Cisco ASA 1000V Cloud Firewall

General Questions

Q. What is the Cisco® ASA 1000V Cloud Firewall?

A. The Cisco® ASA 1000V Cloud Firewall is a virtual security appliance that secures the tenant edge in multitenant private and public cloud deployments. Cisco ASA 1000V employs mainstream, proven Cisco Adaptive Security Appliance (ASA) security technology that has been optimized to cater to this specific use case. It acts as a default gateway (Layer 3 firewall) that provides edge functionality and secures against network based attacks. It integrates with the Cisco Nexus® 1000V Series Switch for enhanced deployment flexibility.

Q. How is the Cisco ASA 1000V Cloud Firewall different from the Cisco Virtual Security Gateway (VSG)?

A. The Cisco ASA 1000V Cloud Firewall provides strong tenant edge security, while the Virtual Security Gateway (VSG) secures traffic within a tenant (intra-tenant security for traffic between virtual machines [VMs]).

The key differences between the two products are outlined in Table 1.

Table 1. Differences between Cisco ASA 1000V Cloud Firewall and Cisco Virtual Security Gateway

Cisco ASA 1000V Cloud Firewall	Cisco Virtual Security Gateway
Secures the tenant edge	Secures intra-tenant (inter-VM) traffic
Default gateway (All packets pass through the Cisco ASA 1000V)	VSG offloads traffic to the vPath offering performance acceleration; only the first packet goes through the VSG
Layer 3 firewall (for north-to-south traffic)	Layer 2 firewall (for east-to-west traffic)
Edge firewall features and capabilities including network-attribute-based access control lists (ACLs), site-to-site VPN, Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP), stateful inspections, IP audit, TCP intercept, authentication, authorization, and accounting (AAA)	Network attribute and VM-attribute based policies

These two products complement each other to provide strong end-to-end security for private and public clouds. As customers move toward a flatter network, the Cisco ASA 1000V Cloud Firewall provides a VLAN-agnostic solution to secure the tenant edge. VSG can be used to segment and secure the flat network within the tenant.

Q. Is Cisco VSG required to run with Cisco ASA 1000V?

A. No. While Cisco ASA 1000V and Cisco VSG provide complementary functionality, they are separate products that can be run independently from one another. Based on the customer environment, the ASA 1000V and VSG can coexist to provide end-to-end (intra-tenant and tenant edge) security for private and public clouds. However, Cisco VSG is not a required component of Cisco ASA 1000V.

Q. How does Cisco ASA 1000V fit into the larger Cisco network virtualization vision?

A. Cisco's vision is to extend the components and "norms" from the physical environment into the virtual environment, while addressing the blind spots and security loopholes created by virtualization:

- Using Cisco Nexus 1000V Series Switches, the Cisco ASA 1000V Cloud Firewall extends Cisco's proven networking components to virtualized and cloud environments.
- Cisco ASA 1000V extends a well-proven security component from the physical environment to private and public cloud deployments, making them secure. It integrates with vPath, an integral component of the Cisco Nexus 1000V Series Switches. vPath serves as a single intelligent data plane for all the virtual service nodes including Cisco ASA 1000V, Cisco VSG, and Cisco Virtual Wide Area Application Services (vWAAS). This integration point provides the Cisco ASA 1000V with the hooks and visibility into the hypervisor. It also helps Cisco build an architecture than can easily scale and support heterogeneous hypervisor environments.
- The Cisco ASA 1000V helps to ensure that current operational workflows are not disrupted, by maintaining separate management control points for security teams, network teams, and server teams. The Cisco Virtual Network Management Center (VNMC) acts as a single point of management for the Cisco virtual security services including Cisco VSG and Cisco ASA 1000V.

Q. How does Cisco ASA 1000V fit into the larger Cisco security strategy?

A. Cisco ASA 1000V uses the existing Cisco Adaptive Security Appliance (ASA) infrastructure. It maintains consistency with other ASA form factors, including Cisco ASA 5500 Series Adaptive Security Appliances and the Cisco Catalyst® 6500 Series ASA Services Module, while being optimized for cloud specific use cases. Customers have the flexibility to choose the ASA form factor that best fits their network infrastructure and deployment use case, while creating an integrated best-in-class security framework. This approach places Cisco in a unique position to consistently secure hybrid infrastructures: physical, virtual, cloud.

