CHAPTER 2

Cloud Security Solution Overview

As more enterprises and small and medium (SMB) businesses move critical data and applications over to virtualized, multi-tenant systems in public and private clouds, cyber-criminals will aggressively attack potential security vulnerabilities. Security strategies and best practices must evolve to mitigate rapidly emerging, increasingly dangerous threats. The Cisco VMDC Cloud Security 1.0 solution protects against such threats, and provides a reference design for effectively and economically securing cloud-based physical and virtualized cloud data center deployments.

This design guide describes how to build security into cloud data center deployments. The VMDC Cloud Security 1.0 solution integrates additional security capabilities into data center design with minimal deployment risks, addresses governance and regulatory requirements, and provides improved technical controls to reduce security threats.

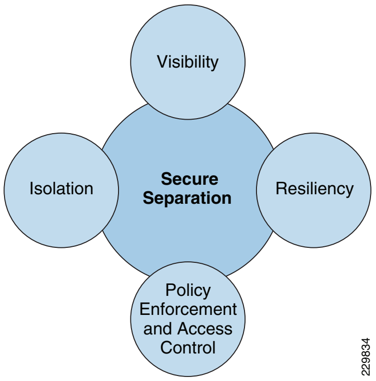
Providing end-to-end security for multi-tenant cloud data centers is a critical task that challenges service providers (SPs) and enterprises. However, deploying successful cloud data centers depends upon on end-to-end security in both data center infrastructures and the virtualized environments that host application and service loads for cloud consumers.

Security Architectural Principles

The primary security architectural principles for VMDC data center security are secure separation, visibility, isolation, resiliency, and policy enforcement as shown below:

Figure 2-1 shows the security principles incorporated in the security architecture.

Figure 2-1 Secure Separation Principles



Secure Separation

Secure separation describes the partitioning that prevents one tenant from having access to other tenants' environments and administrative features of the cloud infrastructure.

Isolation

Isolation provides a secure foundation for multi-tenant data centers and server farms. Depending on the design goals, isolation can be achieved using firewalls; access control lists (ACLs); virtual LANs (VLANs), Virtual Routing and Forwarding tables (VRFs), virtualization, storage networks, and physical separation. In addition, Intrusion Prevention appliances that can inspect traffic and detect security events on a per-VLAN basis can provide an additional level of threat isolation between different tenants. When combined, these can provide appropriate levels of security enforcement to server applications and services for multiple tenants.

Policy Enforcement and Access Control

Role Based access and authentication is an essential part of a comprehensive security framework. Obviously access to network devices and appliances needs to be regulated. If the infrastructure device access is compromised, the security and management of the entire network is at risk. Consequently, it is critical to establish the appropriate security measures and controls in order to prevent unauthorized access to infrastructure devices. Creating common policies and authentication measures across the environment is imperative in minimizing operational complexities and maximizing security. This solution provides policy enforcement and access control methods in a unified approach across all layers of the solution in order to address both complexity and security concerns.

Visibility

Data centers are becoming pliable in scaling to accommodate new virtual machines (VMs) and services. Server virtualization technologies, such as vMotion, enable servers to be deployed in and moved between multiple physical locations with minimal manual intervention. As VMs move and traffic patterns change, security administrators face challenges when attempting to actively monitor threats in the infrastructure. This architecture leverages threat detection and mitigation capabilities with state-of-the-art IPS appliances and cyber-threat-detection applications. This architect dynamically analyzes and correlates alarm, data, and event information to identify threats, visualize the attack paths, and also provide possible enforcement response options.

