-device management solution for locally managing small-scale deployments. Cisco 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.

Reduce complexity:
Get automated threat correlation across tightly integrated security functions, including application firewalling, next-gen intrusion prevention systems (NGIPS), and advanced malware protection (AMP).

Stay ahead of threats:
Gain granular visibility of your infrastructure and quickly identify and remediate vulnerabilities

Cisco Case Study: Lewisville School District

The combination of Umbrella and Firepower NGFW enable us to proactively block threats we weren't blocking before, troubleshoot faster and easier, and know with unprecedented specificity how we're protecting our students against threats, so they can concentrate on acquiring the skills and knowledge they'll need after graduation.

Chris Langford,

Director of Network, Infrastructure, and Cyber Security, Lewisville ISD

Read story

Turn your network into an extension of your security architecture

Today, there no longer is a single network perimeter or control point. Instead we have multiple "micro- perimeters" across a variety of interconnected networks, devices, users and data. Consequently, our traditional firewall devices are being augmented by a mixture of physical and virtual appliances. Some are even taking on new form factors, such as SD-WAN routers and secure internet gateways. As a result, organizations are struggling to operationalize all these disparate security solutions to maintain consistent policies and uniform threat visibility.

Trust your network security with the world leader in enterprise networking, giving you the deepest set of integrations between core networking functions and network security. The result is a complete and integrated security portfolio that turns your network itself into an extension of your security architecture.

Capabilities

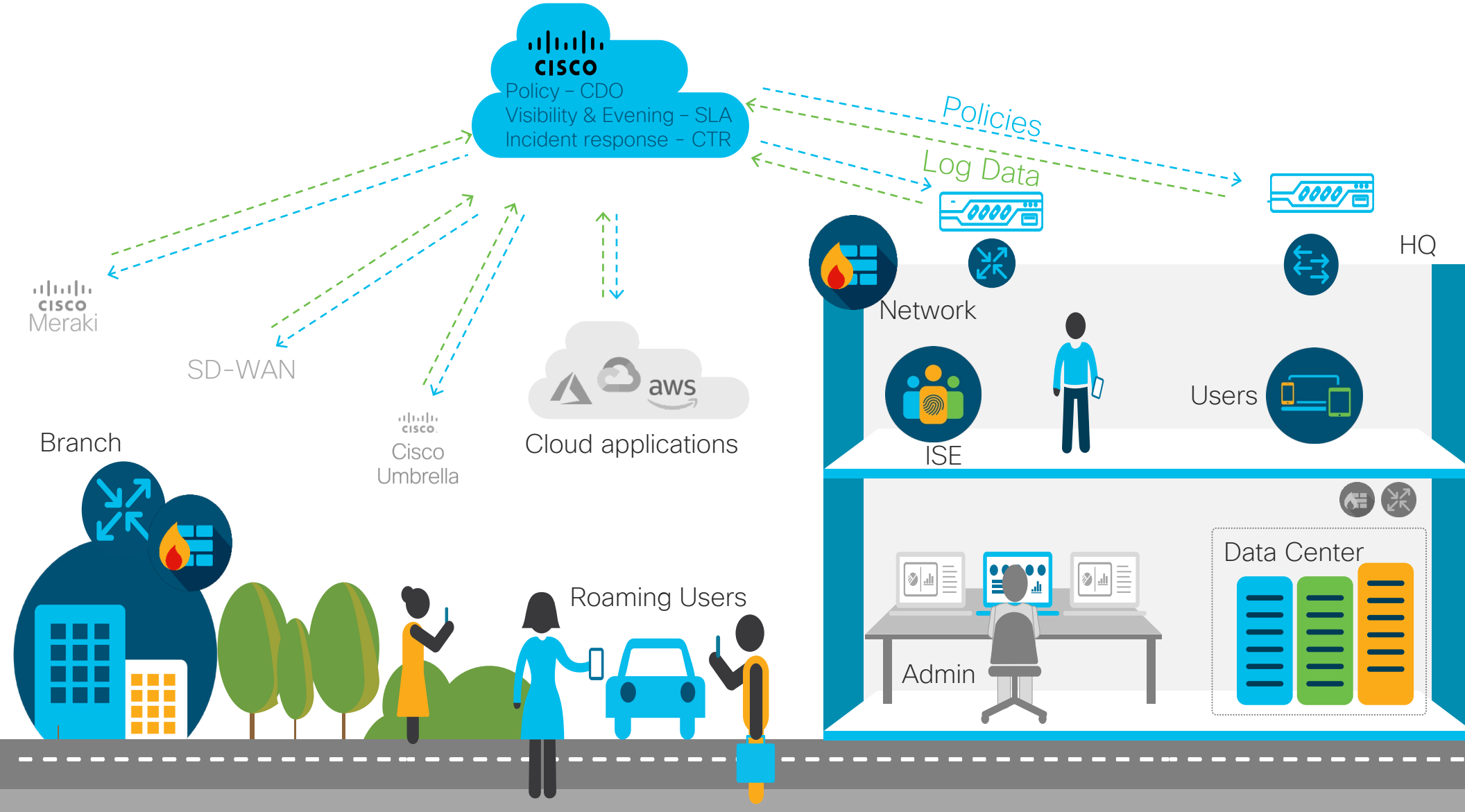
Get more from your existing network:
Enhance security with your existing investments, including Cisco ACI and ISE.

