

Cisco ASA 1000V Cloud Firewall

Product Overview

The Cisco® ASA 1000V Cloud Firewall extends the proven Adaptive Security Appliance security platform to consistently secure the tenant edge in multitenant private and public cloud deployments. Complementing the zone-based security capabilities of the Cisco Virtual Security Gateway (VSG), the Cisco ASA 1000V Cloud Firewall provides multitenant edge security, default gateway functionality, and protection against network-based attacks, for a comprehensive cloud security solution. The Cisco ASA 1000V Cloud Firewall integrates with the Cisco Nexus® 1000V Series Switch to offer a multi-hypervisor-capable solution and enable a single ASA 1000V instance to secure multiple ESX hosts for superior deployment flexibility and simplified management. Cisco Virtual Network Management Center (VNMC) is used to offer dynamic, policy-driven, multitenant management.

Features and Benefits

The Cisco ASA 1000V Cloud Firewall employs mainstream ASA security technology that has been optimized for virtual environments. It transparently integrates with Cisco Nexus 1000V, VSG, and VNMC components, and works in conjunction with physical ASA appliances to provide end-to-end security for hybrid (physical, virtual, cloud) infrastructures. The features and benefits are detailed in Table 1.

Table 1. Cisco ASA 1000V Cloud Firewall Features and Benefits

Feature	Benefit
Proven firewall to secure private and public clouds	<ul style="list-style-type: none"> • Extends proven ASA capabilities to secure the multitenant virtual and cloud infrastructure at the edge • Secures the cloud perimeter against network-based attacks • Supports consistent capabilities across hybrid infrastructures: physical, virtual, and cloud • Uses the most widely deployed secure connectivity solution that reliably extends IT infrastructure to the cloud and transfers mission-critical workloads between distributed locations without compromise
Increased solution flexibility and operational efficiency	<ul style="list-style-type: none"> • Provides deployment flexibility and simpler management with distinctive capabilities for a single ASA 1000V instance to span multiple ESX hosts • Enables consistency and flexibility with a multi-hypervisor-capable solution • Supports enhanced scalability by providing VXLAN gateway capabilities • Enhances efficiency and simplifies management with security policies organized into templated edge profiles • Captures operational efficiency with an option to support consistent address space between the existing physical and extended cloud infrastructure, or between multiple tenants within the cloud infrastructure • Decreases end-to-end time to deploy a fully functional virtual machine by automatically provisioning IP addresses to virtual machines at a rapid pace • Enhances management flexibility through XML APIs that support integration with third-party management and orchestration tools
Comprehensive approach to new virtualization workflows	<ul style="list-style-type: none"> • Employs an advanced, cloud-ready manager, offering a transparent, scalable, multitenant-capable, policy-based solution, for end-to-end security of virtual and cloud environments • Helps ensure collaborative governance with role-relevant management interfaces for network, server, and security administrators

Dynamic Virtualization-Aware Operation

Virtualization can be highly dynamic, with frequent add, delete, and change operations on virtual machines. Live migration of virtual machines occurs through manual or programmed VMware vMotion events. The Cisco ASA 1000V Cloud Firewall operates in conjunction with the Cisco Nexus 1000V Series (and vPath) to support dynamic virtualization, and in conjunction with the Cisco VNMC to create edge profiles per line of business or tenant.

Security profiles are bound to Cisco Nexus 1000V Series port profiles, which are authored on the Cisco Nexus 1000V Series Virtual Supervisor Module (VSM) and published to VMware vCenter. When a new virtual machine is instantiated, the server administrator assigns the appropriate port profile to the virtual machine's virtual Ethernet port. The port and edge profiles are immediately applied to the instantiated virtual machine. A virtual machine can be repurposed simply by assigning different port and edge profiles.

VMware vMotion events trigger movement of virtual machines across physical servers. The Cisco Nexus 1000V Series helps ensure that port and edge profiles both follow the virtual machine. Security enforcement and monitoring remain in place regardless of VMware vMotion events.

Solution Components

- **Integrates with the Nexus 1000V Series Switch:** The Cisco ASA 1000V Cloud Firewall secures virtualized environments using advanced networking concepts to provide efficient deployment and operational simplicity. Operating in conjunction with Cisco Nexus 1000V Series distributed virtual switches in the VMware vSphere hypervisor, the Cisco ASA 1000V Cloud Firewall uses virtual network service data path (vPath) technology embedded in the Nexus 1000V Series Switch.
 - **Efficient deployment:** Each Cisco ASA 1000V can provide protection across multiple physical servers, eliminating the need to deploy one virtual appliance per physical server.
 - **Independent capacity planning:** Cisco ASA 1000V can be placed on a dedicated server controlled by the security operations team so that appropriate computing capacity can be allocated to application workloads, capacity planning can occur independently across server and security teams, and operational segregation can be maintained across security, network, and server teams.
 - **Scalable cloud networking:** Cisco ASA 1000V acts as a VXLAN gateway to send traffic to and from the VXLAN to a traditional VLAN.
 - **Service chaining:** vPath supports service chaining so that multiple virtual network services can be used as part of a single traffic flow. For example, by merely specifying the network policy, vPath can direct the traffic to first go through the ASA 1000V Cloud Firewall, providing tenant edge security, and then go through the Virtual Security Gateway, providing zone firewall capabilities.
- **Integrates with Cisco VNMC:** The Cisco ASA 1000V Cloud Firewall is managed using the Cisco VNMC to provide a nondisruptive administration model.
 - Security administrators can author and manage security profiles and can manage Cisco ASA 1000V instances; security profiles are referenced in Cisco Nexus 1000V Series port profiles.
 - Network administrators can author and manage port profiles and can manage Cisco Nexus 1000V Series distributed virtual switches; port profiles are referenced in the VMware vCenter through the programmatic interface of the Cisco Nexus 1000V Series VSM.
 - Server administrators can select the appropriate port profile in the VMware vCenter when instantiating a virtual machine.

