The bridge to possible

Data sheet
Cisco public

Cisco Secure Firewall Threat Defense Virtual (formerly FTDv/NGFWv)

Contents

Today, organizations rely on a mixture of physical and virtual control points to meet their network security needs. They need the flexibility to deploy different physical and virtual firewalls across a wide range of environments while still maintaining consistent policy across branch offices, corporate datacenters, and all points between. From data center consolidation to office relocations, mergers and acquisitions, as well as seasonal peaks in demand on your applications, Cisco's virtual firewall portfolio helps you simplify security management with the convenience of unified policy and the flexibility to deploy everywhere.

Cisco® Secure Firewall Threat Defense Virtual (formerly FTDv/NGFWv) combines Cisco's proven network firewall with Snort IPS, URL filtering, and malware defense. It simplifies threat protection with consistent security policies across physical, private, and public cloud environments. Get deep visibility into your network and quickly detect threat origin and activity. Then, stop attacks before they impact your operations.

Product overview

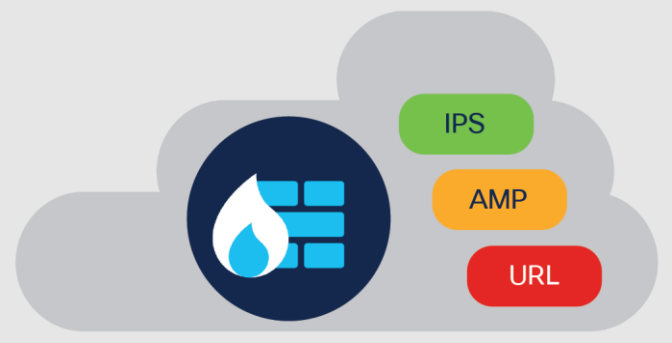

Figure 1.
Cisco Secure Firewall Threat Defense Virtual overview

Secure Firewall Threat Defense Virtual is the virtualized option of our popular Secure Firewall Threat Defense (formerly FTD) solution. Prioritize threats with automated risk rankings and impact flags to focus your resources on events requiring immediate action. License portability provides flexibility to move from your on-premises private cloud to public cloud while maintaining consistent policy and unified management across all of your appliances. Cisco Smart Software Licensing makes it easy to deploy, manage, and track virtual firewall instances.

Benefits

Automated risk ranking and impact flags

Prioritize threats by gaining comprehensive visibility of your environment. Reduce the noise and volume of events to focus on high-impact alerts requiring immediate action. Set rule recommendations that correlate host profiles with a level of vulnerability to automate impact analysis and contextualize the data, leveraging the best-of-breed Snort 3 IPS.

License portability across clouds

Deploy appliances everywhere, from your data center to your branch office, with the portability of one license to support virtual and physical solutions across public or private clouds (VMware, KVM, OpenStack, Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI), government clouds) and hyperconverged infrastructure (Cisco HyperFlex, Nutanix AHV). Expand, contract, and relocate workloads over time spanning physical, virtual, and public cloud infrastructures with one license.

Unified management and automated threat correlation

Stop more threats by containing known and unknown malware with our IPS license, Malware Defense license and URL Filtering license. Reduce the complexity of managing multiple security products through a unified management of integrated tools.

Features and specifications

Table 1. Features and specifications for Secure Firewall Threat Defense Virtual

Features	Specifications
Cisco Firewall device manager (local management)	ESXi, KVM and Openstack: Version 7.0 and above; Azure: Version 6.5 and above; AWS: 6.6 and above, Cisco Hyperflex: Version 7.0 and above; Nutanix AHV: Version 7.0 and above
Centralized management	Centralized configuration, logging, monitoring, and reporting are performed by the Cisco Firewall Management Center (all platforms including on-premises and in AWS, Azure, GCP and OCI(6.7 and above)) or alternatively in the cloud with Cisco Defense Orchestrator (ESXi and KVM; Azure: Version 6.5 and above, Cisco Hyperflex: Version 7.0 and above; Nutanix AHV: Version 7.0 and above)
Application Visibility and Control (AVC)	Standard, supporting more than 4000 applications, as well as geolocations, users, and websites
AVC: OpenAppID support for custom, open-source, application detectors	Standard
Cisco Security Intelligence	Standard, with IP, URL, and DNS threat intelligence
IPS license for Cisco Secure Firewall	Available; Snort 3 IPS can passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC)
Malware Defense license for Cisco Secure Firewall	Available; enables detection, blocking, tracking, analysis, and containment of targeted and persistent malware, addressing the attack continuum both during and after attacks. Integrated threat correlation with Cisco Secure Endpoint is also optionally available.