Greater security control points:
Enforce polices across your entire environment, including any Cisco security device administered by the organization.

Predictable application experience:
Increase user productivity by optimizing cloud and on-premises application performance with real-time analytics, visibility and control with Cisco Stealthwatch.

The future of “firewalling” begins with Cisco NGFW

At Cisco, we’re building a security platform that delivers world-class security controls everywhere you need them, with consistent visibility, policy harmonization, and stronger user and device authentication. We’re bringing networking leadership and cutting-edge security technology together so that the entire network can act as an extension of the firewall, leading to the most secure architecture ever.



Why Cisco?

Instead of the traditional approach where the network is protected by a single control point, organizations need a more agile and flexible approach toward delivering security controls across increasingly heterogenous networks. Cisco's NGFW portfolio provides that flexible approach, allowing organizations to deliver consistent visibility and control to their data centers, branch offices, cloud environments, and everything in between.

Feeding this portfolio is Cisco Talos, an industry-leading threat intelligence research organization. Talos defends Cisco customers by finding new malware domains, malicious URLs as well as unknown or undisclosed vulnerabilities and writing rules to help mitigate them.

By investing in a Cisco NGFW appliance today, you're setting the foundation for the strongest security posture available today and tomorrow. You will benefit from significant performance improvements in NGFW throughput, more connections per second, and better performance for encrypted traffic. Further, integration with other Cisco 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.

Models & Options

Firepower 1000 series

[SMB and branch office]

- Stateful firewall, AVC, NGIPS, AMP, URL Filtering
- 650 Mbps – 3 Gbps NGFW throughput

Firepower 2100 series

[Mid – Large Enterprise]

- 1 RU form factor
- Dual multicore CPU architecture
- Firewall throughput speeds from 2 Gbps to 8.5 Gbps

Firepower 4100 series

[Data center]

- 1 RU form factor
- 1/10/40 Gigabit Ethernet interfaces
- Up to 45-Gbps NGFW throughput
- Radware vDP behavioral DDoS mitigation

Firepower 9300

[Data center and service provider]

- 1.2 Tbps clustered throughput
- 10/40/100 Gb Network Interfaces
- 57 million concurrent connections, with application control
- Radware vDP behavioral DDoS mitigation

Virtual Appliances (VM-based firewalls)

Cisco NGFWv

- Optimized for cloud and data center environments
- VMware, KVM, Hypervisor support
- AWS, Azure, and Azure government cloud
- 1.2 Gps throughput firewall + AVC, 1.1 Gps throughput AVC + IPS
- Stateful firewall, Application Visibility and Control, NGIPS, Advanced Malware Protection, URL filtering, VPN

Next step

To learn more about Cisco Firepower NGFW, visit cisco.com/go/ngfw

To request a free trial, visit https://engage2demand.cisco.com/1829