Q. Does Cisco ASA 1000V Cloud Firewall replace physical ASA deployments?

A. No. Cisco ASA 1000V targets new use cases. The ASA 1000V secures the tenant edge within multitenant private and public cloud infrastructures that require elastic scale and ease of deployment.

Physical ASA appliances are recommended for Internet edge deployments, where performance is key.

Q. How is Cisco ASA 1000V Cloud Firewall different from a physical ASA appliance with a multicontext license?

A. Both are valid options for segmenting and securing multitenant private and public clouds. The most appropriate option depends upon the customer's environment and requirements. The Cisco ASA 1000V Cloud Firewall is most beneficial in environments that require quick deployment and elastic scale, security closer to the virtualized environment (instead of hair-pinning the traffic to the physical security appliance), a VLAN-agnostic solution, and overall higher flexibility (as offered by virtual solutions).

Section 2: Features and Benefits

Q. What features does Cisco ASA 1000V Cloud Builder support?

A. Cisco ASA 1000V uses the ASA infrastructure. The feature set in the first release is optimized to secure the tenant edge. It provides multitenant edge security, default gateway functionality, and protection against network-based attacks. Cisco ASA 1000V:

- Employs 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.
- 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 (VM) by automatically provisioning IP addresses to VMs being provisioned at a rapid pace.
- Secures the cloud perimeter against network-based attacks.
- Acts as a Virtual Extensible LAN (VXLAN) gateway to support highly scalable segmentation of the infrastructure.

Q. How do the features supported by Cisco ASA 1000V Cloud Firewall compare with those of the physical ASA?

A. The ASA 1000V feature set is optimized for the specific use case of securing the tenant edge. Therefore, it acts as a default gateway (Layer 3 firewall) and delivers edge firewall functionality, including network attribute-based ACLs, site-to-site VPN, NAT, DHCP, inspections, TCP intercept, and IP audit. Cisco ASA 1000V also offers additional virtualization-specific features like vMotion and VMware high availability (HA). Detailed notes can be found in the Cisco ASA Software Release 8.7 Release Notes.

Q. Does Cisco ASA 1000V run as a VM on the virtualized infrastructure?

A. Yes.

Q. How many interfaces does Cisco ASA 1000V have?

A. Cisco ASA 1000V has four interfaces: inside, outside, failover, and management.

ASA 1000V brings flexibility and simplicity to policy organization and application by enabling application of different security policies to different groups of VMs on the same VLAN and subnet (based on groups or categories of virtual machines). A single instance of ASA 1000V can support multiple edge profiles, each with distinctly defined security policies attached to different sets of VMs on the same VLAN and subnet.

Cisco ASA 1000V Solution Components

Q. Does Cisco ASA 1000V require the Cisco Nexus 1000V Series Switch?

A. Yes, the ASA 1000V is tightly integrated with the Cisco Nexus 1000V Series Switch, which provides the ASA 1000V with architectural benefits and hooks into the hypervisor. vPath is the single intelligent data plane for all virtual services integrated with the Cisco Nexus 1000V Series, enabling intelligent traffic steering and service chaining between these virtual services. Some of the key differentiators of the solution include:

- Enables significant deployment flexibility with the capability for a single Cisco ASA 1000V instance to secure multiple VMware ESX hosts. This characteristic offers significant resource and cost optimization as it avoids the requirement to deploy an instance on each host. This solution also enables significant deployment flexibility. To avoid resource clashes, customers can segregate the resources on which Cisco ASA 1000V are deployed from the resources on which mission-critical applications are deployed.

- Enables a multiple-hypervisor-capable solution. As customers move toward a heterogeneous hypervisor environment, the Cisco Nexus 1000V Series becomes the point of integration with different hypervisors. Therefore, virtual services like the Cisco ASA 1000V would not need to be custom created for each hypervisor.
- Supports enhanced scalability by acting as a VXLAN gateway (enabled by the Cisco Nexus 1000V).

