Securing Virtual Applications with Cisco and Imperva

Virtualization offers many benefits, but it also introduces a host of new security risks. Organizations wish to consolidate hardware, reduce power consumption, and streamline operations, but they also want to preserve the best-of-breed security that they enjoyed in physical environments.

Simply converting hardware-based security appliances to virtual appliances does not address the unique security, deployment, and management challenges of virtualized environments. New security challenges in virtual environments include: mobility of workloads, increasing points of attack, scale and complexity of consolidated data centers, and separation of duties in administration. To address the new potential threats and complexities of the virtualized environment a new security framework must be developed - one that fully integrates with server hypervisors, connects it to the physical data center, and addresses scalability, routing, and high availability requirements.

Security Must Be Pervasive, Context and Application-Aware

With the proliferation of mobile devices and increasingly sophisticated threats, network firewalls must assume more responsibility than ever before, identifying users and enforcing user access controls. The network security infrastructure is increasingly required to enforce identity and role-based policies, as well as to make other contextual decisions. Network firewalls can no longer just permit or deny access based on IP address and port number. Now, firewalls must correctly identify the role of the user, the location of the user, the device, the process, or application in the transaction and be tenant aware and application aware. Data center firewalls and intrusion prevention systems (IPS), must be context-aware, and they must also identify other security risks such as the presence of malware, unauthorized access attempts, and various attacks.

The challenges of virtualized data centers are requiring the deployment of a number of complimentary security services at the appropriate points within the virtualized data center network. Firewalls built for virtualized environments can extend the well-proven security component of the physical environment and secure the tenant edge, create trust zones and enforce access policies to these tenants, zones and virtual applications.

Web applications are also a top target of attack. Hackers continually probe applications, attempting to exploit vulnerabilities and steal data. Web application firewalls (WAFs) can protect Web applications from attack because they dynamically learn application structure, protect sessions, and virtually patch custom application vulnerabilities. Web application firewalls provide a complete defense against Web-based threats because they not only stop technical Web attacks, but they also prevent business logic attacks like site scraping and online fraud.

Integration of Cisco ASA 1000V, Cisco VSG, and Imperva SecureSphere WAF with Cisco Nexus 1000V

Cisco and Imperva have collaborated to offer a complete security solution for a virtualized data center. The Cisco ASA 1000V Cloud Firewall, the Cisco Virtual Security Gateway (VSG) and the Imperva SecureSphere Web Application Firewall interoperate with the Cisco Nexus 1000V series switch to streamline management and deployment in virtual environments.

- **Cisco ASA 1000V Cloud Firewall** acts as the default gateway, secures the tenant edge and provides security against network-based attacks. 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; the Cisco ASA 1000V provides that essential network segmentation.

- **Cisco Virtual Security Gateway (VSG)** integrates with the Cisco Nexus 1000V Series virtual switch to provide granular inter-VM security within a tenant. It is a transparent L2 firewall with virtual machine context-aware and zone-based security capabilities. 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.
- **The Imperva SecureSphere Web Application Firewall (WAF)** protects sensitive Web applications from Web-borne threats that can lead to a Website breach. The Imperva SecureSphere WAF is available as a virtual appliance and integrates with the Cisco Nexus 1000V Series virtual switch.

The Cisco VSG, ASA 1000V, and Imperva SecureSphere WAF provide a trusted and strong security architecture for virtualized data centers. The vPath technology in the Cisco Nexus 1000V Series Switch provide service-chaining capabilities between Cisco VSG, Cisco ASA 1000V Cloud Firewall, and the Imperva SecureSphere WAF.

To enforce granular security policies specific to individual virtual machines, Cisco VSG, the Cisco ASA 1000V, and the Imperva SecureSphere WAF are designed to integrate with the Cisco Nexus 1000V Series virtual switch. As new virtual machines are instantiated or migrate to new servers, the appropriate security policies also migrate along with the virtual machine, providing all the necessary security services automatically. You can optimize traffic flow by chaining services as per the particular use case. In addition, vPath offers performance acceleration for Cisco VSG by offloading the ACL to the switch for subsequent packets of the flow.

The virtual firewall and WAF instances can be created as multi-tenant environment demands and service loads require, for optimal resource utilization. The Cisco ASA 1000V, the Cisco VSG, and the SecureSphere WAF use the Cisco vPath traffic steering capability to steer traffic to appropriate networking services for policy enforcement. This approach enables a single instance of a Cisco ASA 1000V, VSG, or WAFs 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, Cisco VSG or SecureSphere WAFs can grow according to need so that you can enforce a large number of policies specific to the various virtual applications. The architecture helps optimize resources and lower costs.

Integration with the Cisco Nexus 1000V also helps customers secure heterogeneous hypervisor environments. Since the Cisco Nexus 1000V Series Switch will be deployed across multiple hypervisors, it can correctly route traffic through firewall and WAF virtual instances running on other host servers.

Integration Benefits

Integration of the Cisco ASA 1000V, the Cisco VSG, Imperva SecureSphere WAF with the Cisco Nexus 1000V enables:

- **Traffic steering** using vPath technology to allow services to be deployed anywhere with no need to replicate services on every host server
- **Application mobility** enabling applications to be migrated seamlessly without disrupting services or security policies
- **Support for heterogeneous hypervisor environments** since the Cisco Nexus 1000V will be supported on multiple hypervisors - VMware vSphere, Microsoft Hyper-V, KVM and Xen Server
- **A non-disruptive operational model**

Conclusion

Virtualization introduces security and management challenges. New virtual security services with visibility into virtual applications and switches are required to complement the traditional physical security appliances that protect the data center.

The three solutions, the Cisco ASA 1000V, the Cisco VSG, and the Imperva SecureSphere WAF, integrate with the Cisco Nexus 1000V switch to provide a powerful defense against application threats originating from the Internet or from other virtual hosts in a multitenant environment. Together, the combined solution offers highest security available to stop network and Web application attacks.

C96-726705-00 02/13