Cisco Secure Firewall Threat Defense Container

Contents

Introduction

In today's fast-paced digital landscape, organizations are rapidly embracing containerized applications to achieve unparalleled scalability, flexibility, and efficiency. However, as the adoption of containers grows, so does the complexity of securing them. Traditional security measures often fall short in providing the necessary protection for these dynamic environments. This is where the need for a specialized container firewall becomes essential.

Cisco® Secure Firewall Threat Defense Container (FTDc) extends Cisco Hybrid Mesh Firewall architecture to container networks by delivering next-generation firewall capabilities with AI-powered threat inspection and uniform security policy enforcement. It enables you to select the performance level that best suits your organization. With scalable VPN capabilities, it ensures secure access to your organization's resources while safeguarding workloads against evolving and complex threats.

Table 1. Key capabilities of Secure Firewall Threat Defense Container

Secure Firewall Threat Defense Container	
Robust connectivity and portability • Deploy appliances everywhere, from your data center to your branch office, with the portability of one license to support virtual and container deployments across public or private clouds. • Container lifecycle management via HELM charts. • Low-Touch Provisioning (LTP) via Sidecar. • Layer 3 through Layer 7 firewalling based on traditional network constructs and container-native attributes.	**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 physical, virtual, or container firewalls across various global branch locations using a single unified management console, available in both on-premises and cloud-delivered form factors.	**Seamless integration** • Achieve comprehensive, end-to-end protection through native integration with Cisco Umbrella®, Cisco Secure Access, and Cisco Endpoint Security.

Flexible performance-based licensing

Cisco's container firewall leverages the same performance-based licensing model as the virtual form factor, designed to deliver deployment flexibility across a wide range of infrastructure environments. This unified licensing approach allows a single set of PIDs to entitle both virtual and containerized deployments across public and private cloud environments.

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
FTDc5	100 Mbps	50 Sessions
FTDc10	1 Gbps	250 Sessions
FTDc20	3 Gbps	250 Sessions
FTDc30	5 Gbps	250 Sessions
FTDc50	10 Gbps	750 Sessions
FTDc100	16 Gbps	10,000 Sessions
FTDcU (Unlimited)	No Rate Limiter	32,000 Sessions

Important: FTDc performance tiers have no impact on the underlying compute resources (vCPUs and memory) assigned to the container 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 container 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

Table 3. Deployment Environment Summary

Category	Supported Environment
Private Cloud/On-Premises	
Container runtime	Docker: 26.1.3+
Kubernetes version	Kubernetes – Min: 1.29.15, Max: 1.31.14
Operating System and Version	Ubuntu - Min: 20.04 LTS, Max: 22.04 LTS
CNI (Container Network Interface)	Macvlan, SR-IOV
Public Cloud	
AWS	EKS (Elastic Kubernetes Service) - Min: 1.30, Max: 1.31
System and Deployment Requirements	
Minimum System Requirements	4 vCPUs | 8 GB RAM | 50 GB Disk
Maximum System Requirements	32 vCPUs | 64 GB RAM | 500 GB Disk
Deployment Mode	Routed
High Availability	Planned for future release
Clustering	Planned for future release

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 4. Performance specifications for FTDc (Docker/Kubernetes) version 10.0+ running Snort3 and SR-IOV

Metric	4 x vCPU	8 x vCPU	12 x vCPU	16 x vCPU	32 x vCPU
Throughput: FW + AVC (1024B)	5Gbps	7.2Gbps	19Gbps	26Gbps	59Gbps
Throughput: FW + AVC + IPS (1024B)	4.5Gbps	7Gbps	18Gbps	25Gbps	55Gbps
IPSec VPN Throughput (1024B TCP w/ Fastpath)	2.2Gbps	3.2Gbps	7Gbps	10.5Gbps	35Gbps
Maximum concurrent sessions, with AVC	100K	250K	500K	2M	4M
Maximum new connections per second, with AVC	27K	44K	80K	135K	300K
Maximum VPN peers	250	250	750	10K	20K
Maximum Virtual Router Instances (VRF)	30	30	30	30	30
High Availability – Active/Standby	Planned for future release				
High Availability – Clustering	Planned for future release				

Ordering information

Performance tiered licensing is available starting from Firewall Threat Defense 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 5. Ordering information for Secure Firewall Threat Defense Container

Product ID	Description
FTDV-SEC-SUB	Secure Firewall Threat Defense Virtual/Container 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.