CHAPTER 1

Introduction

As service providers increasingly provide cloud-based services to enterprises and small businesses in virtual and multi-tenant environments, their security strategies must continually evolve to detect and mitigate emerging threats. In the VMDC reference architecture, physical and virtual infrastructure components such as networks (routers and switches), network-based services (firewalls and load balancers) - and computing and storage resources are shared among multiple tenants, creating shared multi-tenant environments.

Security is especially important in these environments because sharing physical and virtual resources increases the risk of tenants negatively impacting other tenants. Cloud deployment models must include critical regulatory compliance such as Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS).

The VMDC Cloud Security 1.0 solution enables customers to:

- Detect, analyze, and stop advanced malware and advanced persistent threats across the attack continuum.
- Consistently enforce policies across networks and accelerate threat detection and response.
- Access global intelligence using the right context to make informed decisions and take fast, appropriate action.
- Comply with security requirements for regulatory requisites such as FISMA, HIPAA, and PCI.
- Support secure access controls to prevent business losses.
- Secure data center services using application and content security.

Challenges

When deploying multi-tenant cloud data centers, Service providers are challenged to provide a secure, physical and virtual, environment for tenants. When onboarding tenants of different vertical segments such as financial, health care, or federal the service provider faces a bigger challenge in terms of meeting industry standards and legal compliance within their data center and services. The following sections highlight the key challenges the service provider may have.

Multi-Tenancy and Secure Segmentation

Service Providers (SPs) can use multi-tenant data centers to efficiently and economically provide cloud services using shared hardware and network infrastructures. For security, this approach requires complete separation of network traffic by tenant, along with strict access control policies, because multiple tenants share the same network infrastructure, and compute and storage resources. This is also true for large enterprises deploying private virtual data centers and private clouds, in which internal tenants require separation.

As SPs support multiple tenants in shared data centers, each tenant must be completely and securely segmented to protect them from external threats. Segmentation also provides threat boundaries that can confine threats. Data center tenants must be protected using consistent, ongoing security controls that span the physical and virtual infrastructures.

Secure Data Center Access

In multi-tenant environments with increased mobile device access and network and application virtualization, networks must perform increasing security enforcement in the face of new, highly sophisticated threats. Networks must do this before granting access to applications. As networks become more aware of context and applications, networks are taking over more user authentication and access policy authorization and enforcement tasks from applications.
The network security infrastructure is increasingly required to enforce identity and role-based policies, and to make other contextual decisions. The capability to block traffic to an application or server in the data center or cloud cannot be based simply on typical host source and destination addresses. Network and data center security must be based on the identities and roles of users, security policies, blacklisting, and application transactions.

In multi-tenant data centers, multiple tenants remotely access their applications, which typically share hardware and systems software with other tenants. The access can also depend on context-specific attributes other than identity, such as the type of device accessing the application, the location of the user, and the time of the request. Context-aware policies are increasingly the responsibility of data center firewall and intrusion prevention systems (IPS), intelligent log monitoring and detection. These capabilities must expand to detect and control traffic based on sophisticated policies and monitoring for the presence of malware, unauthorized access attempts, and attacks.

Industry Standards and Regulatory Compliance

Multi-tenant/multiservice data center deployments, which provide multiple cloud services to multiple enterprises, must ensure compliance with industry standards and regulatory requirements to support various different vertical industries, such as health care, finance, and defense. When SPs provide services and provision such tenants, they must comply with the industry standards and regulations, and must provide audit trails.

Solution Benefits

The VMDC Cloud Security Release 1.0 solution integrates Cisco and third-party products to deliver comprehensive, cohesive security frameworks for SPs and enterprises. The solution provides clear guidance for achieving compliance with industry standards and regulatory requirements in public,

private, and hybrid cloud deployments. The solution is built on a vPC-based VMDC release that is extensively validated for performance and scaling, and is widely deployed by enterprises and SPs worldwide. The following significant solution benefits are derived.

End-to-End Security

The numerous aspects of data center security are deployed among several network infrastructure elements. When deploying cloud data centers, service providers need to secure the data center end-to-end to protect their network environment and their customers data. VMDC Cloud Security 1.0 brings together many security devices in a cohesive manner with end-to-end validation to significantly reduce the implementation complexity enabling public cloud providers to improve time to market their services.

Integrates Additional Security Components with VMDC

VMDC provides a seamless approach and architecture for integration with various security elements, such as Cisco CTD, NGIPS, NGA, ACS, and Splunk. This significantly reduces implementation time and risks.

Addresses Key Cloud Provider Challenges

VMDC Cloud Security 1.0 validates use cases that address the key challenges that cloud providers face today, enabling them to achieve end-to-end security and data center compliance.

Provide Guidance for FISMA, HIPAA, and PCI DSS Compliance

VMDC Cloud Security 1.0 undergoes extensive third-party auditing to ensure that the security framework is compliance-ready. This potentially enables cloud providers to achieve compliances in an efficient and cost effective way. The solution provides detailed guidance and gap analysis to reduce the risk of compliance failure.

Audience

This guide document is intended for, but not limited to, security architects, system architects, network design engineers, system engineers, field consultants, Advanced Services specialists, and customers who want to deploy end-to-end security and achieve industry-standards and regulatory compliance in public and private cloud data center deployments.

- Readers should be familiar with the basic concepts of IP protocols, quality of service (QoS), High Availability, security technologies and requirements, and industry-standards and regulatory compliance acumen.
- Readers should understand general system requirements, along with enterprise and SP network and data center architecture.

