Q&A

Cisco Secure Data Center Solutions for Virtual and Private Cloud Infrastructures

Customer Concerns

Q. Why is securing your virtual and cloud infrastructure important?

A. Virtualization and cloud computing change the way information and services are delivered and consumed. Agile and more efficient use of resources lead to better business performance and competitiveness, allowing organizations to achieve their business goals at an accelerated pace. At the same time, virtualization and cloud computing introduce new security risks and challenges around new technologies and changing business processes. To succeed, organizations must address these security concerns.

Q. What are some examples of customer virtualization and cloud security concerns?

A. Here are four typical categories of security issues related to virtualization and cloud computing:

- **Threat defense:** Networks must be protected from both external and internal threats. Externally, you must protect infrastructure and applications from data loss, network and application attacks, and other sophisticated attacks using state of the art techniques like threat intelligence, passive OS fingerprinting, and reputation, along with contextual analysis, to deliver superior security protection. Internally you must protect from threats caused by general attacks on the framework DNS, ports, and protocols or by disgruntled employees.
- **Challenges posed by new technology:** Multitenancy is a good example. Instead of having a physically dedicated infrastructure (servers, switches, storage) for each application, business unit, or function, large virtual and cloud infrastructures use multitenancy to logically separate those business groups that require a protected and trusted virtual computing environment. Secure data flow between these segmented environments must ensure that data flows only into and out of its assigned tenant and only persons or services with approved access to that tenant can add or retrieve data.
- **Visibility:** Maintaining compliance and providing visibility into the virtual and cloud data center is of primary concern. Customers want to ensure that the same controls used in the physical world are present in the virtual. Granular visibility is also a precursor to compliancy with internal, industry, and regulatory standards.
- **Server virtualization challenges:** VMware vMotion moves virtual machines across physical ports, and the network policy must follow this migration (across racks, pods, and data center). Administrators must view or apply network and security policy to locally switched traffic. Administrators need to maintain segregation of duties while helping ensure nondisruptive operations. Organizations need a VLAN-agnostic solution to decrease complexity and enhance scalability.

Cisco's Approach to a Secure Data Center

Q. What should I think about first when considering a secure transformation to a virtualized environment and migration to the cloud?

A. Virtualization and cloud security need to be addressed at both the technology and business levels. Organizations need to include security in their overall data center and cloud computing planning process from day one and make it an integral part of organizational governance and culture. When deciding when and what to virtualize and move to the cloud, customers should assess their IT plans through a business lens by reviewing objectives, processes, and applications. These business objectives should be balanced with risk factors, architectural requirements and limitations. Organizations should then plan on strategically building security into the virtual and cloud architecture so that it is both agile and robust. Once a virtual and cloud security solution has been implemented, accountability and improvement processes are critical to keep up with changing threats and evolving technologies.

Q. How does Cisco deliver a secure data center solution?

A. Cisco® secure data center solutions deliver a full set of proven security features that don't impact business-critical services and applications, that provide the flexibility to integrate with complex, multisite networks and offer scalable and reliable capabilities. Cisco security products are integrated with the Cisco Unified Data Center and extensively tested and validated in environments simulating whole customer infrastructures and not just point solution scenarios. By pairing Cisco Validated Designs with Cisco architectures comprising network, compute, and security products, Cisco enables predictable, reliable deployment of solutions and business services. In addition, these validated designs allow the infrastructure to evolve with customer needs.

Q. What are Cisco's core data center security objectives and requirements?

A. Cisco's secure data center solutions enable s secure **segmentation** of the network, compute, and virtual boundaries, and enforce segmented policy based on function, device, and organization. Finally, they provide controlled access to network resources and applications. They **block** external and internal **threats** at the DC data center edge and zones and to applications because well-defined policies are already in place. These solutions provide **visibility** to network entities and flows, to drive consistent enforcement and policy regardless of deployment model.

Q. What are architectural considerations for securing the virtualized and cloud infrastructures?

A. A virtualization and cloud security solution needs to meet the following architectural requirements:

- **Logical separation:** Security controls need to be implemented to secure logical entities, which can include both physical and virtual infrastructure components.
- **Policy consistency:** It is critical to have a security policy design that can be enforced consistently in both physical and virtual environments.
- **Automation:** In a cloud computing environment, where resources are shared dynamically, there are two requirements: resources such as virtual machines (VMs) may be instantiated and move around in an automated manner, and VM zones and the security policy need to move along with the VMs.
- **Authentication and access control:** With the "anytime, anywhere" availability of cloud services, security policies are needed to validate user credentials and authorize their cloud services.

- **Scalability and performance:** A virtual and cloud computing implementation will need to securely support large workloads and the underlying infrastructure, such as high-density VMs as well as multi-data-center interconnects and workload mobility. Firewall and intrusion prevention system (IPS) services, for instance, must be able to scale so that they do not become the bottleneck.

