Cisco Secure Data Center Solutions

SECURITY, EFFICIENCY, AGILITY, AND SCALABILITY FOR YOUR DATA CENTER

Transforming the Data Center Securely

With increasing demands on their data centers, enterprises must find ways to reduce capital investments, free up business with greater efficiency, optimize IT resources, provide agility and scalability, and enable new business models for revenue growth. To attain these business goals, enterprises are evolving their data center architectures, moving from traditional data centers to virtualized environments – and eventually to the cloud.

This move to new business computing models has introduced security challenges, both technological and process-oriented, which are the primary barrier to making the transition from the virtualized data center to the cloud. We must rethink how security fits and develop new tools to ensure that the transfer of information is protected.

Providing Optimal Security in the New Data Center

The Cisco® Secure Data Center solution enables secure segmentation of the network and of policy to virtual machines and users. Because policy is already in place, the Cisco Secure Data Center solution blocks internal and external threats at the data center edge and zones, and in applications. The solution's security context capabilities provide visibility into network entities and flows to drive consistent enforcement and policy regardless of deployment model.

Core components of the Cisco Secure Data Center solution include:

- Secure segmentation
- Threat defense
- Visibility

Secure Segmentation

Large enterprises use segmentation to manage and organize data in their data centers. However, building a segmented framework has a direct impact on security – where it is implemented, for whom, and how. As an organization segments, virtualizes, and moves applications to the cloud, the network becomes more complex. Security must be built into the network fabric and must work with the network to ensure consistent policy and visibility to sensitive information as it flows through the network.

- Cisco ASA 5585-X Adaptive Security Appliances are tailored to meet the performance needs of mission-critical data centers. The appliances combine the world's most proven firewall with the industry's most widely deployed, context-aware IPS, offering the most effective security solution in the industry to significantly decrease business risk and address regulatory compliance – all in a compact 2-rack-unit footprint.
- Cisco ASA Software Release 9.0 delivers enterprise-class security capabilities in a variety of form factors, including a wide range of standalone appliances, hardware blades that integrate with an organization's existing network infrastructure, and software that can secure and protect public and private clouds. Major new features in Release 9.0 include clustering; 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 is an innovative solution that classifies systems or users based on context as they connect, and then transforms the way organizations implement security policy across their data center infrastructure. This context-based classification propagates using SGTs to make intelligent policy-based forward or blocking decisions in the data center. In addition, Cisco TrustSec SGA automates firewall rules and removes the management complexity of access control administration.
- The Cisco ASA 1000V Cloud Firewall provides security to the tenant edge inside the data center, separating the compute from the virtual. Built using the ASA infrastructure, the firewall offers edge functionality, including site-to-site VPN, Network Address Translation (NAT), Dynamic Host Control Protocol (DHCP), and inspections into network-based attacks. A multitenant data center or private cloud naturally requires complete isolation of application traffic between different tenants, applications, and user groups depending on the policies that are in place. It integrates with the Nexus 1000V switch for enhanced deployment flexibility.
- The Cisco Virtual Security Gateway integrates with the Cisco Nexus® 1000V Series Switch to provide granular inter-virtual-machine security within a tenant. It provides gateway services and virtual machine context-aware and zone-based security capabilities. The Virtual Security Gateway uses the virtual network service data path (vPath) technology embedded in the Cisco Nexus 1000V Series Virtual Ethernet Module.

- Cisco vPath technology steers traffic via the ASA 1000V Cloud Firewall, whether inbound or traveling from virtual machine to virtual machine, to the designated Cisco Virtual Security Gateways. It offers service chaining capabilities between the integrated virtual services deployed as part of the solution (including the Virtual Security Gateway and Cloud Firewall). It also offers virtual extensible LAN (VXLAN) capabilities for enhanced scalability.
- 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. The Nexus 1000V Series supports a wide range of hypervisor environments, including VMware vSphere and Microsoft Windows 2012 Server Hyper-V, . The Nexus 1000V Series Switch also forms the foundation of virtual overlay networks, a key pillar of software-defined networking.

Threat Defense

According to the 2011 Verizon Data Breach Investigation report, 92% of network threats are external: They originate from outside sources such as hackers, organized crime groups, and government entities and typically are targeted against a specific organization. Cisco solutions protect infrastructures and applications from advanced persistent threats (APTs) and other sophisticated external attacks using threat intelligence, passive OS fingerprinting, and reputation and contextual analysis.

- The Cisco IPS 4500 Series delivers hardware-accelerated inspection, real-world performance, high port density, and energy efficiency in an expansion-ready chassis designed for future growth and investment protection. Its small form factor and low power consumption make it ideal for space-challenged data center environments.
- The Cisco ASA CX can be deployed in the data center as a department-edge application firewall. It brings in the capability to identify and log or block the use of rogue (unapproved) servers in a departmental network.

Visibility

Customers want to ensure that the same controls available in the physical world are present in the virtual world. Cisco solutions simplify operations and compliance reporting, provide visibility into security elements in the network, and apply business context to network activity.

- Cisco Security Manager 4.3 is a comprehensive management solution that enables consistent policy enforcement, rapid troubleshooting of security events, and summarized reports across a 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 security environment for Cisco ASA 5500 Series Adaptive Security Appliances, Cisco IPS 4500 Series Sensor Appliances, the Cisco AnyConnect® Secure Mobility Client, and Cisco Secure Routers.
- Cisco Virtual Network Management Center (VNMC) is a centralized virtual security management console that administers the security policies for the Cisco ASA 1000V Cloud Firewall and the Cisco Virtual Security Gateway. Cisco VNMC is a transparent, scalable, multitenant-capable, policy-driven management solution that provides end-to-end security for 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 the applications, servers, and network, for compliance purposes.