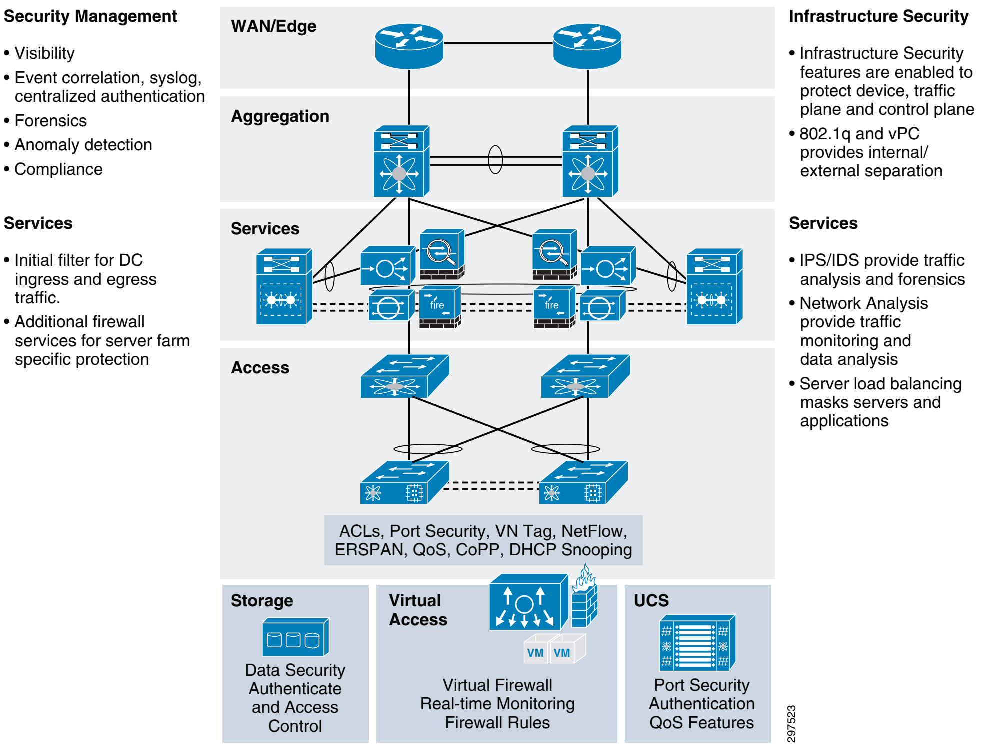
Resiliency

Resiliency implies that endpoints, infrastructure, and applications in multi-tenant environments are protected and can withstand attacks that would otherwise cause service disruptions, data exposure and unauthorized access. Proper infrastructure hardening, application redundancy, and firewalls are some of the approaches needed to achieve the desired resiliency.

VMDC Cloud Security Control Framework

Figure 2-2 shows a high level overview of the VMDC Cloud Security solution framework.

Figure 2-2 VMDC Cloud Security Solution Framework


Security Management
• Visibility
• Event correlation, syslog, centralized authentication
• Forensics
• Anomaly detection
• Compliance
Services
• Initial filter for DC ingress and egress traffic.
• Additional firewall services for server farm specific protection
WAN/Edge
Aggregation
Services
fire
fire
Access
ACLs, Port Security, VN Tag, NetFlow, ERSPAN, QoS, CoPP, DHCP Snooping
Storage
Data Security Authenticate and Access Control
Virtual Access
VM
VM
Virtual Firewall Real-time Monitoring Firewall Rules
UCS
Port Security Authentication QoS Features
Infrastructure Security
• Infrastructure Security features are enabled to protect device, traffic plane and control plane
• 802.1q and vPC provides internal/ external separation
Services
• IPS/IDS provide traffic analysis and forensics
• Network Analysis provide traffic monitoring and data analysis
• Server load balancing masks servers and applications
297523

The framework addresses three categories of security:

- Infrastructure Security, page 2-3
- Security Services, page 2-4
- Management Security, page 2-4

Infrastructure Security

Infrastructure security features protect devices and the network traffic and control planes. Key infrastructure security elements include:

- Internal and external separation using 802.1q and virtual port channels (vPCs)
- Storage separation, redundancy, and security (data-at-rest encryption)
- Industry standards and regulatory compliance, focusing on Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS)
- High availability (HA) and redundancy

Security Services

To provide end-to-end security in a multi-tenant cloud deployments, service providers need to deploy various security services. These security services, or features, can be offered to all the tenants or based on the service level. For example, for card processing customers, service providers must be providing firewall, and encryption services. Similarly, any high availability application requires load balancing services. The following security services are implemented in Cloud Security 1.0.

- Intrusion prevention systems (IPS) and intrusion detection systems (IDS) provide traffic analysis and forensics
- Network analysis provides traffic monitoring and data analysis
- Server load balancing masks servers and applications
- Line-rate NetFlow using Cisco NetFlow Generation Appliance (NGA)
- Intelligent centralized log monitoring using Splunk
- Centralized threat monitoring and detailed forensics using Cisco Cyber Threat Defense (CTD)
- Perimeter firewall services
- Remote Access VPN (RA-VPN) services
- Additional compute firewall services for server farm protection using VSG (virtual security gateway)

Management Security

When deploying a multi-tenant cloud data center, service providers need to protect their assets and tenants from security breaches. In a multi-tenant environment, there may be multiple admins managing the infrastructure, applications, and security, and there may be tenant admins accessing their virtual data center. To protect these activities, service providers need to conscientiously address the following:

- Visibility using Cisco CTD
- Event correlation and syslog using Splunk
- Centralized authentication using Cisco Secure Access Control Server (ACS)
- Segmented management traffic and data traffic, with additional firewall services between management plane and data plane

Secure Data Centers for Public and Private Cloud Providers

Aspects of security for secure cloud data centers include:

- Physical Data Center Security, page 2-5
- Network Infrastructure Security, page 2-5
- Content Security, page 2-5
- Data Security, page 2-6
- Operating System Security and Hardening, page 2-6
- Secure Access Control, page 2-6
- Network Visibility and Operation Intelligence and Monitoring, page 2-6

- Compliance, page 2-7

Physical Data Center Security

This includes having secure physical locations and controlled physical access to buildings and data center and network devices. Data centers must have badged or biometrically controlled access for data center administrators and maintenance personnel only. Physical data center security also applies to power management and heating/cooling equipment.

