Cisco Secure Firewall Threat Defense Virtual

Contents

Introduction

Cisco® Secure Firewall Threat Defense Virtual delivers next-generation firewall capabilities purpose-built for public, private, and hybrid cloud environments. It provides robust, scalable security and simplified management without the constraints of physical hardware.

Secure Firewall Threat Defense Virtual extends Cisco Hybrid Mesh Firewall architecture to the cloud, delivering AI-powered threat inspection and uniform security policy enforcement across workloads, regardless of where they reside. It integrates seamlessly with cloud-native networking constructs to enhance application performance and ensure reliable, secure access for users and workloads alike.

Table 1. Key capabilities of Secure Firewall Threat Defense Virtual

Secure Firewall Threat Defense Virtual	
Robust connectivity and portability • Deploy appliances everywhere, from your data center to your branch office, with the portability of one license to support virtual deployments across public or private clouds. • Automatically scale firewall capacity in response to real-time traffic demands with native auto-scale support, while clustering delivers high-performance throughput and resilience across distributed cloud environments.	**Superior visibility** • Leverage the AI-powered Encrypted Visibility Engine (EVE) to gain insights into and control over encrypted traffic, including Transport Layer Security (TLS) 1.3, thereby eliminating the need to decrypt traffic. • Protect networks against zero-day vulnerabilities with SnortML, a machine learning-based exploit detection technology integrated into the industry-leading Snort 3 Intrusion Prevention System (IPS) and powered by the Cisco Talos Intelligence Group.
Simplified management • Manage hundreds of firewalls across various global branch locations using a single unified manager, available in both on-premises and cloud-delivered platforms. • Accelerate and simplify firewall deployment across public cloud environments with Cisco Multicloud Defense, providing centralized orchestration, consistent policy management, and streamlined operations.	**Seamless integration** • Achieve comprehensive, end-to-end protection through native integration with Cisco Umbrella®, Cisco Secure Access, and Cisco Endpoint Security. • Optimize application performance and user experience through seamlessly integrated SD-WAN capabilities, accelerated by Zero-Touch Provisioning (ZTP).

Flexible performance-based licensing

Cisco's virtual firewall appliance leverages a performance-based licensing model designed to deliver deployment flexibility across a wide range of infrastructure environments, including public, private, and hybrid-cloud deployments.

Each performance license tier enforces two key parameters:

- **Throughput (Rate Limit)** – Controls the maximum firewall inspection throughput via an integrated rate limiter, ensuring predictable and consistent performance aligned to the selected tier.
- **Remote Access (RA) VPN Session Limit** – Defines the maximum number of concurrent Remote Access VPN sessions supported under the license tier.

Table 2. Performance License Tiers

Performance Tier	Throughput (Rate Limit)	RA VPN Session Limit
FTDv5	100 Mbps	50 Sessions
FTDv10	1 Gbps	250 Sessions
FTDv20	3 Gbps	250 Sessions
FTDv30	5 Gbps	250 Sessions
FTDv50	10 Gbps	750 Sessions
FTDv100	16 Gbps	10,000 Sessions
FTDvU (Unlimited)	No Rate Limiter	32,000 Sessions

Important: Secure Firewall Threat Defense Virtual performance tiers have no impact on the underlying compute resources (vCPUs and memory) assigned to the virtual appliance or the compute instance/shape selected in public cloud environments. The allocated compute resources drive appliance scale for capabilities such as routing table size, access control rules, and more. This decoupled approach gives customers the flexibility to independently size their virtual firewall with the compute resources needed to meet their specific requirements, while selecting the performance license tier that aligns with their throughput and VPN session needs.

