Cisco NGIPSv for VMware

Product Overview

Industry-leading threat protection. Real-time contextual awareness. Full-stack visibility. Intelligent security automation. Together they equal security you can count on when using Cisco® NGIPSv for VMware, the virtualized offering of the Cisco FirePOWER™ next-generation IPS (NGIPS) solution. This highly effective intrusion prevention system provides reliable performance and a low total cost of ownership. Threat protection can be expanded with optional subscription licenses to provide Advanced Malware Protection (AMP), application visibility and control, and URL filtering capabilities. Cisco FirePOWER appliances set the industry benchmark for threat detection effectiveness, inspected throughput, and value as measured by studies conducted by NSS Labs, the world's leading information security research and advisory company.

The Benefits of a Virtualized Solution

Server virtualization brings significant business benefits. It is capable of reducing costs, enabling rapid deployment, and improving system availability. Yet implementing virtualization introduces potential security risks:

- “Blind spots” are created because changes in topology or configuration will not be detected.
- Functions are consolidated that other groups previously managed separately, such as networking or security, which can lead to configuration mistakes.
- Virtual machines (VMs) quickly propagate without adequate coordination or oversight, a problem known as VM sprawl.

Cisco NGIPSv for VMware addresses the risks posed by virtualization by enabling you to deploy Cisco’s leading NGIPS solution within your virtual environments. This virtualized NGIPS is able to inspect traffic between virtual machines and make it easier to deploy and manage NGIPS solutions at remote sites where resources may be limited, increasing protection for both physical and virtual assets.

Reclaim the Visibility Lost When Virtualizing

The dynamic nature of virtual networks regularly involves changes to the virtual network’s topology as well as configuration changes to individual virtualized hosts. Unfortunately, most systems management solutions are blind to these changes. If the changes are done incorrectly, either on purpose or accidentally, security exposures can be introduced into your critical processing environments without your knowledge.

For example, two different virtual networks are deployed on the same physical host. One is a production environment, and the other is a development environment that contains source code for the production environment. Due to misconfiguration or an inadvertent policy violation, these two virtual networks become connected: a major security exposure but one that’s invisible to the outside world.

Cisco NGIPSv for VMware will alert you to these changes so that misconfigurations and violations of policy can be addressed before they become problems. It also provides threat protection by identifying and blocking any malicious traffic between your virtualized networks and individual VMs. Cisco NGIPSv for VMware provides visibility into your virtualized world so that you can better control and secure this critical part of your processing environment.

Deploy Protection Easier and Wider

The dedicated hardware used by physical appliances, while especially valuable for high-performance deployments such as data centers, have additional costs associated with them and may not meet every use case. Physical appliances must be shipped to their eventual location. Some international destinations have challenging customs requirements for hardware that incur significant costs or delays. Rack space and power must be allocated. Finally, some environments have stringent hardware requirements, either because of required certification or hostile operating conditions.

Because virtual appliances are software-based, Cisco NGIPSv for VMware is able to satisfy NGIPS deployment use cases that physical appliances cannot, and with lower operating costs. It can:

- Be deployed in existing hardware and start monitoring traffic right away
- Monitor locations where IT security resources do not exist
- Monitor network segments where deployment of physical appliances is impractical (e.g., retail locations, remote offices)
- Maintain separation of duties because security analysts can manage both physical and virtual NGIPS appliances from the same Cisco FireSIGHT™ Management Center

Extend Payment Card Industry (PCI) Compliance to Virtual Environments

"Securing Virtual Payment Systems," an information supplement from the Virtualization Special Interest Group (SIG) of the PCI Security Standards Council, provides clear guidance for how to achieve and maintain PCI compliance in virtual environments. The new guidance is far-reaching and establishes specific security recommendations for virtualized cardholder data environments (CDEs). Recommendations include:

- Network security must now be specifically applied to virtual environments
- The use of an intrusion detection system (IDS) or IPS to monitor critical points within the CDE is mandated (PCI Requirement 11.4)
- IDS and IPS tools should be able to monitor virtual networks and traffic between VMs

Cisco NGIPSv for VMware monitors critical virtual networks containing cardholder data or personally identifiable information (PII) and inspects traffic between VMs. It provides the same NGIPS control and protection as its physical counterpart. Cisco NGIPSv provides inspection using up to 8 vCPUs and supports VMware ESXi 5.x platforms.

PCI Requirement 6.3.2 also requires that development, test, and production environments must be isolated from one another. Cisco NGIPSv for VMware helps to provide compliance with this requirement because it will produce alerts if it sees any traffic between these networks.

Cisco NGIPSv for VMware Applicability

- PCI-critical servers, small branch offices, and remote locations (e.g., retail stores)
- Organizations with distributed IT security organizations
- Environments with hardware restrictions (e.g., mobile vehicles, military ships, outdoor deployments)
- Organizations with lengthy hardware certification requirements
- Environments with space constraints (little rack space remains in the data center)
- Expanded real-time network, user, and VM discovery

- Lab or training networks
- Managed security service provider or cloud computing environments

System Requirements

Table 1 shows the minimum requirements for Cisco NGIPSv for VMware.

Table 1. System Requirements

Hypervisor	VMware ESX 5.0, 5.1
CPU	4 vCPU
Memory	4 GB
Disk Space	40 GB
Network Interface	Minimum 2 vNICs, maximum 10 vNICs

Warranty Information

Find warranty information on Cisco.com on the Product Warranties page.

Ordering Information

Help customers understand all the components or parts they need to purchase in order to install and use the product. See Table 2 for part numbers. This section also provides a direct link to the Cisco Ordering Tool and lists part numbers for customer convenience.

To place an order, go to How to Buy. You can download software here.

Table 2. Ordering Information

Product Name	Part Number
Cisco FirePOWER Virtual Appliance and Support Bundle	FP-VMW-IPS-BUN
Cisco FirePOWER Virtual IPS and Apps 1YR Service Subs	FP-VMW-TA-1Y
Cisco FirePOWER Virtual IPS and Apps 3YR Service Subs	FP-VMW-TA-3Y
Cisco FirePOWER Virtual IPS, Apps and URL 1YR Service Subs	FP-VMW-TAC-1Y
Cisco FirePOWER Virtual IPS, Apps and URL 3YR Service Subs	FP-VMW-TAC-3Y
Cisco FirePOWER Virtual IPS, Apps and AMP 1YR Service Subs	FP-VMW-TAM-1Y
Cisco FirePOWER Virtual IPS, Apps and AMP 3YR Service Subs	FP-VMW-TAM-3Y
Cisco FirePOWER Virtual IPS, Apps, AMP and URL 1YR Svc Subs	FP-VMW-TAMC-1Y
Cisco FirePOWER Virtual IPS, Apps, AMP and URL 3YR Svc Subs	FP-VMW-TAMC-3Y
Cisco AMP for FirePOWER Virtual Appl. 1YR Svc Subscription	FP-VMW-AMP-1Y
Cisco AMP for FirePOWER Virtual Appl. 3YR Svc Subscription	FP-VMW-AMP-3Y
Cisco FirePOWER Virtual Appl. URL Filtering 1Y Service Subs	FP-VMW-URL-1Y
Cisco FirePOWER Virtual Appl. URL Filtering 3Y Service Subs	FP-VMW-URL-3Y

For More Information

To learn more about any of the Cisco NGIPSv for VMware please visit http://www.cisco.com/c/en/us/products/security/index.html or contact your local account representative.

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 www.cisco.com/go/offices.

Printed in USA C78-733165-00 11/14