Q. Which hypervisors does the ASA 1000V support?

A. The Cisco ASA 1000V, in its initial release supports VMware vSphere hypervisor 4.1 and onwards.

Q. When will Cisco ASA 1000V support other hypervisors?

A. The Cisco Nexus 1000V Series provides the required visibility into the hypervisor - unlike competitive offerings, which require the APIs provided by hypervisor vendors (for example, VMSafe) to gain this visibility. Cisco ASA 1000V is multiple-hypervisor-capable and can easily extend to other hypervisors in its future versions.

Q. Is the ASA 1000V a feature on the Cisco Nexus 1000V Series?

A. No, the Cisco ASA 1000V is a separate product. However, it has been specifically developed for environments that have Cisco Nexus 1000V Series deployments.

Q. Is Cisco ASA 1000V supported on the Cisco Nexus 1010 Virtual Services Appliance?

A. No, not in the first release.

Q. How is the Cisco ASA 1000V managed?

A. Cisco Virtual Network Management Center (VNMC) is the primary manager for both the Cisco ASA 1000V and Cisco Virtual security Gateway (VSG). In addition, Cisco Adaptive Security Device Manager (ASDM) can also manage the Cisco ASA 1000V.

Q. What is VNMC? Why do we require VNMC for ASA 1000V?

A. Cisco Virtual Network Management Center (VNMC) is a multitenant-capable, multidevice, policy-driven management solution for Cisco virtual security services (such as Cisco ASA 1000V Cloud Firewall and Cisco Virtual Security Gateway [VSG]) to provide end-to-end security of virtual and cloud infrastructures. It has been custom-created for the virtualization-specific workflows. VNMC delivers the following benefits:

- Helps enable rapid and scalable deployment through dynamic, template-driven policy management based on security profiles.
- Integrates with VMware vCenter to use VM attributes (required for policies based on VM attributes).
- Enhances management flexibility through an XML API that helps enable programmatic integration with third-party management and orchestration tools.
- Helps ensure collaborative governance with role-relevant management interfaces for network, server, and security administrators.

Q. Does Cisco Security Manager manage the Cisco ASA 1000V?

A. No, the ASA 1000V is not managed by Cisco Security Manager. VNMC is custom created to cater to virtualizatiuon specific workflows. It offers a multi-tenant of structure, templatized way of attaching policies, and integrates with vCenter to provide visibility into VM attributes. These features are key for a virtual security appliance manager.

Q. Does Cisco ASA 1000V have to be deployed on the Cisco Unified Computing System™?

A. No, Cisco ASA 1000V is capable of running on any of the hardware platforms supported by VMware. The Cisco UCS® platform is just one of them.

Licensing, Timelines, and Other Details

Q. What are the performance metrics?

A. The performance of the Cisco ASA 1000V Cloud Firewall will depend on the physical hardware on which it is running and the resources available.

Q. What are the resources consumed by a single instance of Cisco ASA 1000V?

A. A single image of the ASA 1000V consumes 1 vCPU and 1.5-GB RAM.

Q. Can I modify the resources allocated to an instance of Cisco ASA 1000V?

A. No. Allotting more resources to a single instance would generate a warning. Allotting lower resources than the prescribed specifications would impact the performance of the ASA 1000V.

Q. What ASA software versions does the ASA 1000V support?

A. The ASA 1000V is supported on Cisco ASA Software Release 8.7, which is based on Cisco ASA Software Release 8.4.

Q. Does Cisco ASA 1000V support the identity firewall feature?

A. Not at initial release, due to the focus on multitenant edge use cases.

Q. Will the Cisco ASA 1000V be available as part of the vBlock package?

A. Yes, Cisco is currently working with the vBlock team to include the ASA 1000V as part of the vBlock package. This should be available in the near future.

Q. How is the Cisco ASA 1000V Cloud Firewall licensed?

A. The Cisco ASA 1000V is licensed per CPU socket protected. The licensing model is similar to the one used by the Cisco Nexus 1000V Series and Cisco VSG. The Cisco ASA 1000V is licensed per CPU socket protected.

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 C67-688050-01 08/12