Features	Specifications
Cisco Secure Malware Analytics sandboxing	Available
URL filtering: number of categories	More than 80
URL filtering: number of URLs categorized	More than 280 million
Automated threat feed and IPS signature updates	Yes: Class-leading Collective Security Intelligence (CSI) from the Cisco Talos® group (https://www.cisco.com/c/en/us/products/security/talos.html)
Third-party and open-source ecosystem	Open API for integrations with third-party products; Snort® and OpenAppID community resources for new and specific threats
High availability and clustering	Active/standby (ESXi and KVM only)
Deployment modes	Routed, transparent (inline set – IPS-only), and passive; AWS, Azure, GCP and OCI: routed mode only

Note: Performance will vary depending on features activated, network traffic protocol mix, and packet size characteristics. Performance is subject to change with new software releases. Consult your Cisco representative for detailed sizing guidance.

Product performance guidelines

Note: Your performance may vary from the below. These should be considered general guidelines. Your actual performance will depend on your test environment, including CPU type, CPU speed, cache, number of interfaces, etc.

Table 2. Performance specifications for Secure Firewall Threat Defense Virtual (ESXi/KVM/OpenStack) version 7.0 and later

License Type	FTDv5 (100M)	FTDv10 (1G)	FTDv20 (3G)	FTDv30(5G)	FTDv50(10G)	FTDv100(16G)
Specification	**4 vCPU**	**4 vCPU**	**4 vCPU**	**8 vCPU**	**12 vCPU**	**16 vCPU**
Throughput: FW + AVC (1024B)	100 Mbps	1 Gbps	3 Gbps	5.5 Gbps	10 Gbps	15.5 Gbps
Throughput: FW + AVC + IPS (1024B)	100 Mbps	1 Gbps	3 Gbps	5.5 Gbps	10 Gbps	15.5 Gbps
Throughput: FW + AVC (450B)	100 Mbps	1 Gbps	1.5 Gbps	3 Gbps	5 Gbps	7 Gbps
Throughput: FW + AVC + IPS (450B)	100 Mbps	1 Gbps	1 Gbps	2 Gbps	3 Gbps	7 Gbps
Maximum concurrent sessions	100,000	100,000	100,000	250,000	500,000	2,000,000
Maximum new connections per second	12,500	20,000	20,000	20,000	40,000	130,000

License Type	FTDv5 (100M)	FTDv10 (1G)	FTDv20 (3G)	FTDv30(5G)	FTDv50(10G)	FTDv100(16G)
Specification	**4 vCPU**	**4 vCPU**	**4 vCPU**	**8 vCPU**	**12 vCPU**	**16 vCPU**
Maximum VPN peers	250	250	250	250	750	10,000
IPSec VPN throughput(1024B) TCP w/Fastpath)	100 Mbps	1 Gbps	1.1 Gbps	2 Gbps	4 Gbps	6 Gbps 8 Gbps with QAT(ESXi/KVM)

Table 3. Performance specifications for Threat Defense Virtual 7.0 and later – AWS*

License Type	FTDv5 (100M)	FTDv10 (1G)	FTDv20 (3G)	FTDv30 (5G)	FTDv50 (10G)	FTDv100 (16G)
AWS Instance type	**c5.xlarge**	**c5.xlarge**	**c5.xlarge**	**c5.2xlarge**	**c5.4xlarge**	**c5.4xlarge**
Throughput: FW + AVC (1024B)	100 Mbps	1 Gbps	2.2 Gbps	4.3 Gbps	8.6 Gbps	8.6 Gbps
Throughput: FW + AVC + IPS (1024B)	100 Mbps	1 Gbps	2.2 Gbps	4.3 Gbps	8.4 Gbps	8.4 Gbps
Throughput: FW + AVC (450B)	100 Mbps	1 Gbps	830 Mbps	1.4 Gbps	3.8 Gbps	3.8 Gbps
Throughput: FW + AVC + IPS (450B)	100 Mbps	1 Gbps	830 Mbps	1.4 Gbps	3.2 Gbps	3.2 Gbps
Maximum concurrent sessions	100,000	100,000	100,000	200,000	2M	2M
Maximum new connections per second	24,500	24,500	24,500	45,900	82,800	82,800
Maximum VPN peers	250	250	250	250	750	10,000
IPSec VPN throughput(1024B) TCP w/Fastpath)	100 Mbps	1 Gbps	1.4 Gbps	1.4 Gbps	4 Gbps	4 Gbps

* For non-tiered licenses the performance for 4vCPU instances matches FTDv20, performance of 8vCPU matches the FTDv30 and the performance of 16 vCPU instances matches FTDv100.

