White Paper

Securing Virtual Applications and Servers

Overview

Security concerns are the most often cited obstacle to application virtualization and adoption of cloud-computing models. Merely replicating the security policies of physical environments is not an option because these policies can limit the advantages of virtualization and do not address new security challenges inherent in applications and data residing in virtual server environments.

Virtual applications - applications that have been optimized to run on virtual infrastructures - are typically web-based, making it possible for authorized users to input information, synchronize it, and later access it. Examples include business application servers such as Microsoft Exchange Server, SAP, and Oracle E-Business Suite, as well as custom developed applications typically consisting of a web server, database server, development framework, and the application itself.

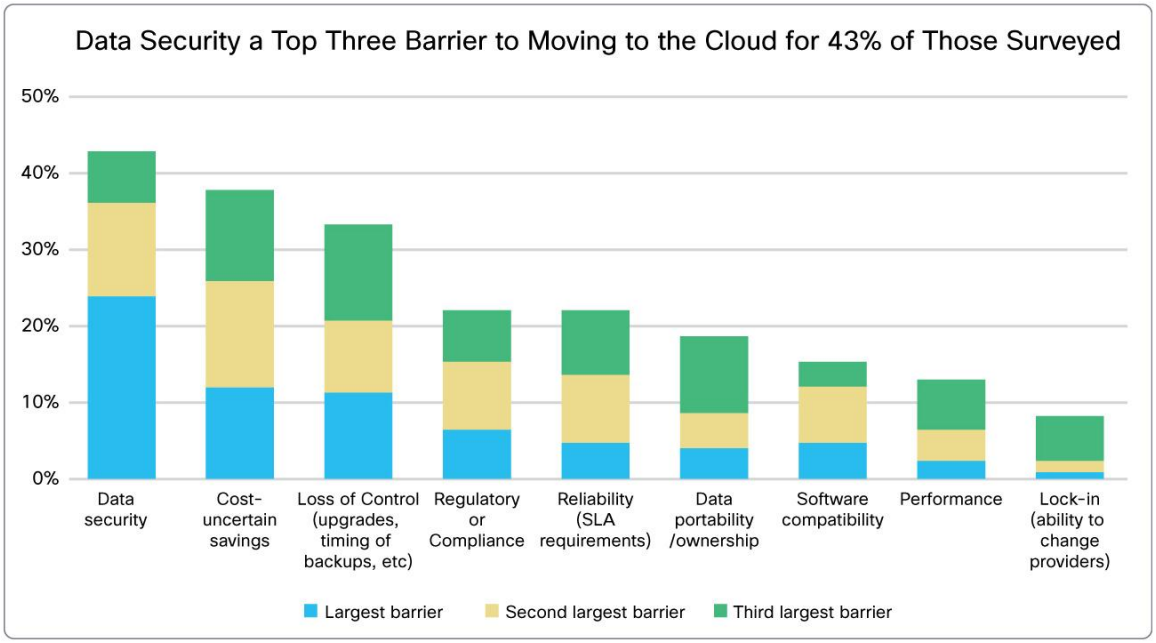
To secure these virtual applications, a new security framework must be deployed - one that works within the virtualization layer of the data center, connects it to the physical data center, and addresses additional requirements of scalable, multitenant environments.

Security Concerns: The Number One Challenge to Widespread Application Virtualization

For enterprise applications, server virtualization is a strategic initiative that is fostering consolidation, cost reduction, and more efficient use of resources. Virtualization typically starts with specific applications in the enterprise data center, but large-scale virtualization of multiple applications can permit organizations to get ready for the economies of scale and efficiency of cloud computing, enabling both internally managed private clouds and outsourced public clouds.

While most large organizations have taken advantage of virtualizing non-mission-critical applications, many remain concerned about widespread virtualization of mission-critical applications and migration to the cloud. By far the most frequently cited concern about virtualization is the security of virtual applications and the virtual environment (Figure 1). Until recently, organizations have had to compromise on the level of security that could be achieved by applying the known best practices in the physical world.