Deployment and system requirements

Secure Firewall Threat Defense Virtual is available across all major public cloud marketplaces and supports deployment on the industry's leading hypervisor platforms:

Table 3. Deployment Environment Summary

Category	Supported Platforms
Private Cloud/On-Premises	VMware, KVM, OpenStack, Nutanix, Microsoft Hyper-V
Public Cloud	AWS, Azure, GCP, OCI, Alibaba Cloud, Megaport, Equinix
Minimum System Requirements	4 vCPUs | 8 GB RAM | 100 GB Disk
Maximum System Requirements	64 vCPUs | 128 GB RAM | 500 GB Disk

Table 4. Deployment Environment (Public Cloud) Compatibility Matrix

Category	AWS	Azure	GCP	OCI	Alibaba	Megaport	Equinix
BYOL (Bring Your Own License)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PAYG (Pay As You Go)	Yes	Yes	No	No	No	No	No
Auto-Scale	Yes	Yes	Yes	Yes	No	No	No
High Availability (Clustering)	Yes	Yes	Yes	No	No	No	No
Orchestration via Cisco Multicloud Defense	Yes	Yes	Yes	No	No	No	No
Management via Cisco Firewall Management Center	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Management via Cisco Firewall Device Manager	Yes	Yes	Yes	No	No	No	No

Table 5. Deployment Environment (Private Cloud) Compatibility Matrix

Category	VMware	KVM	Nutanix	OpenStack	Hyper-V	HyperFlex
BYOL (Bring Your Own License)	Yes	Yes	Yes	Yes	Yes	Yes
High Availability (Active/Standby)	Yes	Yes	Yes	Yes	Yes	Yes
High Availability (Clustering)	Yes	Yes	No	No	No	No
Management via Firewall Management Center	Yes	Yes	Yes	Yes	Yes	Yes
Management via Firewall Device Manager	Yes	Yes	Yes	Yes	No	Yes

Note: For more information on each of the supported deployment environments, please reference the corresponding Getting Started Guide and the Secure Firewall Threat Defense Compatibility Guide.

Performance and scale

Your performance may vary from the below. These should be considered general guidelines. Your actual performance will depend on the environment, including traffic type and profile, CPU type, CPU speed, cache, number of interfaces, etc. For a complete list of supported compute instances and shapes, please reference the corresponding Getting Started Guide.

Table 6. Performance specifications for Secure Firewall Threat Defense Virtual (ESXi/KVM/OpenStack) version 10.0+ running Snort3 and SR-IOV

Metric	4 x vCPU	8 x vCPU	12 x vCPU	16 x vCPU	32 x vCPU	64 x vCPU
Throughput: FW + AVC (1024B)	5Gbps	7.2Gbps	19Gbps	26Gbps	59Gbps	90Gbps
Throughput: FW + AVC + IPS (1024B)	4.5Gbps	7Gbps	18Gbps	25Gbps	55Gbps	85Gbps
IPSec VPN Throughput (1024B TCP w/Fastpath)	2.2Gbps	3.2Gbps	6Gbps	10.5Gbps	35Gbps	67Gbps

Metric	4 x vCPU	8 x vCPU	12 x vCPU	16 x vCPU	32 x vCPU	64 x vCPU
Maximum concurrent sessions, with AVC	100K	250K	500K	2M	4M	8M
Maximum new connections per second, with AVC	27K	44K	80K	135K	300K	500K
Maximum VPN peers	250	250	750	10K	20K	32K
Maximum Virtual Router Instances (VRF)	30	30	30	30	30	30
Clustering*	Yes	Yes	Yes	Yes	Yes	Yes

Table 7. Performance specifications for Secure Firewall Threat Defense Virtual (AWS) version 10.0+ running Snort3 and SR-IOV

Metric	4 x vCPU	8 x vCPU	16 x vCPU
	c5n.xlarge	c5n.2xlarge	c5n.4xlarge
Throughput: FW + AVC (1024B)	4Gbps	4.1Gbps	12Gbps
Throughput: FW + AVC + IPS (1024B)	3Gbps	4.1Gbps	12Gbps
IPSec VPN Throughput (1024B TCP w/ Fastpath)	2.5Gbps	2.5Gbps	7.2Gbps
Maximum concurrent sessions, with AVC	250K	250K	2M
Maximum new connections per second, with AVC	13K	30K	80K
Maximum VPN peers	250	250	10K
Clustering	No	Yes	Yes

Table 8. Performance specifications for Secure Firewall Threat Defense Virtual (Azure) version 10.0+ running Snort3 and SR-IOV