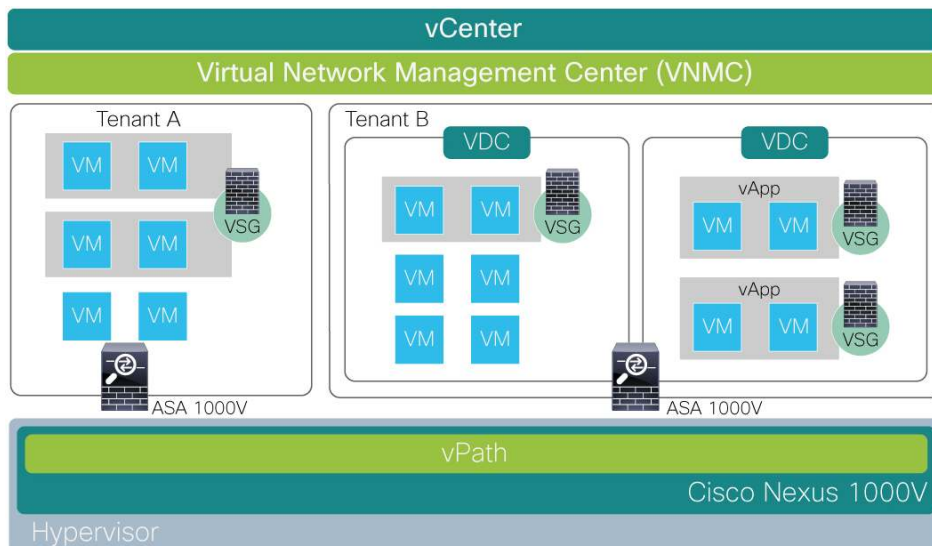
Additionally, third-party management and orchestration tools can interact programmatically, through XML APIs, with Cisco VNMC for automated management and provisioning of the Cisco VSG.

Cisco ASA 1000V Cloud Firewall can also be managed by Cisco Adaptive Security Device Manager (ASDM).

- **Complements Cisco VSG:** Cisco VSG integrates with Cisco Nexus 1000V Series Switches to provide granular, inter-VM-zone-based security within the tenant. The Cisco ASA 1000V Cloud Firewall complements Cisco VSG to provide multitenant edge security and default gateway functionality and protect against network-based attacks.

Figure 1 illustrates the integration of solution components.

Figure 1. Cisco ASA 1000V Cloud Firewall Solution Components



Software Packaging and Installation

Table 2 describes how to obtain the Cisco ASA 1000V Cloud Firewall

Table 2. Software Packaging and Installation

Package	Description
Open Virtualization Format (OVF)	<ul style="list-style-type: none"> • Downloadable OVF virtual appliance in the form of a single file with the .ova extension • Deployed with OVF Templates/Packages • Cisco ASA Software Release 8.7

Solution Deployment Requirements

The products listed in Table 3 must be deployed to secure virtualized and cloud environments using the Cisco ASA 1000V Cloud Firewall.

Table 3. Cisco ASA 1000V Cloud Firewall Deployment Requirements

Product	Requirement
Cisco ASA 1000V Cloud Firewall	Cisco ASA 1000V Cloud Firewall as a virtual appliance <ul style="list-style-type: none"> • 1 virtual CPU • vRAM: 1.5 GB • vHard disk: 2.5 GB • Network data interfaces: 2 • Management interface: 1 • High-availability interface: 1

Product	Requirement
Hypervisor and hypervisor management	<ul style="list-style-type: none"> VMware vSphere 4.1 or later releases with VMware ESX or ESXi VMware vCenter 4.1 or later releases
Distributed virtual switch	Cisco Nexus 1000V Series Software Release 4.2(1)SV1(4) or later, including the Virtual Ethernet Module (embedded in the VMware vSphere ESX or ESXi hypervisor); Essential edition or Advanced edition
Management	Cisco Virtual Network Management Center Release 2.0 or later (deployed as a virtual appliance)

Product Performance Guidance

Table 4 provides the performance guidance for a single instance of the Cisco ASA 1000V Cloud Firewall. Testing was conducted on a VMware ESX 5.0 host running on an Intel Xeon Processor X5670 (Westmere) at 2.93 GHz with dual hex-core. 1 vCPU, 1.5 GB vRAM, and 2.5 GB vHD are allocated to the ASA 1000V instance.