Table 4. Performance specifications for Threat Defense Virtual 7.0 and later- Azure*

License type	FTDv5 (100M)	FTDv10 (1G)	FTDv20 (3G)	FTDv30(5G)	FTDv50 (10G)	FTDv100 (16G)
Azure VM type	**D3_v2, D3**	**D3_v2**	**D3_v2**	**D4_v2**	**D5_v2**	**D5_v2**
Throughput: FW + AVC (1024B)	100 Mbps	1 Gbps	1.4 Gbps	1.5 Gbps	5.0 Gbps	5.0 Gbps
Throughput: FW + AVC + IPS (1024B)	100 Mbps	1 Gbps	1.4 Gbps	1.5 Gbps	4.5 Gbps	4.5 Gbps
Throughput: FW + AVC (450B)	100 Mbps	700 Mbps	700 Mbps	940 Mbps	1.0 Gbps	1.0 Gbps
Throughput: FW + AVC + IPS (450B)	100 Mbps	700 Mbps	700 Mbps	920 Mbps	1.0 Gbps	1.0 Gbps
Maximum concurrent sessions	100,000	100,000	100,000	250,000	1.5M	1.5M
Maximum new connections per second	11,550	11,550	11,550	12,480	14,540	14,540
Maximum VPN peers	250	250	250	250	750	10,000
IPSec VPN throughput (1024B) TCP w/Fastpath)	100 Mbps	830 Mbps	830 Mbps	1.6 Gbps	4 Gbps	4 Gbps

* Measured on virtual machines with Accelerated Networking (AN) enabled. For non-tiered licenses the performance for 4vCPU virtual machine type matches FTDv20, performance of 8vCPU matches the FTDv30 and the performance of 16 vCPU matches FTDv100.

Table 5. Performance specifications for Threat Defense Virtual 7.0 and later- GCP*

License type	FTDv5 (100M)	FTDv10 (1G)	FTDv20 (3G)	FTDv30 (5G)	FTDv50 (10G)	FTDv100 (16G)
GCP machine type	**c2-standard-4**	**c2-standard-4**	**c2-standard-4**	**c2-standard-8**	**c2-standard-16**	**c2-standard-16**
Throughput: FW + AVC (1024B)	100 Mbps	1 Gbps	1.5 Gbps	5 Gbps	9.9 Gbps	9.9 Gbps
Throughput: FW + AVC + IPS (1024B)	100 Mbps	1 Gbps	1.4 Gbps	5 Gbps	9.7 Gbps	9.7 Gbps
Throughput: FW + AVC (450B)	100 Mbps	450 Mbps	450 Mbps	1.7 Gbps	2.3 Gbps	2.3 Gbps
Throughput: FW + AVC + IPS (450B)	100 Mbps	450 Mbps	450Mbps	1.2 Gbps	2 Gbps	2 Gbps
Maximum concurrent sessions	100,000	100,000	100,000	250,000	2M	2M
Maximum new connections per second	12,000	12,000	12,000	45,000	84,000	84,000
Maximum VPN peers	250	250	250	250	750	10,000

License type	FTDv5 (100M)	FTDv10 (1G)	FTDv20 (3G)	FTDv30 (5G)	FTDv50 (10G)	FTDv100 (16G)
GCP machine type	c2-standard-4	c2-standard-4	c2-standard-4	c2-standard-8	c2-standard-16	c2-standard-16
IPSec VPN throughput (1024B) TCP w/Fastpath)	100 Mbps	1 Gbps	1.5 Gbps	1.5 Gbps	4 Gbps	4 Gbps

* For non-tiered licenses the performance for 4vCPU machine type matches FTDv20, performance of 8vCPU matches the FTDv30 and the performance of 16 vCPU matches FTDv100

Table 6. Performance specifications for Threat Defense Virtual 7.0 and later- OCI*

License type	FTDv5 (100M)	FTDv10 (1G)	FTDv20 (2G)/ FTDv 30(5G)	FTDv50 (10G)	FTDv100 (16G)
OCI Shape type	VM.Standard2.4	VM.Standard2.4	VM.Standard2.4	VM.Standard2.8	VM.Standard2.8
Throughput: FW + AVC (1024B)	100 Mbps	1 Gbps	1.2 Gbps	2.4 Gbps	2.4 Gbps
Throughput: FW + AVC + IPS (1024B)	100 Mbps	1 Gbps	1.2 Gbps	2.4 Gbps	2.4 Gbps
Throughput: FW + AVC (450B)	100 Mbps	410 Mbps	410 Mbps	920 Mbps	920 Mbps
Throughput: FW + AVC + IPS (450B)	100 Mbps	390 Mbps	390 Mbps	910 Mbps	910 Mbps
Maximum concurrent sessions	250,000	250,000	250,000	2M	2M
Maximum new connections per second	4900	4900	4900	10,000	10,000
Maximum VPN peers	250	250	250	750	10,000
IPSec VPN throughput (1024B) TCP w/Fastpath)	100 Mbps	1 Gbps	1.2 Gbps	1.5 Gbps	1.5 Gbps

* Measured with paravirtualized interfaces. For non-tiered licenses the performance for 4 OCPU shape types matches FTDv30, performance of 8OCPU shape types matches the FTDv100.