Note Physical data center security outside the scope of this guide.

Network Infrastructure Security

To secure the network infrastructure, SPs must protect and secure the physical and virtual infrastructure. For VMDC Cloud Security 1.0, the infrastructure is made up of the following elements:

- Data center border routers
- Data center edge/aggregation switches
- Access switches
- Load balancers
- Firewalls
- FirePOWER Next Generation Intrusion Prevention System (NGIPS)
- Compute, including Fabric Interconnect and Cisco Unified Computing System (UCS) chassis
- Storage area network (SAN) storage
- Cisco Nexus 1000V virtual switch
- Management components
- Cisco Virtual Security Gateway (VSG)

To provide network security, each element must be deployed redundantly so that the data center can sustain an element failure in any layer. For example, failure of an edge switch, load balancer, or IPS should not result in a system failure. We also recommend multiple paths among the infrastructure elements to protect data center integrity in case of a link failure in any layer.

Content Security

The Cisco Hosted Security Solution (HSS) validated design includes email and web security virtual appliances, ESAv and WSAv, to provide content security services. The HSS solution will reside in the service provider data center, and can be managed directly by the service provider, Cisco Smart Ops team, or a third party managed service provider.

For further details, refer to the HSS Design Guide.

Data Security

To protect a cloud data center in which multiple tenants use the same infrastructure, data paths must be secured so that intrusions and malware are detected and blocked. At a minimum, data must be secured using encryption, both while data is in transit and data at rest.

The data path can be north-south (server to client) and east-west (between VMs). For example, consider a tenant in which departments must be separated so that the departments cannot access applications in other departments. This can be achieved using multiple security elements, such as physical firewalls, NGIPS, and VSG that provide access control in the virtual environment.

Operating System Security and Hardening

We recommend updating the network infrastructure, virtual and physical systems, and applications to the most recent validated releases to ensure that no known security vulnerabilities are present. Install antivirus software and all operating patches and keep them current.

Secure Access Control

In multi-tenant data centers, cloud administrator can potentially access the entire infrastructure, and may have remote access, along with local access, to manage it. Because the infrastructure is the heart of the data center, all communication among devices in the data center must be encrypted; no unencrypted connections to any device should be allowed. For example, accessing a device over a Web interface must use HTTPS using Secure Socket Layer (SSL) 2.0 and higher). HTTP must not be enabled for web portal access.

To reduce security risks when accessing the data center, we recommend implementing RBAC to control access so that administrators have access only to systems for which they have administrative responsibilities.

For example, cloud administrators are typically responsible for the data center infrastructure and may not need access to the individual tenants and applications. Similarly, database and other services and application administrators should not have access to the data center virtual and physical infrastructure, but need access to certain portals. If an SP gives access to a tenant administrator to perform tasks in the SP virtual environment, the access must be read only or otherwise restricted to reduce security breach risks.

Network Visibility and Operation Intelligence and Monitoring

In environments for SPs and large enterprises having SP-type deployments, in which multiple tenants access the same physical and virtual data center infrastructure for services, complete network visibility is required. Centralized logging and event monitoring potentially helps in operations and maintenance. CTD and the third-party logging and monitoring appliance Splunk can provide the required visibility.

Centralized logging, monitoring large amounts of data, and recording transaction history is required for regulatory compliance for FISMA, HIPAA, and PCI DSS.

Compliance

When deploying public cloud data centers, SPs and large enterprises must comply with various industry standards and regulatory requirements, such as FISMA, HIPAA, and PCI DSS. The compliance requirements are based on the provided services.

For financial institutions and onboarding a financial institution or any type of card payments, data centers must comply with PCI DSS. Similarly, for health-care enterprises, data centers must comply with HIPAA standards to secure patients records and other medical research and communications. Data centers used by federal and defense agencies or contractors must comply with FISMA standards to ensure that communications and records are secure and that any compromise results in minimal and isolated breaches.

Solution Components

Table 2-1 summarizes the major solution components.

Table 2-1 VMDC Cloud Security 1.0 Solution Components

Components	Hardware
WAN EDGE	ASR 1000
DC AGGREGATION	Nexus 7000
FIREWALL	ASA 5585
IPS	FirePower IPS 8250
FIRESIGHT MANAGEMENT CENTER	DC 1500
NETFLOW GENERATOR	NGA 3240
LOAD BALANCER	CITRIX SDX 20550
DC ACCESS	Nexus 5548
UCS	UCS 5108 chassis, B200 M3, 2208 IOM
VIRTUAL SWITCH	Nexus 1KV
CISCO THREAT DEFENSE	Collector
LOG MONITORING	Splunk
STORAGE	NETAPP FAS 6080/6040
Virtual Firewall	VSG
Hypervisor	VMWare vSphere 5.1
Virtual Network Management Center	PNSC