Cisco Virtualization Experience Infrastructure: Secure the Virtual Desktop

What You Will Learn

Cisco® Virtualization Experience Infrastructure (VXI) delivers a service-optimized desktop virtualization platform with comprehensive services across three Cisco architectures: Cisco Data Center, Borderless Networks, and Collaboration.

Cisco VXI is redefining desktop virtualization to encompass the full suite of tools that make up an employee's collaborative workspace, delivering an uncompromised user experience that supports pervasive, interactive media not traditionally supported in a virtual desktop environment.

Cisco VXI permits you to deliver to your employees an environment that is both agile and efficient, that enables personalized and pervasive user interactions, and that combines both openness and control through centralization and consolidation of business assets, while delivering a fully virtualized, collaborative workspace.

The centralization of desktops as virtual machines in a data center presents new security challenges, necessitating a holistic, end-to-end security approach that extends from the client endpoint to virtual machine.

Why Is Cisco VXI Security Important?

Cisco VXI is an end-to-end system across three architectures: Cisco Data Center, Borderless Networks, and Collaboration. Best practices in security must be applied in this architecture, employing traditional security measures to protect the data center and the infrastructure, secure remote access, and securing the traffic from endpoints. Additional measures must be taken to secure the virtual desktops and the communication between one virtual desktop and another as well as communication between one virtual desktop and a virtual server. Because virtual desktops are now consolidated within the data center, it is more important than ever to separate desktop and server traffic and protect mission-critical servers and applications running on the back end.

Virtual desktops add a new set of security challenges. Hosted virtual desktops (HVDs) replace a very static environment (physical users and machines) with a potentially very dynamic one. Virtual machines can be viewed as containers that use an allocation of a physical host's CPU, memory, network interface, storage, I/O processing, etc. and that dictate the boundaries and rules of engagement with the hypervisor. Hosted virtual desktops are contained in these virtual machines and use the parameters associated with the virtual machine. If a disaster (natural or human made) occurs, or if the organization simply needs to rebalance the use of physical hosts or perform an equipment upgrade during a maintenance window, virtual desktops can be migrated from one cluster of physical hosts to another. This migration can be implemented through administrator intervention, or it can be automated using rules and policies established with the hypervisor management platform. When virtual machines move between servers, maintaining a security policy for the virtual machine requires constant monitoring of the virtual machine. Monitoring these policies is critical to help ensure that any data access being requested from within the HVD has security policies associated with the HVD so that the end user can access only the servers and applications that the user is allowed to access. There is also a risk of an insider having access to all the virtual machines in the same virtual LAN. Current solutions to solve the problem with Layer 3 firewalling mechanisms are often inefficient and can negatively affect data center scalability and performance.

Virtualization also opens up a new area of attacks. The hypervisor can act as a single point of failure and can be a source of corruption for any virtual desktops that it hosts. Virtual machine API calls are targets for malicious code, and it is important to enforce policies that allow only authenticated and authorized API calls to be made, keeping the performance intact. It is also important to implement best practices, such as eliminating the exposure of hypervisor IP addresses. Exposure of hypervisor IP addresses can lead to distributed-denial-of-service (DDoS) attacks, which in turn can lead to risk of losing encryption keys residing in virtual memory.

Another consideration relates to the organization's migration to virtual desktops. During the transition, there will be a mixed environment of PCs and virtual desktops. This raises the additional challenge of maintaining security in both traditional and virtual environments and performing compliance checks in mixed environments. It is important to reduce the inconsistency and deliver a security policy and administrative mechanism that is well suited to both environments. Additionally, moving to HVDs does not eliminate the need for traditional security. Traditional security challenges still apply for the virtualized environment, and most of the existing firewall, Intrusion Prevention, Email and Web Security, and secure mobility continue to apply to the data center and end-user perimeters.

Traditional Security for the End User

A system administrator must facilitate access to the data center from multiple locations. The administrator also must challenge the end user for authentication. The connection originating from the end user must be encrypted. Depending on where the user is accessing the desktop, the type of VPN encryption technology varies: EasyVPN, Dynamic Multipoint VPN (DMVPN), or SSLVPN. In addition, the end user is authenticated for IEEE 802.1x against the role-based access policies defined by Cisco Identity Service Engine (ISE). Capabilities on the LAN such as hop-to-hop LAN Security (MACsec) encryption can encrypt the display protocol on the LAN.