Figure 1. Barriers to Virtualization



Source: AlphaWise[SM], Morgan Stanley, **"Cloud Computing Takes Off, Market Set to Boom as Migration Takes Off"** May 23, 2011.

Security Challenges for Virtual Environments

Let's take a quick look at the potential threats and complexities that are introduced with application virtualization and cloud-computing environments:

- **High-value targets:** Data center and mission-critical applications are increasingly recognized as high-value targets both for hackers and threats that come from inside the organization. The 2011 Verizon Data Breach Investigations Report indicated that 94% of all data reported stolen came from servers (an increase of 18%), and 96% of victims who were subject to the Payment Card Industry Data Security Standard (PCI DSS) had not achieved compliance. Continuing on this path in 2012, every month compared to the corresponding month in the previous year has a higher number of data breaches.
- **Mobility of workloads:** Server virtualization enables mobility of applications between servers, or even between remote data centers and clouds. This mobility introduces complexity in the network security layer, which has typically relied on fixed-resource locations and static private networks to enforce security policies. Flexibly moving security policies along with virtual workloads has been challenging.
- **Increasing points of attack:** Server virtualization introduces additional points of attack, particularly in the virtualization layer, including the hypervisor, the virtual machine environment, and the soft switches that replace the physical access-layer switches in the network. These additional layers introduce more vulnerable points into the data center. Indeed, the software-virtualization layer is less inherently secure than physical devices typically are due to lack of physical separation and the nature of multitenancy.

- **Multitenancy:** Whereas small, distributed data centers host a small number of applications or support a single organization, today's consolidated data centers and clouds have disparate user groups that require complete separation of network traffic and strict access control policies, even though they are sharing the same physical servers and network infrastructure. This is also true of private virtual data centers and private clouds, as internal tenants require separation.
- **VLAN limitations:** In physical LAN environments, the predominant mechanism for separating user groups and resources is the VLAN. VLANs cannot be used in virtual data centers in the same way because applications typically cannot migrate between VLANs. This, in turn, undermines the primary advantage of virtualization: the capability to use any available resource in the data center. There is a need for new network separation and segmentation capabilities as well as a suitable security construct.
- **Separation of duties in data center administration:** IT environments have had a strict division of responsibilities between the server administrators, network administrators, and the security team. Server virtualization has complicated this division of labor because the server teams have typically taken over the networking and security aspects of the virtualization layer that runs on the servers and the virtual machine environment. Tools are needed that allow security groups and consistent security policies to be applied to this new virtualization layer.
- **Scale and complexity of consolidated data centers:** Consolidation brings concerns about scalability and complexity. These issues are constraints that IT must deal with in designing and implementing security policies and solutions in the network and in managing them over time.

Requirements for Context-Aware Security Policies in the Data Center

Traditionally, data center applications and desktop clients have been responsible for most user authentication and access control. In a world of increasing mobility, unsecured devices, and increasingly sophisticated threats, the network must take over more of the security policy enforcement responsibilities from application endpoints as networks become more context and application aware.

The network security infrastructure is increasingly required to enforce identity and role-based policies, as well as to make other contextual decisions. The capability to block traffic to an application or server in the data center or cloud can no longer be based on the typical source or destination addresses of hosts. Now it must be based on the identity or role of the user, the process, or application in the transaction. Access can also depend on context-specific attributes other than identity, including the type of device accessing the application, the location of the user, the time of the request, and more. These context-aware policies are increasingly becoming the responsibility of the data center firewall and intrusion prevention system (IPS), which have to expand their capabilities to detect and decide based on these factors, as well as to monitor for the presence of malware, unauthorized access attempts, and various attacks.

Designing a Security Model for the Consolidated, Multitenant Data Center

The challenges of virtual data centers are causing organizations to review the way that network security solutions are deployed. A proper defense-in-depth security approach requires deployment of a number of complementary security services at appropriate points in the data center network. The following list summarizes fundamental best practices in designing data center networks, general requirements for viable network security solutions, and the role of each of the security services.