System requirements

Table 7. System requirements for Secure Firewall Threat Defense Virtual

Specification	Description
VMware and KVM: Virtual CPUs and memory (6.4 and above)	• 4 vCPU/8GB • 8 vCPU/16GB • 12 vCPU/24GB • 16vCPU/32GB (Threat Defense Virtual Version 7.0 and above)
VMware and KVM: Virtual CPUs and memory (6.3 and earlier)	4 vCPU/8GB
VMware and KVM: Intel QuickAssist Technology(QAT) support(7.0 and above)	Intel QAT 8970 PCI adapter certified on UCS M5 servers. Supported for FTDv100 only.
Storage	50GB for all FTDv configurations
Hypervisor support	ESXi 6.0, 6.5, 6.7, 7.0; KVM, Openstack, Nutanix AHV: AOS version 5.20, AHV Version 20201105.2030. Cisco Hyperflex: Data Platform version 4.5.1a-39020
AWS Support	• Instances: c3.xlarge, c4.xlarge • Instances: c5.xlarge, c5.2xlarge, & c5.4xlarge (6.6 and above) • Gov Marketplace • China Marketplace • Auto-Scale • Enhanced Networking
Azure Support	• Instances: D3, D3_v2, • Instances: D4_v2 and D5_v2 (6.5 and above) • Gov Marketplace • China Marketplace • Auto-Scale • Accelerated Networking
GCP Support (6.7 and above)	• Instances: c2-standard-4, c2-standard-8, c2-standard-16, n1-standard-4, n1-standard-8, n1-standard-16, n2-standard-4, n2-standard-8, n2-standard-16, n1-highcpu-8, n2-highcpu-8, n1-highcpu-16, n2-highmem-4, n2-highmem-8, n2-highmem-16, n2-highcpu-16
OCI Support (6.7 and above)	• Instances: VM.Standard2.4, VM.Standard2.8

Ordering information

Table 8. Ordering information for Secure Firewall Threat Defense Virtual version 7.0 (Tiered licenses)

Part number	Description
FTDV-SEC-SUB	Cisco Firepower TD Virtual Subscription
Once the above PID is selected, you can choose from the following Tiered Base and Tiered Threat, Malware and URL Filtering Subscriptions	
FTD-V-(X)S-BSE-K9*	Cisco Firepower TD Virtual Base License
FTD-V-(X)S-T*	Cisco Firepower TD Virtual Threat Protection
FTD-V-(X)S-TM*	Cisco Firepower TD Virtual Threat and Malware Protection
FTD-V-(X)S-TC*	Cisco Firepower TD Virtual Threat Protection and URL
FTD-V-(X)S-TMC*	Cisco Firepower TD Virtual Threat, Malware, and URL Filtering
FTD-V-(X)S-AMP*	Cisco Firepower TD Virtual Malware Protection
FTD-V-(X)S-URL*	Cisco Firepower Threat Defense Virtual URL Filtering

*'X' denotes the specific tier model number 5,10,20,30,50 and 100

Table 9. Ordering information for non-Tiered Secure Firewall Threat Defense Virtual licenses

Part number	Description
FPRTD-V-K9	Cisco Firepower Threat Defense (TD) Virtual Appliance
L-FPRTD-V-T	Cisco Firepower TD Virtual Threat Protection
L-FPRTD-V-TM	Cisco Firepower TD Virtual Threat and Malware Protection
L-FPRTD-V-TC	Cisco Firepower TD Virtual Threat Protection and URL
L-FPRTD-V-TMC	Cisco Firepower TD Virtual Threat, Malware, and URL Filtering
L-FPRTD-V-AMP	Cisco Firepower TD Virtual Malware Protect
L-FPRTD-V-URL	Cisco Firepower Threat Defense Virtual 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 "Environment 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.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

The Cisco Security Advantage

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. The latest generation of Cisco Secure Firewallshas the power and flexibility that you need to stay one step ahead of threats. With Cisco Secure Firewall, you're investing in a foundation for security. Every Secure Firewall includes entitlement for Cisco SecureX, providing unified visibility across all Cisco security products, giving you security that is both agile and integrated.

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 C78-742858-09 06/21