Traditional Security for the Data Center

A system administrator must protect the data center against all threats. Appropriate firewall policies at the edge allow or deny the display protocol traffic destined for the data center. Therefore a key data center security mechanism is a high performance firewall that controls network access to sensitive information assets and critical resources in a data center. Furthermore, an intrusion prevention system is necessary to detect and stop viruses, malware or hackers from attacking data center resources. In addition, the VPN head-end at the data center must terminate the VPN connections originating from the end client. Also, all email and web traffic leaving the enterprise must be scanned to meet regulatory and corporate compliance regulations. Cisco IronPort™ Email and Web Security Solutions provide integrated in depth scanning and only allow authorized content to enter and leave the premises.

Secure Borderless Networks for Cisco VXI

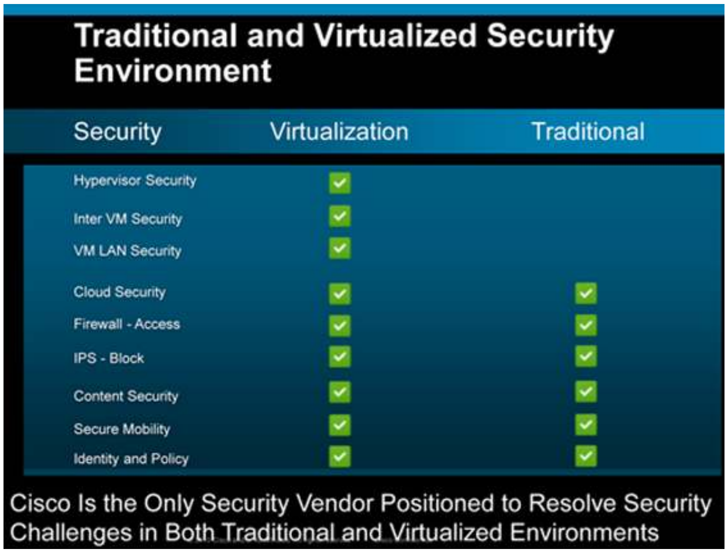
Cisco Borderless Networks integrate into the network to grant highly secure resource access to the right people using the right devices. The Cisco Borderless Networks portfolio helps enable:

- Controlled access to data center resources with a consistent, context-aware security policy
- Delivery of virtualization-aware, enhanced application performance
- Enforced security policies for traffic between virtual machines
- Policy consistency for highly mobile, densely populated virtual machines
- Delivery of more secure video, voice, wireless, and data services to your remote workforce
- Confidence that your systems are safeguarded from the latest threats.

- Protection of valuable data, control and monitoring of network access, and enforcement of content policies

Cisco's leadership in security makes Cisco well positioned to solve the security challenges for both physical and virtual desktops (Figure 1). Its end-to-end security architecture can scale well and create uniformity in policy creation for both virtual and non-virtual environments. Typically, servers are maintained in the server administrative group, and security, compliance, and the network is the domain of the security and network groups. In most companies, the group enforcing security policies is different than the group handling server administration. Security policies and regulatory compliance are best handled when the end-to-end scope of implementation is under the administration of one group. Now security administrators can use familiar tools, approaches, and policies to extend their control over domains that they do not currently manage, such as virtual machines .

Figure 1. Securing Virtual Environments



Traditional and Virtualized Security Environment

Security	Virtualization	Traditional
Hypervisor Security	✓	
Inter VM Security	✓	
VM LAN Security	✓	
Cloud Security	✓	✓
Firewall - Access	✓	✓
IPS - Block	✓	✓
Content Security	✓	✓
Secure Mobility	✓	✓
Identity and Policy	✓	✓

Cisco Is the Only Security Vendor Positioned to Resolve Security Challenges in Both Traditional and Virtualized Environments