Defend the Data Center from Unauthorized Users and Outside Attacks

The first step in securing the data center is to block from the rest of the LAN all traffic that is not authorized, valid traffic to and from the data center. Deploy a stateful firewall in front of the data center or a large segment of shared server resources that can block all traffic from unauthorized sources to invalid data center destinations. This defense can be achieved with a high-bandwidth network security appliance such as the Cisco® ASA 5585-X Adaptive Security Appliance.

Prevent Intrusion and Contain Malware

Legitimate traffic from outside the data center may still contain malware, including Trojan horses, viruses, and worms. Deploy a scalable, high-bandwidth IPS to inspect all traffic coming into the data center, or at appropriate points within the data center. This inspection can reasonably ensure that all data center traffic and virtual machines are clean of threats. There is minimal risk that malware will attack other virtual machines if these are blocked from applications in other trust zones by the virtual firewall. The Cisco ASA 5585-X is a multipurpose network security appliance that provides IPS functions in addition to stateful firewall capabilities.

Defend the Tenant Edge with a Proven Firewall

Extend the well-proven security component of the physical environment to the virtual and cloud infrastructure and secure different department, business unit, or client zones with strong multitenant edge security for highly secure communications between multiple tenants. The Cisco ASA 1000V Cloud Firewall integrates with the Cisco Nexus® 1000V Virtual Switch and provides this security along with default gateway functionality and protection against network- based attacks.

Assign Virtual Machines to Segmented Trust Zones and Enforce Access Policies

Inside the data center, enforce security policies that isolate traffic between application groups to help ensure that users and services authorized for one application cannot inappropriately access other applications residing in other trust zones. This degree of access control and logical isolation is easily provided by firewalls, but it has previously been impossible to provide firewall capability at the virtual machine level or to isolate virtual machines on the same server. Virtual machines were not visible to the physical network and firewall as separate entities. This granular control is now attainable using virtual network- specific firewalls such as the Cisco Virtual Security Gateway (VSG) for the Cisco Nexus 1000V Series Switch.

Provide Centralized Multitenant Policy Management

Creating security profiles using a template-based configuration approach can simplify authoring, deployment, and management of your security policies by reducing complexity and simplifying provisioning. This administration model is made possible with the Cisco Virtual Network Management Center (VNMC) that can manage the Cisco VSG virtual gateway inside a tenant and the Cisco ASA 1000V virtual firewall at the tenant edge.

Support Virtual Machine Mobility

When security policies are assigned to virtual machines, or virtual machines are assigned to trust zones, those policies need to move around the data center with the virtual machine as it moves to a new server. Since firewall policies are enforced by the firewall outside the virtual machine, this kind of mobility has been particularly challenging to provide. It is, however, a fundamental capability of Cisco VSG, which is designed to be virtualization-aware of the VM attributes.

Secure Access to Your Virtualized Data Center and Applications

VPNs are a viable means of connecting outside users directly to hosted services, particularly in public cloud environments that run web application servers. Traditionally, a VPN is thought of as a gateway to a LAN, but a VPN can also be a secure gateway to hosted data center servers and applications. Data-center-class VPN systems are nearly universally coresident with firewalls and need to provide the same levels of scalability, performance, connectivity, and reliability that the rest of the data center infrastructure provides. VPNs also allow granular remote access to applications residing in a private cloud in the data center.

Provide Scalability

Today's data centers and cloud networks are straining current scalability capabilities as organizations increase consolidation and outsourcing to achieve dramatically better cost models. This trend is in its early stages, with large organizations just beginning to move to internally hosted private clouds and large public cloud environments. Already, large commercial cloud providers have constructed single data centers with tens of thousands of servers and global clouds with remote sites consisting of hundreds of thousands of servers.

- To take full advantage of resource availability at the lowest cost in the optimal location, scalability of the Layer 2 network domain is of critical importance, since scalability will generally limit the range over which a particular application workload can migrate. Scalability can be particularly challenging for security policies and enforcement points of the network, which have to remain intact with the virtual application as it migrates between servers, data centers, and cloud sites. Automating the provisioning of security services and policies as applications are deployed and expanding their data center footprints is critical to making a cloud deployment successful and cost-efficient.

