Cisco Secure Firewall Threat Defense Container

Contents

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) is the containerized solution for cloud firewall needs. It delivers the same robust security in container networks that enterprises have gotten used to in traditional data centers. 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 with top-tier security controls.

Product overview

Cisco Secure Firewall Threat Defense Container is a firewall that can be deployed and scaled in your container environments. Using the container form factor simplifies how you deploy, scale, and manage your container firewall. Secure Firewall Threat Defense Container gives you powerful stateful L3/L4 firewalling that can be configured to protect your network, your user access through the VPN, and how your containers access the rest of your network.

In addition to the stateful L3/L4 firewalling, Secure Firewall Threat Defense Container includes powerful VPN capabilities with policy consistency that simplifies how you manage your virtual, physical, and container Secure Firewall solutions. Cisco Smart Licensing makes it easy to deploy, manage, and track containerized instances of the appliance running in your private cloud or in a public cloud.

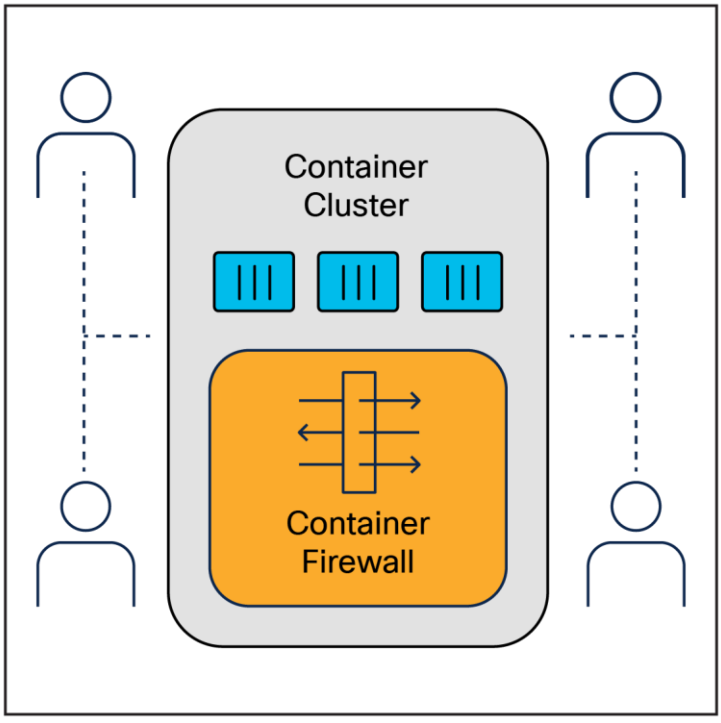

Figure 1.
Cisco Secure Firewall Threat Defense Container deployed into the public or private cloud

Benefits

L3/4 firewalling

Cisco Secure Firewall Threat Defense Container provides L3/L4 firewalling to achieve robust security and traffic management. It provides efficient traffic control by enabling customers to filter and manage network traffic with precision, allowing only authorized data packets to pass through, thus securing your container environments from unauthorized access. It also provides scalable network segmentation by allowing network segmentation into secure zones, applying tailored security policies to protect sensitive workloads and enhance overall security posture.

VPN head-end

Cisco Secure Client empowers employees to work from home (or anywhere) on any device at any time, securely. You can give any user highly secure access to your enterprise network and provide visibility and control to your IT and security teams to identify who and which devices are accessing the infrastructure. And you alleviate strain on your IT and security teams as they support offsite workers and personal devices. Cisco Secure Firewall Threat Defense Container supports site-to-site VPN for connecting your data centers.

License portability across clouds

Deploy Cisco Secure Firewall Threat Defense Container everywhere—from your data center to your branch office, to a public cloud— with the portability of one license across public or private clouds (VMware, Kernel-based Virtual Machine [KVM] and Hyper-V, OpenStack, Amazon Web Services [AWS], Microsoft Azure, Google Cloud Platform [GCP], Oracle Cloud Infrastructure [OCI] and government clouds). Expand, contract, and relocate workloads over time spanning private and public cloud infrastructures with one license.

Low-touch deployment

Rapidly deploy additional Cisco Secure Firewall Threat Defense Container appliances to your container clusters to support unplanned or seasonal surges on your applications or VPN. Add more bandwidth or protection for remote offices by spinning up a new virtual machine. Choose from higher-performance model options if you need more protection.

Smart Software Licensing

Cisco Smart Licensing makes it easier to buy, deploy, track, and renew Cisco licenses. You will enjoy:

- Simpler purchase and activation of the virtual appliance
- Easier license management and reporting of virtual appliances due to license pooling
- Automatic license activation when the virtual appliance is provisioned

Customers, select partners, and Cisco can view product entitlements and services in the Cisco Smart Software Manager. Configuration and activation are done with a single token. Cisco Secure Firewall Threat Defense Container will self-register with a Cisco server in the cloud, eliminating the need to register products with Product Activation Keys (PAKs). Instead of using PAKs or license files, Smart Software Licensing establishes a pool of software licenses or entitlements that can be used across your organization. When a virtual appliance is instantiated on a customer's premises, an entitlement is subtracted from the pool. When a virtual appliance is decommissioned, or when it is uninstantiated within the Smart Software Manager, an entitlement is added to the pool.

With the Smart Software Manager, you can manage license deployments throughout your organization easily and quickly. You can also manage multiple products from Cisco that support Smart Software Licensing.

Cisco Secure Firewall Threat Defense Container uses Smart Software Licensing exclusively. Older forms of licensing are not supported.

Any Cisco Secure Firewall Threat Defense Container license can be used on any supported FTDc vCPU/memory configuration. This functionality allows customers to run on a wide variety of VM resource footprints. This also increases the number of supported AWS, Azure, GCP, and OCI instance types. When configuring the Cisco Secure Firewall Threat Defense Container VM, the maximum supported number of vCPUs is 16, and the maximum supported memory is 128GB RAM.

Table 1. Standalone FTDc on K8s and Docker

Standalone FTDc	
FTDc vCPU/Mem	**1vCPU/2GB**
Stateful inspection throughput (maximum)[1]	1 Gbps
Throughput: FW (450B)	500 Mbps
IPsec VPN throughput (AES 450B UDP test)[2]	250 Mbps
Connections per second	6000
Concurrent sessions	100,000
VLANs	50
Bridge groups	25
IPsec VPN peers	250
Cisco Secure Client or clientless VPN user sessions	250
Virtual CPU core allocation[3]	1
Memory allocation	2GB

[1] Stated resource allocation is required to achieve the documented performance metrics for each tier. Decreased allocations are supported but will result in lower performance

[2] Throughput measured with 1500B User Datagram Protocol (UDP) traffic measured under ideal test conditions.

[3] The VPN throughput and the number of sessions depend on the FTD device configuration and VPN traffic patterns. These elements should be taken into consideration as part of your capacity planning

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-5121851-00 04/25