Efficient and Seamless Security

The Cisco SecureX Architecture™ is a context-aware, network-centric approach to security that enables consistent security enforcement throughout the organization, increased alignment of security policies with business needs, integrated global intelligence, and greatly simplified delivery of services and content. Supporting business goals such as an optimized and managed experience that goes beyond secure data center is core to this approach. The result is end-to-end, automated security enforcement that is transparent to the end user and more efficient for the IT organization.

The Cisco difference:

- A full set of proven security features delivered without impacting business-critical services
- The densest high-speed firewall that scales to meet new data center demands
- Flexibility to integrate with complex multisite networks
- Flexibility to secure inter-virtual-machine and multitenant architectures (zone and edge deployments)
- Operational consistency (policy and management) across physical, virtual, and cloud deployments while delivering form-factor-agnostic security solutions such as network-integrated and overlay platforms

- Transparent integration of policy movement into the network fabric through innovative designs such as VM-Fex, OTV, LISP and vPath
- Multicontext designs and clustering to scale virtual environments
- Integration of products into Cisco Unified Data Center validated designs that are thoroughly tested

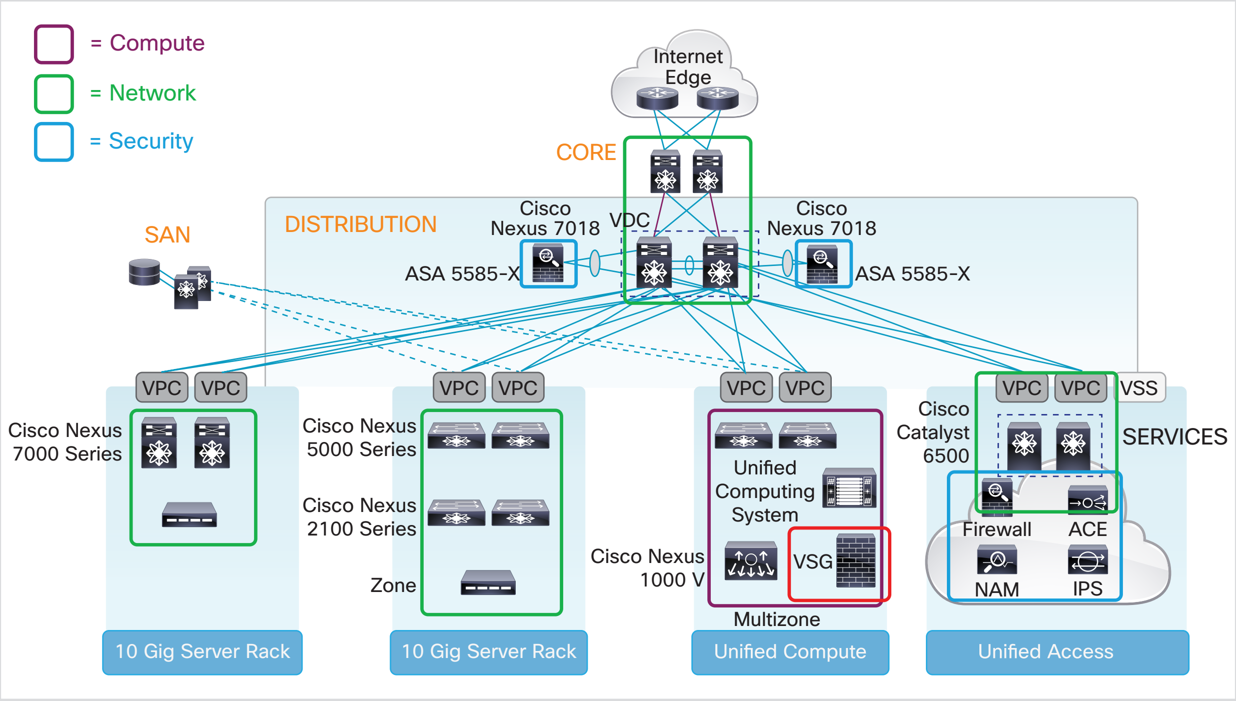
Integrating Security with the Unified Data Center

At Cisco, intensive testing is met with design reliability and stability requirements to secure the data center, the virtual data center, and the cloud. Cisco Virtualized Multi-Services Data Center (VMDC) is a validated design with security imbedded in the Cisco Unified Data Center The Unified Data Center changes the economics of the data center by unifying compute, storage, networking, virtualization, and management into a single, fabric-based platform designed to increase operating efficiencies, simplify IT operations, and provide business agility.

Tightly integrated with Unified Data Center are security controls provided by a market-leading firewall, VPN, and hardware-accelerated IPS, as well as 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 virtual machine motion. Edge security protects the data center from external threats and offers secure contextual access to data center resources. This VMDC environment is intuitive, powerful, and secure, providing superior real-time protection for critical information assets using innovative IPS with Global Correlation, firewall and web application firewall, and VPN technology.

Figure 1 shows the products included in the Cisco VMDC solution framework.

Figure 1. Cisco VMDC Solution Framework



Why Cisco?

Cisco is the leader in secure networks and holds a proven track record in network security innovation. The Cisco SecureX Architecture uniquely brings together three key elements: a network that provides contextual information and consistently enforces security policies; global threat intelligence; and one of the broadest security portfolios in the industry.

For More Information

http://www.cisco.com/en/US/netsol/ns340/ns394/ns224/ns376/index.html