Separate Security, Network, and Server Administrator Duties

The virtualization of application workloads, and security services in particular, has created an additional challenge for IT departments. As virtual security services migrate from the network onto virtual hosts running in the server, implementation of security policies and management of the security infrastructure falls to the server administration teams, rather than the network security administrators. Even when teams work collaboratively, enterprise policies frequently require a strict separation of duties between these teams, helping ensure that network security staff remains wholly in charge of security policies and enforcement and management of virtual devices. The deployment and implementation of virtualized security devices must be managed off the server, and they must be managed in a way that is consistent with other physical security appliances with strict separation of duties.

Tight Integration of Cisco ASA 1000V Cloud Firewall and Cisco VSG with Cisco Nexus 1000V Switches

Cisco ASA 1000V Cloud Firewall and the Cisco Virtual Security Gateway (VSG) complement each other in terms of functionality. The ASA 1000V integrates with the Cisco 1000V Nexus Series virtual switch to help secure multitenant virtual and cloud environments at the tenant edge.

Cisco ASA 1000V Cloud Firewall acts as the default gateway, and provides security against network-based attacks. An organization may want to separate different tenants to meet compliance requirements: for instance, to isolate all applications that touch R&D information, sensitive financial information, or credit card payment information from all other applications. A multitenant data center or private community cloud naturally requires complete isolation of application traffic between different tenants, applications, and user groups, depending on the policies that are in place.

Cisco VSG integrates with the Cisco Nexus 1000V Series virtual switch to provide granular inter-VM security within a tenant. It provides gateway services and virtual machine context-aware and zone-based security capabilities.

If an organization requires multiple policy features within a single tenant, these areas can be separated even further into trusted zones. Zones are defined as isolated virtual machines with an OS instance. Since the Cisco VSG is a virtual firewall service that provides granular policy enforcement at the virtual machine level, it effectively separates virtual machine workloads that reside in different trust zones, even if the virtual machines reside on the same physical server.

Cisco VSG provides the logical separation of virtual machines and traffic in different trust zones without the overhead of creating and managing the VLANs that typically isolate portions of the network. VLANs in the data center can quickly limit scalability and reduce the benefits of data center consolidation and virtualization. Only a virtualized security service embedded in the virtualization layer of the network can mirror the capabilities provided by VLANs in physical networks while overcoming the obstacles to virtualization.

Together, Cisco VSG and ASA 1000V provide a trusted and strong edge security for highly secure communications between multiple tenants. The Cisco Nexus 1000V Series Switch provides service-chaining capabilities between Cisco VSG and Cisco ASA 1000V Cloud Firewall.

For example, in a healthcare usage scenario, hospitals that have embraced virtualization may have separate tenant entities for billing, medical records, business intelligence, and research projects. However, sometimes information in medical records is needed to support data in a clinical trial. The complimentary features of the Cisco ASA 1000V with VSG enable secure communication between the medical record tenant and the research project tenant to permit accepted data to enter the research project tenant while maintaining privacy and policy controls of unnecessary medical record data from entering.

