Cisco Firepower NGFW Virtual (NGFWv) Appliance

Contents

Cisco Firepower NGFW Virtual (NGFWv) Appliance

The Cisco® Next-Generation Firewall (NGFW) portfolio enables you to protect your workloads from an increasingly complex set of threats while delivering consistent security policies, visibility, and improved threat response. From your data center, branch offices, cloud environments, and everywhere in between, leveraging the power of Cisco turns your existing network infrastructure into an extension of your firewall solution, leading to adaptive security everywhere you need it. Our world-class NGFW sets the foundation for consistent visibility, policy harmonization, and unified management. Cisco Threat Response automates integrations across the entire Cisco security portfolio so you can rapidly detect, investigate, and remediate threats.

The physical and virtual Cisco Firepower NGFW appliances offer the same threat protection features, resulting in consistent security effectiveness and visibility across physical and virtual workloads.

The Cisco Firepower® NGFWv is available on VMware, KVM, Amazon Web Services (AWS), and Microsoft Azure environments for virtual, public, private, and hybrid cloud deployments. Organizations employing a software-defined network can rapidly provision and orchestrate flexible network protection with Cisco Firepower NGFWv. As well, organizations using network function virtualization can further lower costs by avoiding upfront network infrastructure costs when utilizing Cisco Firepower NGFWv.

Features and benefits

Table 1. Features and benefits for NGFWv

Features	Benefits
Cisco Firepower Device Manager (local management)	Yes (ESXi and KVM only)
Centralized management	Centralized configuration, logging, monitoring, and reporting are performed by the Cisco Firepower Management Center (all platforms including on-premises and in AWS and Azure) or alternatively in the cloud with Cisco Defense Orchestrator (ESXi and KVM only)
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
Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS)	Available; can passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence
Cisco Advanced Malware Protection (AMP) for Networks	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 AMP for Endpoints is also optionally available.
Cisco AMP Threat Grid sandboxing	Available
URL filtering: number of categories	More than 80

Features	Benefits
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
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

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 NGFWv

Specification	4 vCPU	8 vCPU	12 vCPU
Throughput: FW + AVC (1024B)	3 Gbps	5.5 Gbps	10 Gbps
Throughput: FW + AVC + IPS (1024B)	3 Gbps	5.5 Gbps	10 Gbps
Throughput: FW + AVC (450B)	1.5 Gbps	3 Gbps	5 Gbps
Throughput: FW + AVC + IPS (450B)	1 Gbps	2 Gbps	3 Gbps
Maximum concurrent sessions	100,000	250,000	500,000
Maximum new connections per second	20,000	20,000	40,000
Throughput: NGIPS (1024B)	3 Gbps	5 Gbps	10 Gbps
Throughput: NGIPS (450B)	1 Gbps	2.5 Gbps	5 Gbps
Maximum VPN peers	250	250	750

System requirements

Table 3. System requirements for NGFWv

Specification	Description
Virtual CPUs and memory (6.4 and later)	● 4 vCPU/8GB ● 8 vCPU/16GB ● 12 vCPU/24GB
Virtual CPUs and memory (6.3 and earlier)	4 vCPU/8GB
Storage	50GB for all FTDv configurations
Hypervisor support	ESXi 6.0 and 6.5; KVM
Public cloud support	● AWS (c3.xlarge and c4.xlarge) ● Azure (Standard_D3, Standard_D3_V2)

Ordering information

Table 4. Ordering information for NGFWv

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.

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 Firepower NGFWs has the power and flexibility that you need to stay one step ahead of threats. With Cisco NGFW, you're investing in a foundation for security that is both agile and integrated—leading to the strongest security posture available today and tomorrow.

Connection™
we solve IT™

Contact an Account Manager for more information.
1.800.800.0014 ■ www.connection.com/Cisco

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

Printed in USA C78-742858-00 09/19