Cisco Secure Firewall Threat Defense Virtual on AWS

Hybrid and multicloud is here – are you ready?

The world has gone hybrid and multicloud, and most, if not all business success depends on secure connected experiences.

Today, 82% of global IT professionals have adopted hybrid cloud and 47% of organizations use between two and three public IaaS clouds.[2] Hybrid and multicloud environments offer organizations greater agility and flexibility, but the hyper-distribution of resources and applications across these environments makes it difficult for NetOps, SecOps, and DevOps teams to keep up. Additionally, the unforeseen byproduct of hybrid and multicloud adoption is complexity – limiting critical security functions including visibility, control, and the ability to gain context.

Benefits

- Get up and running in minutes with our AWS Quick Starts or Infrastructure-as-a-Code (IaaC) scripts
- Deploy policy controls consistently regardless of if you are on-premises or in the cloud
- Scale up your firewall capacity automatically with AWS Auto Scaling support
- Deeper visibility into QUIC and TLS 1.3 encrypted traffic without breaking Layer 7 policies or compliance
- Quickly boot up or recover your virtual firewalls with snapshot support
- Firewall clustering for highly available threat defense
- Return on investment in less than 12 months[1]

Stronger security against a new generation of threats

Cisco® Secure Firewall Threat Defense Virtual helps drive stronger security by seeing more, detecting faster, and streamlining operations. It combats complexity with consistent policy enforcement, promotes visibility and control with deep packet inspection, as well as ingress and egress traffic inspection – all within a virtualized form factor.

Superior threat defense

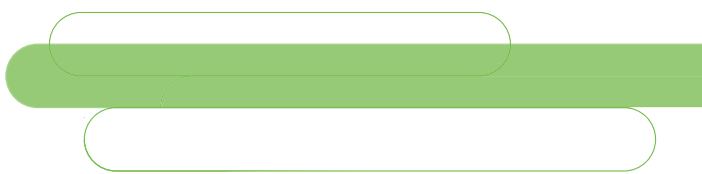
Protect your hybrid and multicloud environment against known and unknown threats with advanced threat defense options including malware defense and URL filtering. And with the Snort 3 IPS, you can obtain hourly threat intelligence updates from Cisco Talos®, enabling faster inspection without slowing down your network.

Greater visibility

Secure Firewall's Encrypted Visibility Engine protects against malicious applications embedded in encrypted traffic, maintains Layer 7 policies on encrypted traffic, and delivers insights into application behavior. Only Cisco is addressing this critical concern for networking and security professionals, 65% of whom reported loss of IPS and Layer 7 efficacy with new protocols like TLS 1.3 and QUIC.[3]

Dynamic policy management

Reduce policy maintenance and complexity in the cloud with dynamic attribute support for AWS tags. As workloads spin up and down in your AWS environment, your organization can keep policies current without redeploying with dynamic objects.



Save time with simplified firewall management

Cisco Secure Firewall Management Center (FMC) reduces up to 95% of network operation workstreams (www.cisco.com/go/firewallTEI) by helping organizations correlate and prioritize threats, as well as quickly act on them in a single pane of glass. It also gives teams the freedom and choice for administering firewalls with a consistent experience across its cloud-delivered, virtual, and on-premises form factors. Secure Firewall Management Center also helps SecOps teams save time by speeding up incident response with a built-in ribbon that pivots you to the Cisco SecureX™ open platform. And for organizations looking for flexibility to migrate their firewall from on-premises to the cloud, or vice versa, Cisco offers a migration tool to assist with policy carryover.

Make zero trust practical by integrating with Cisco Secure Workload

Integrating Secure Firewall with Secure Workload brings security closer to your applications. Secure Workload provides visibility, dynamic policy automation, and enforcement of a zero-trust approach through microsegmentation – across the entire application environment. This eliminates unauthorized lateral movement, minimizing the risk of ransomware and other distributed attacks. This combination unifies network and application security controls, enabling network security teams to keep pace with rapidly changing application environments.

To pinpoint changes in your dynamic application environments, Secure Workload offers real-time monitoring, vulnerability management, and automation so your teams can assess and act on anomalies and threats quickly. Secure Workload supports any application, any workload, anywhere—including Amazon EKS managed Kubernetes environments.

Accelerate incident response with Cisco SecureX

Cut incident response time by 70% with Cisco SecureX (www.cisco.com/go/securexTEI), our open security platform included with every Cisco Secure Firewall. It accelerates the time to detect, investigate, and remediate threats by aggregating and correlating global intelligence and local context in one centralized view. SecureX also integrates with Amazon GuardDuty to monitor your AWS accounts and workloads for malicious activity.

Why Cisco?

Today's business depends on the hybrid and multicloud environment. The need for security resilience is paramount to protect the integrity of your business amidst unpredictable threats and change, and it starts by securing the core of your environment with Cisco. We are simplifying security, providing the same experience and policy controls regardless of location or form factor as well as tools and templates to help you spin up the infrastructure you need in minutes.

With workers, data, and offices located all over, your firewall is more relevant than ever. Secure Firewall helps you plan, prioritize, close gaps, and recover from disaster – stronger. By investing in Secure Firewall, you are taking a significant step toward robust protections against even the most sophisticated threats, bringing visibility back to your team, and safeguarding your data, wherever it may roam without compromising performance.

Tools and templates

Getting Started Guide

AWS Quick Starts

Cisco Secure Firewall DEVNET Templates and GitHub

AWS Marketplace listings

Cisco Secure Firewall Threat Defense Virtual – Pay-As-You-Go

Cisco Secure Firewall Threat Defense Virtual – Bring-Your-Own-License

Advanced capabilities	Details
Introduce AWS services for added benefits	• Combine with AWS Gateway Load Balancer to dynamically insert scalable security into your AWS environment and reduce complexity. • Leverage Amazon Route 53 for remote access VPN. • Integrate with AWS Transit Gateway for scalable inter-VPC traffic.
Transport Layer Security (TLS) Server Identity and Discovery	• Enables you to maintain Layer 7 policies on encrypted 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. Competing firewalls break your Layer 7 policies with encrypted TLS 1.3 traffic.
Firewall clustering	• Combine multiple firewalls into a single logical firewall for ease of management and performance scale. • Laterally scale your virtual firewall deployments with predictable performance.
Cisco 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. 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.
Cisco Talos threat intelligence	• 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.

References

[1] Forrester Total Economic Impact of Cisco Secure Firewall, 2022. www.cisco.com/go/firewallTEI

[2] 2022 Global Hybrid Cloud Trends Report. S&P Global Market Intelligence, 2022.

[3] Steffen, Christopher M. & Buckler, Ken. (2022). TLS 1.3's Third Anniversary: What Have We Learned About Implementation and Network Monitoring?. Enterprise Management Associates (EMA).

[4] Forrester Total Economic Impact of Cisco SecureX, 2021. www.cisco.com/go/securexTEI