Table 4. Cisco ASA 1000V Cloud Firewall Performance Capabilities

Feature	Cisco ASA 1000V Cloud Firewall
Maximum Firewall Throughput (max)	1.2 Gbps
Maximum Firewall Throughput (multi-protocol)	400 Mbps
Maximum Concurrent Sessions	200,000
Maximum Connections per Second	10,000
VPN Throughput	200 Mbps
Maximum VPN Tunnels	750

Note: The performance capabilities of the ASA 1000V depend upon the deployment scenario, ASA 1000V device configuration, resources available to the ASA 1000V instance, and the traffic patterns. These elements should be taken into consideration as part of your planning.

Licensing and Ordering Information

Cisco ASA 1000V Cloud Firewall is licensed based on the number of physical server CPU sockets that are being protected. Each protected CPU also requires a Cisco Nexus 1000V Series license.

Table 5 lists ordering information for the Cisco ASA 1000V.

Table 5. Cisco ASA 1000V Cloud Firewall Ordering Information

Part Number	Description
ASA1000V-01=	ASA 1000V Paper CPU License Qty 1-Pack
ASA1000V-04=	ASA 1000V Paper CPU License Qty 4-Pack
ASA1000V-16=	ASA 1000V Paper CPU License Qty 16-Pack
ASA1000V-32=	ASA 1000V Paper CPU License Qty 32-Pack
L-ASA1000V-BASE	ASA 1000V eDelivery CPU License Qty 1-Pack
L-ASA1000V-04=	ASA 1000V eDelivery CPU License Qty 4-Pack
L-ASA1000V-16=	ASA 1000V eDelivery CPU License Qty 16-Pack
L-ASA1000V-32=	ASA 1000V eDelivery CPU License Qty 32-Pack
ASA1000V-K9-CD=	ASA 1000V on Physical Media

Table 6 lists ordering information for the Nexus 1000V Advanced Security bundle, which includes Nexus 1000V Advanced Edition and ASA 1000V licenses.

Table 6. Cisco Nexus 1000V Advanced Security Bundle Ordering Information

Part Number	Description
N1K-ASA1K-01	Nexus 1000V Advanced Edition and ASA 1000V Paper CPU License Qty 1-Pack
N1K-ASA1K-04	Nexus 1000V Advanced Edition and ASA 1000V Paper CPU License Qty 4-Pack
N1K-ASA1K-16	Nexus 1000V Advanced Edition and ASA 1000V Paper CPU License Qty 16-Pack
N1K-ASA1K-32	Nexus 1000V Advanced Edition and ASA 1000V Paper CPU License Qty 32-Pack
L-N1K-ASA1K-01	Nexus 1000V Advanced Edition and ASA 1000V eDelivery CPU License Qty 1-Pack
L-N1K-ASA1K-04	Nexus 1000V Advanced Edition and ASA 1000V eDelivery CPU License Qty 4-Pack
L-N1K-ASA1K-16	Nexus 1000V Advanced Edition and ASA 1000V eDelivery CPU License Qty 16-Pack
L-N1K-ASA1K-32	Nexus 1000V Advanced Edition and ASA 1000V eDelivery CPU License Qty 32-Pack

Warranty Information

Find warranty information on Cisco.com at the [Product Warranties](#) page.

Service and Support

Cisco Services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. Cisco Services address all aspects of planning, building, and running the network; helping you shorten implementation times, lower operating costs, capture new business opportunities, mitigate risk, and accelerate growth. Cisco Security Services can help you plan, build, and run secure networks that protect your organization from attack and disruption, protect privacy, and support regulatory compliance controls. Included in the “Run” phase of the service lifecycle are Cisco Security IntelliShield Alert Manager Service, Cisco SMARTnet®, and Cisco Service Provider Base. These services are suitable for enterprise, commercial, and service provider customers.

Cisco Security IntelliShield Alert Manager Service provides a customizable, web-based threat and vulnerability alert service that allows organizations to easily access timely, accurate, and credible information about potential vulnerabilities in their environment.

For More Information

For more information, please contact your local account representative, or visit the following websites:

- Cisco ASA 1000V Cloud Firewall: <http://www.cisco.com/go/asa1000v>
- Cisco Nexus 1000V Series Switch: <http://www.cisco.com/go/nexus1000v>
- Cisco Virtual Security Gateway: <http://www.cisco.com/go/vsg>
- Cisco Virtual Network Management Center: <http://www.cisco.com/go/vnmc>
- Cisco ASA 5500 Series Adaptive Security Appliance: <http://www.cisco.com/go/asa>
- Cisco Security Services:
http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html




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.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

C78-687960-02 12/12