Securing the Virtual and Private Cloud Infrastructure

Q. How do Cisco secure data center solutions help meet architectural requirements for bare metal, virtual, and multitenant environments?

A. Many architectural considerations are built into Cisco secure data center solutions.

For the Physical Environment

- Cisco ASA 5585-X Adaptive Security Appliance provides industry-leading MultiScale™ performance, enabling rapid connections per second, an abundance of concurrent sessions, accelerated throughput, and multiple security services for exceptional flexibility.
- Cisco IPS 4500 Series Sensors have been built from the ground up for data center deployments. The 4500 Series Sensor delivers hardware-accelerated inspection, real-world performance, high port density, and energy efficiency in an expansion-ready chassis for future growth and investment protection. Its slim, high-performance density form-factor and low power consumption were specifically engineered for space-challenged data center environments.
- Cisco ASA-CX Context-Aware Security Appliance can be deployed in the data center as a department-edge application firewall. It provides the capability to identify and log or block the usage of rogue (unapproved) servers in a departmental network.
- Cisco Adaptive Security Appliance (ASA) Software Release 9.0 delivers enterprise-class security capabilities for ASA devices in a variety of form factors, including a wide range of standalone appliances, hardware blades that integrate with the organization's existing network infrastructure, and software that can secure and protect public and private clouds. Major new features in Release 9.0 include: the ability to join up to eight Cisco ASA 5585-X or 5580 adaptive security appliances in a single cluster; integration with Cisco Cloud Web Security (formerly ScanSafe), which allows enterprises to enforce granular web access and web application policy while providing protection from viruses and malware; and Cisco TrustSec® Security Group Tags (SGTs), which integrate security into the network fabric to extend the policy construct on the ASA platform.
- Cisco TrustSec Security Group Access (SGA) is an innovative technology that classifies systems or users based on context as they connect. TrustSec SGA transforms the way organizations implement security policy across their data center infrastructure. This context-based classification system propagates using Security Group Tags (SGTs) to make intelligent policy-based blocking decisions in the data center. In addition, TrustSec SGA automates firewall rules and removes the management complexity in access control administration.
- Cisco Security Manager 4.3 is a comprehensive management solution that enables consistent policy enforcement, rapid troubleshooting of security events, and summarized reports across the security deployment. It manages the Cisco security environment, provides visibility across the deployment, and enables information sharing with other essential network services. Lastly, it maximizes operational efficiency with a powerful suite of automated capabilities. Cisco Security Manager manages the Cisco security environment for Cisco ASA 5500 Series Adaptive Security Appliances, Cisco IPS 4500 Series

Sensor Appliances, the Cisco AnyConnect® Secure Mobility Client, and Cisco SR 500 Series Secure Routers.

For the Virtual Environment

- For environments that don't require tenant separation, a multi-context firewall such as the Cisco ASA 5585-X Adaptive Security Appliance can be viewed as having multiple separate (virtual) firewalls on the same hardware. Each context is managed as a separate security entity with its own interface and security policy.
- The Cisco Virtual Machine Fabric Extender (VM-FEX) technology built into the Cisco Unified Computing System™ (Cisco UCS®) collapses virtual and physical networking into a single infrastructure. Along with VMware's vMotion, Cisco VM-FEX permits network policies to be carried with VMs as they move to new physical servers or virtual environments. Combining the multi-context firewall of the ASA 5585-X with Cisco IPS 4500 and VM-FEX offers a secure solution for virtual environments that don't need large-scale tenant separations.

If the virtual environment requires more scalability, flexibility, and agility, and more granular security is needed at the tenant and zone level, the Cisco ASA 1000V Cloud Firewall and the Cisco Virtual Security Gateway (VSG) are the way to go. This security solution is supported by the Cisco Nexus® 1000V Series virtual switch.

- Cisco Nexus 1000V Series Switches deliver highly secure, multitenant services by adding virtualization intelligence to the data center network. These soft switches extend the network edge to the hypervisor and virtual machines, and are built to scale for cloud networks. Cisco Nexus 1000V supports a wide range of hypervisor environments, including VMware vSphere and Microsoft Windows 2012 Server Hyper-V. The Cisco Nexus 1000V Series Switch also forms the foundation of virtual overlay networks, a key pillar of Software Defined Networking (SDN).
- Cisco Virtual Security Gateway is integrated into the Cisco Nexus 1000V Series virtual switch, and allows the creation of multiple network zones utilizing VM awareness to provide granular, inter-VM, zone-based security, including full logical separation of different servers, services, and applications running on virtual machines owned by different tenants.
- Cisco ASA 1000V Cloud Firewall offers tenant edge capabilities like site-to-site VPN, Dynamic Host Configuration Protocol (DHCP), Network Address Translation (NAT), and inspections. It also integrates with the Cisco Nexus 1000V Series virtual switch for enhanced deployment flexibility. It acts as a default gateway, securing the tenant against network-based attacks.
- Cisco Virtual Network Management Center (VNMC) is a centralized virtual security management console that administers the security policies for the Cisco ASA 1000V and the Cisco VSG. VNMC is a transparent, scalable, multitenant-capable, policy-driven management solution for end-to-end security of virtual and cloud environments. It 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 applications, servers, and the network for compliance purposes.