Metric	4 x vCPU	8 x vCPU	16 x vCPU
	Standard_D3_v2	Standard_D8_v5	Standard_D16_v5
Throughput: FW + AVC (1024B)	2.7Gbps	5.7Gbps	11Gbps
Throughput: FW + AVC + IPS (1024B)	2.6Gbps	5.6Gbps	10.5Gbps
IPSec VPN Throughput (1024B TCP w/ Fastpath)	1.6Gbps	3.4Gbps	8.5Gbps
Maximum concurrent sessions, with AVC	250K	250K	2M
Maximum new connections per second, with AVC	20K	38K	100K
Maximum VPN peers	250	250	10K
Clustering	No	Yes	Yes

Table 9. Performance specifications for Secure Firewall Threat Defense Virtual (GCP) version 10.0+ running Snort3 and SR-IOV

Metric	4 x vCPU	8 x vCPU	16 x vCPU
	C2-Standard-4	C2-Standard-8	C2-Standard-16
Throughput: FW + AVC (1024B)	4.5Gbps	4.5Gbps	12.5Gbps
Throughput: FW + AVC + IPS (1024B)	2.7Gbps	4.5Gbps	12Gbps
IPSec VPN Throughput (1024B TCP w/ Fastpath)	3Gbps	3Gbps	7.5Gbps
Maximum concurrent sessions, with AVC	250K	250K	2M
Maximum new connections per second, with AVC	13K	32K	95K
Maximum VPN peers	250	250	10K
Clustering	No	Yes	Yes

Table 10. Performance specifications for Secure Firewall Threat Defense Virtual (OCI) version 10.0+ running Snort3 and SR-IOV

Metric	VM.Standard3		VM.Standard.A1		
	8 x vCPU (4 x OCPUs)	16 x vCPU (8 x OCPUs)	4 x vCPU (4 x OCPUs)	8 x vCPU (8 x OCPUs)	16 x vCPU (16 x OCPUs)
Throughput: FW + AVC (1024B)	4Gbps	8.1Gbps	3Gbps	4.5Gbps	13Gbps
Throughput: FW + AVC + IPS (1024B)	4Gbps	8.1Gbps	3Gbps	4.5Gbps	13Gbps
IPSec VPN Throughput (1024B TCP w/Fastpath)	3.5Gbps	7.9Gbps	1.8Gbps	2.5Gbps	8Gbps
Maximum concurrent sessions, with AVC	250K	2M	100K	250K	2M
Maximum new connections per second, with AVC	40K	120K	20K	32K	100K
Maximum VPN peers	250	10K	250	250	10K
Clustering	No	No	No	No	No

Table 11. Performance specifications for Secure Firewall Threat Defense Virtual (Alibaba) version 10.0+ running Snort3 and SR-IOV

Metric	4 x vCPU	8 x vCPU	16 x vCPU
	g5ne.xlarge	g5ne.2xlarge	g5ne.4xlarge
Throughput: FW + AVC (1024B)	3.1Gbps	3.7Gbps	9.6Gbps
Throughput: FW + AVC + IPS (1024B)	2.1Gbps	3.6Gbps	9Gbps
IPSec VPN Throughput (1024B TCP w/ Fastpath)	2Gbps	2.2Gbps	6.1Gbps
Maximum concurrent sessions, with AVC	250K	250K	2M
Maximum new connections per second, with AVC	10K	25K	70K
Maximum VPN peers	250	250	10K
Clustering	No	No	No

Ordering information

Performance tiered licensing is available starting from Firewall Threat Defense Virtual version 7.0. The new licensing model also includes Base License as a subscription. For information on licenses, subscriptions, and other options associated with the product, refer to the Network Security Ordering Guide.

Table 12. Ordering information for Secure Firewall Threat Defense Virtual

Product ID	Description
FTDV-SEC-SUB	Secure Firewall Threat Defense Virtual Subscription
Once the above PID is selected, you can choose the appropriate performance tier along with one or more of the available add-on subscription licenses (T-Threat, M-Malware Defense, and URL Filtering).	

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environmental Sustainability" section of Cisco's Corporate Social Responsibility (CSR) report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.