Virtualization Security

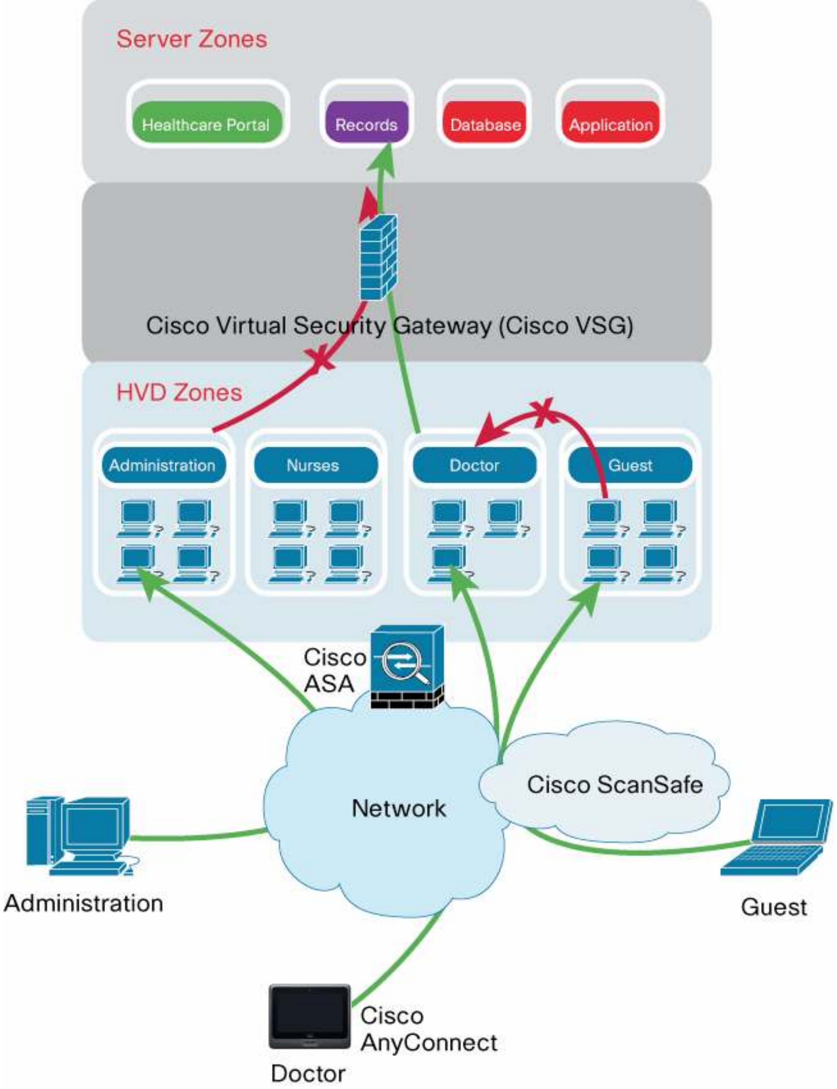
Cisco Nexus 1000V Switch: Follow Virtual Machine Security Policies

The Cisco Nexus® 1000V Switch offers a management interface similar to a command-line interface (CLI), which allows network and security administrators to apply access policies and other parameters through an administrative interface with which they are already familiar and to create the port profiles individually. These port profiles are then attached to the virtual machines by the server administrators, and they remain attached to the virtual machines even when the virtual machines (and the virtual desktops residing within them) migrate between servers. This approach helps ensure that an appropriate access policy for the user is enforced with the virtual machine regardless of where the virtual machine is hosted.

Cisco Virtual Security Gateway: Virtual Machine–to–Virtual Machine Firewall and Virtual Machine Zoning

Cisco Virtual Security Gateway (VSG) provides secure segmentation of data center virtual machines using granular, zone-based control and monitoring with context-aware security policies (Figure 2). Controls can be applied across organizational zones, lines of business, or multi-tenant environments. Context-based access logs are generated with network and virtual machine activity levels. Trust zones and security templates can be provisioned on demand as virtual machines are created. These zones, containing like-purposed virtual machines (user desktop zone, enterprise resource planning [ERP] application zone, web server zone, etc.) can be applied globally.

Figure 2. Healthcare Use Case: Bringing it all together



Cisco VSG employs the virtual network service data path (vPath) technology that is embedded in the Cisco Nexus 1000V distributed virtual switch. Cisco vPath steers traffic to a designated Cisco VSG for initial policy evaluation and enforcement. Subsequent policy enforcement is offloaded directly to vPath. Cisco VSG can provide protection across multiple physical servers and virtual machines.

As a result, in a typical healthcare setting, for example, doctors can be in zone 1, and nurses can be separated into a zone 2 . Doctors will be given access to dictation notes about patients, patient records, etc., but access for nurses can be limited to other databases that allow them to enter patients’ vital signs, view patients’ blood work, etc. The hospital administrators will be in a separate zone (zone 3) and will not have access to the patient records database because they are concerned with general administration of the hospital and not patient records. There can also be a fourth zone (zone 4, the guest zone) for patients and guests that allows access to the Internet through secure, browser-based kiosks running on Microsoft Windows 7 non-persistent virtual desktops. Giving desktop virtualization−based Internet access during wait time is one way to improve patient satisfaction without the burden of maintaining the desktop. The IT administrative can mitigate any malicious activity or high-bandwidth-consuming activity and to make administrative decisions such as moving a virtual machine from zone 3 to a quarantine zone.

Intervirtual machine security can also be taken one step further in improving the security of the hypervisor itself. The hypervisor abstracts the physical host's resources into virtualized resources each virtual machine can access. It also manages the system's LAN and SAN interfaces. It is essential to ensure that only necessary, authenticated, and authorized API calls are made to the hypervisor from guest virtual machines.