Virtualization and Cloud Services

Q. What services does Cisco provide for virtualization and cloud?

A. Cisco offers professional and support services to help ensure your success in planning, building, and managing secure data center and cloud environments. Cisco Services help customers plan, build, and manage complex data center and cloud infrastructures that are secure. Whether your challenge is securely connecting multisite or multitenant physical and virtual environments, providing secure access to business applications and data from any device, protecting information and privacy, or enabling secure collaboration anywhere, we help you enable policies, governance, compliance, and pervasive security across the data center infrastructure and within and between clouds to protect your business.

For more information on security services, go here.

For more information on data center services, go here.

Q. How does Cisco help build and secure private cloud?

A. The Cisco Intelligent Automation for Cloud software solution provides powerful automation and orchestration tools for building and operating a private cloud service in the virtualized data center. Processes can be defined in the system to instantiate VMs on demand and allocated them in the right networks where security policies have first been defined by Cisco ASA, ASA 1000V, and VSG. In addition, VNMC (centralized multi-tenant manager for VSG and ASA 1000V) offers an XML API for integration into third-party managers and orchestrator tools to further automate security policies in the orchestrated private cloud environment.

Cisco's Advantages Compared to the Competition

Q. What are Cisco's advantages?

A.

- Cisco is the proven security technology leader, offering the densest, high-speed firewall that scales to meet the new demands of the data center with the ASA 5585-X.
- Cisco provides the flexibility to secure inter-VM and multi-tenant architectures (zone and edge deployments) with Cisco VSG and ASA 1000V.
- Cisco provides operational consistency (policy and management) across physical, virtual, and cloud deployments while delivering form-factor-agnostic security solutions, including network integrated and overlay platforms like Cisco ASA 1000V and VSG.
- Cisco integrates policy movement seamlessly into the network fabric, taking advantage of innovative designs like VM-FEX, Overlay Transport Virtualization (OTV), Cisco Locator/ID Separation Protocol (LISP), and vPath.
- Cisco offers multi-context designs and clustering to scale virtual environments.
- Cisco integrates products into Cisco Unified Data Center validated designs that are thoroughly tested.

Q. What is the Cisco Virtualized Multi-Service Data Center (VMDC)?

A. VMDC is a Cisco validated architecture. At Cisco, our solutions undergo intensive testing to ensure they meet the stringent design reliability and stability requirements that you require of a secure data center, secure virtual data center, and secure private cloud.

Cisco's VMDC secures the Unified Data Center that hosts mission-critical applications and sensitive data. Cisco Unified Data Center changes the economics of the data center by converging compute, storage, networking, virtualization, and management into a single, fabric-based platform, designed to increase operating efficiencies, simplify IT operations, and provide business agility.

Unlike other solutions, which add layers of management software to achieve integration, Cisco Unified Data Center is specifically designed for virtualization and automation, and enables on-demand provisioning from shared pools of infrastructure across physical and virtual environments. This approach allows IT to move from being a cost center to providing IT services that create competitive advantage.

Tightly integrated with UDC in the VMDC are security controls provided by Cisco's market-leading firewall, VPN, hardware-accelerated IPS, and appliances and applications for the virtual environment. This secure, validated design enables a seamless network flow from physical to virtual networks, allowing agile operations and simpler management. It can create multiple security zones that logically separate tenant resources from one another in the virtual network and allow for fault-tolerant VM motion. Edge security protects the data center from external threats and offers secure contextual access to data center resources. The Cisco VMDC environment is intuitive, powerful, and secure - providing superior real-time protection for critical information assets using innovative IPS with Global Correlation, firewall, and VPN technology.

Additional Questions

Q. Where should I go for more information?

A. Secure Data Center

Secure Data Center VMDC

Secure Multitenancy

Cisco Unified Data Center

Cisco ASA 5585-X Adaptive Security Appliance

Cisco IPS 4500 Series Sensor

Cisco ASA 1000V Virtual Firewall

Cisco Nexus 1000V Virtual Switch

Cisco Virtual Security Gateway

Cisco Virtual Network Management Center

Cisco ASA CX Context-Aware Adaptive Security Appliance

Cisco TrustSec

Cisco Security Manager

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 C67-714776-00 09/12