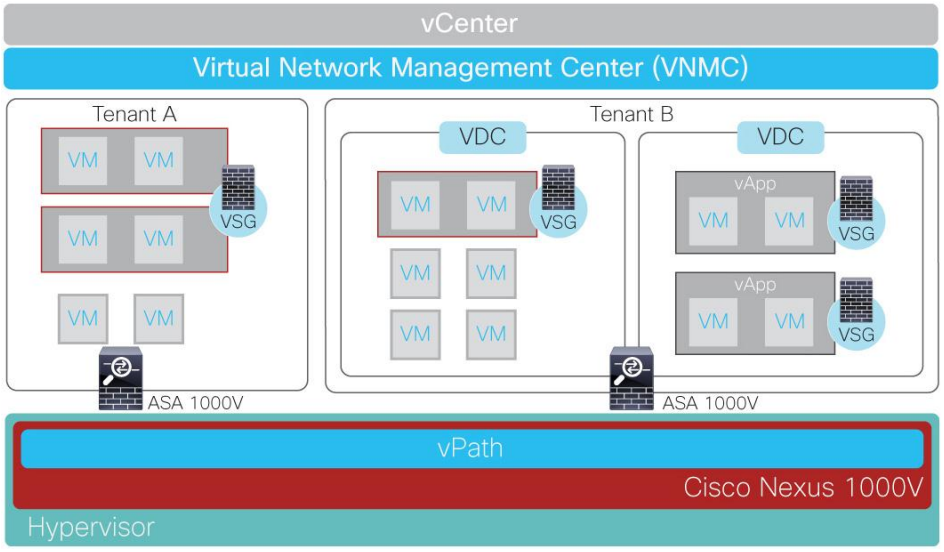
A virtual firewall operating between virtual machines can also prevent malicious attacks between virtual machines, attacks against the hypervisor or the host operating systems, and network reconnaissance from a compromised application or host. To enforce granular security policies specific to individual virtual machines, Cisco VSG and the Cisco ASA 1000V are designed to tightly integrate with the Cisco Nexus 1000V Series virtual switch and the resident hypervisor in the virtualization layer of the server. As new virtual machines are instantiated or migrate between servers, the appropriate security policies for the virtual machine also migrate along with the virtual machine, providing all the necessary security services automatically.

The virtual firewall instances can be created and shared as demands and service loads require, for optimal resource utilization. Both Cisco ASA 1000V and Cisco VSG use the Cisco Nexus 1000V Series Swicth’s vPath traffic steering capability to steer traffic to appropriate networking services for policy enforcement. This approach enables a single instance of Cisco ASA 1000V or VSG to secure the VMs on multiple hosts, helping to ensure that the security infrastructure of the data center or cloud is scalable and can be easily managed. The number of instances of Cisco ASA 1000V and Cisco VSG firewalls can grow according to need so that you can enforce a large number of policies specific to the various virtual applications. The architecture helps to ensure resource optimization and cost savings for the end user.

The integrated solution is also built to scale across heterogeneous hypervisor environments. As the Cisco Nexus 1000V Series Switch scales across different types of hypervisors, the services that run on the Cisco Nexus 1000V, including the VSG and ASA 1000V, also scale to secure these heterogeneous environments.

For both the ASA 1000V and the Cisco VSG the security policies are administered from a centralized virtual security management console, the Cisco Virtual Network Management Center (VNMC), which is a transparent, scalable, multitenant-capable, policy-driven management solution for end-to-end security of virtual and cloud environments. Cisco VNMC helps to enable rapid and scalable deployment through dynamic, template-driven policy management based on security profiles. It enhances flexibility through an XML API that helps enable programmatic integration with third-party management and orchestration tools. VNMC allows security administrators to control security policies separately from the applications, servers, and network, for compliance purposes.

Figure 2. Illustrates how the Cisco ASA 1000V integrates with the Nexus 1000V virtual switch and Cisco VSG.



Conclusion

Securing virtual applications and the virtualization layer of the data center is the most challenging obstacle to achieving the benefits of data center consolidation and virtualization and moving to a cloud cost model. New virtual security services with visibility into virtual applications and switches are required to complement the traditional data center-class physical security appliances and modules that protect the data center.

The Cisco ASA 1000V firewall blocks external attacks to virtual and cloud tenants in the virtual data center and drops traffic if not permitted. It enforces existing security policy in a virtualized application environment and overcomes security concerns of shared resources of multi tenant cloud deployments.

The Cisco VSG firewall enforces detailed security policies that are virtual machine aware and helps ensure isolation of traffic and applications in a way that traditional security devices cannot, without limiting scalability of the overall data center or complicating the delivery of virtual applications.

The Cisco ASA 1000V and Cisco VSG benefit from a tight integration with the Cisco Nexus 1000V Series virtual switch. The centralized management center for both the Cisco ASA1000V and Cisco VSG helps ensure separation of duties between network security and application server teams for compliance purposes, and it simplifies the overall administration of large cloud environments.

For More Information

http://www.cisco.com/go/vsg

http://www.cisco.com/go/asa1000v

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 C11-652663-01 09/12