Cisco AnyConnect and AnyConnect Secure Mobility Solutions

Beyond data center security, organizations need to consider the security of the WAN and extended remote branch-office and small-office and home-office (SOHO) environments from which users will access their virtual desktops. They must help ensure that the connection to the data center itself is secure. HVDs can be accessed through a variety of end clients such as thin clients, zero clients, repurposed PCs, and business tablets, and users can be expected to demand access to their HVDs at any time, and from anywhere. Cisco AnyConnect™ Secure Mobility provides the capability to connect to an HVD session securely through SSL and maintain encrypted access even when the user is mobile. Cisco AnyConnect capabilities such as always-on VPN and session persistence help ensure an optimal user experience. Cisco AnyConnect offers secure split tunneling capability and directs traffic to enterprise or to Cisco ScanSafe software-as-a-solution(SaaS) based web security. The Cisco ScanSafe solution works with the Cisco AnyConnect solution, and users can access Cisco ScanSafe services from outside the corporate infrastructure. Its location-aware capabilities and high availability offers an excellent user experience while continuing to offer web security both on and off premises. In a geographically dispersed data center deployment, HVDs within the remote data center can access the Cisco ScanSafe services that are closest to the data center and improve security without compromising the user experience.

Threat Defense and Cisco Data Loss Prevention

In addition to intervirtual machine security, traditional security mechanisms such as firewall and intrusion protection systems (IPS) are still required to protect the data center infrastructure itself. Even though the data in an HVD session is considered secure primarily due to the consolidation of data storage and access in the data center, there is still a risk of data loss either through email or the web. A user can accidently attach a highly confidential document to an unintended recipient in the email. An inappropriate posting of content to the web can also lead to the leaking of important documents. Cisco's content security continues to offer data leak protection for email and web data originating from an HVD.

Conclusion

Cisco is well positioned to address the security challenges presented by the new and evolving virtualized collaborative workspace. In both physical and virtual environments, Cisco VXI can address the security challenges from the client to the hypervisor: in campus and off campus, at remote branches, in SOHO environments, at hotspots, and within the data center (Table 1).

Table 1. Cisco VXI Security Portfolio

Challenge	Security For	Solution
Secure remote access	Thin clients, thick clients, zero client, smartphones, and tablets	Cisco AnyConnect Secure Mobility (Cisco AnyConnect 3.0 for email and web security); and EasyVPN, DMVPN, and GETVPN for site-to-site VPN technologies

Challenge	Security For	Solution
Virtualization security	Hypervisor, virtual machines, and virtual switches	Cisco VSG, Cisco Nexus 1000V, virtual machine LAN security, PVLAN, IP source guard, Domain Host Configuration Protocol (DHCP) snooping, Address Resolution Protocol (ARP) Inspection, and NetFlow
Threat defense	Data center defense	Cisco ASA 5585-X Adaptive Security Appliance, firewall, and IPS
Application and content Security	HTTP an XML attacks	Email and web security with Cisco IronPort and Cisco ScanSafe appliances
Secure user virtual experience	Display protocol and interactive media	Secure integrated desktop virtualization and secure interactive media experience

The Cisco VXI offers these security benefits:

- Cisco Unified Computing System™ and Cisco VN-Link technology provide visibility into and security of the network to the virtual machine and address the challenge of the complexity of security policy enforcement on the virtual ports of the server.
- The Cisco Nexus 1000V and Cisco VSG secure intervirtual machine traffic and address the challenges of user segmentation and isolation from mission-critical applications such as ERP, customer relationship management (CRM), and web services. Users are placed in multiple zones, and appropriate security policies are applied to the zone, even as virtual machine−based desktops migrate from one physical host to another.
- Cisco AnyConnect Secure Mobility and Cisco ASA enable any time, anywhere secure access to HVDs and integrate with Cisco email and web security to deliver a secure and productive end user experience.
- Role-based access restrictions with Cisco ISE address the challenge of restricting user access on the basis of the user's role, user's device and its posture compliance.

Cisco VXI security is well suited to address the challenges of desktop virtualization security whether the deployment is for customers with no prior virtualization solutions or for customers in the process of migrating to HVDs. Cisco VXI helps ensure that security best practices for physical systems are extended to virtual systems, allowing coexistence of physical and virtual desktops and consistent security policy enforcement across the two architectures.

For More Information

Cisco Desktop Virtualization Solutions: http://www.cisco.com/go/vdi

Cisco Virtualization Experience Infrastructure: http://www.cisco.com/go/vxi

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 C11-665340-00 05/11