Solution Scope

VMDC Cloud Security 1.0 provides a complete end-to-end data center security design with best practices for public and private cloud SPs, including:

- Policies, procedures, and best practices for an operational security framework to help mitigate risks, reduce deployment overhead and time to market, and assure cloud security in multi service data centers.
- Integrated, validated end-to-end security using elements in the VMDC reference architecture:
  - FirePOWER Next Generation Intrusion Protection System (NGIPS)
  - Cisco NetFlow Generation Appliance (NGA)
  - Cisco Secure Access Control System (ACS)
  - Cisco Cyber Threat Defense (CTD)
  - Splunk
- Performed Independent assessment and gap analysis of this design, with external auditors, with respect to PCI, FISMA, & HIPAA compliance frameworks.
- Enabling Service providers by leveraging security capabilities within the VMDC architecture, and refreshing prior VMDC cloud security related work where appropriate.
- Extending actionable recommendations to service providers seeking alignment with the aforementioned security compliance framework.

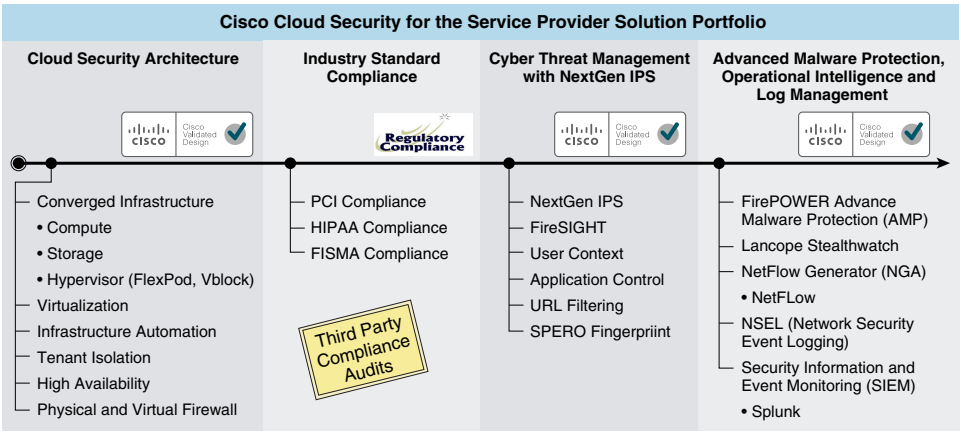
VMDC Cloud Security 1.0 is built on the VMDC 2.3 vPC-based Layer 3 (L3) hierarchical VRF-Lite DC design, supporting multi-tenancy, secure separation, differentiated service tiers, defense-in-depth, and high availability (HA).

This guide:

- Demonstrates recommended best practices and insertion strategies for a cohesive framework comprising key Cisco and third-party security elements.
- Provides comprehensive security guidance and an operational framework to support VMDC customer deployments.
- Provides detailed security guidance for using VMDC to support various security regulatory requirements; this solution release focuses FISMA, HIPAA, and PCI DSS.

Figure 1-1 shows the VMDC Cloud Security 1.0 solution portfolio.

Figure 1-1 VMDC Cloud Security 1.0 Solution Portfolio



Use Cases for End-to-End Secure Cloud Deployments

Cloud data center security is an important concern for both SPs and enterprises. SPs must protect their infrastructure, tenants, and services, and provide HA, and comply with industry standards and regulatory requirements. SPs must ensure that their security implementations do not adversely impact data center and network infrastructure performance.

Enterprises must trust that SPs deploy secure computing environments that isolate enterprise data and applications. Enterprises, like SPs, must comply with regulatory requirements.

This guide covers the following use cases:

- Compliance Fulfillment, page 1-5
- Identity and Access Management, page 1-6
- Next Generation Intrusion Prevention, page 1-6
- Network Visibility, Monitoring, and Threat Detection, page 1-6
- Real-Time Operational Intelligence—Event Monitoring and Logging, page 1-6
- Site-to-Site Virtual Private Networks, page 1-6

Compliance Fulfillment

Service providers when providing services from cloud to various different vertical markets such as card processing, Financial, Healthcare and Federal, they need to abide with the industry standard compliance. To achieve compliance on a complex data center cloud is a tedious, time consuming and costly, and without any proper guidance one can ran into failure and pay hefty fines for not getting compliant. Lack of compliance knowledge can cause major delays in service delivery, incurring huge opportunity costs in terms of time to market.

Note This release covers guidance on FISMA, HIPAA, and PCI DSS.

Identity and Access Management

Identity and access management is one of the issues service providers face in a multi-tenant environment where one or more tenants have access to various components of the data center. This creates a dire security threat if there is no centralized monitoring and management of access control.

Cisco Secure Access Control Server (ACS) provides a centralized highly scalable, policy-based network access and device access administration control platform that operates as a centralized RADIUS and TACACS+ server. It extends access security by combining authentication, user access, and administrator access with policy control within a centralized identity networking solution, allowing greater flexibility and mobility, increased security, and user-productivity gains.

Next Generation Intrusion Prevention

In multi-tenant cloud deployment virtualization and cloud computing introduce new security risks and challenges around new technologies and changing business processes. To succeed, organizations must address threat defense in depth to protect network from external and internal threats.

The Next Generation Cisco FirePOWER IPS provides threat detection capabilities that are currently required in multi-tenant cloud data centers deployments to mitigate new and emerging cyber threats.

Network Visibility, Monitoring, and Threat Detection

Network visibility in a multi-tenant data center with virtual environment is of primary concern for the service providers. They have to ensure that the same controls used in the physical world that are used in the virtual world. These controls need with the same consistent visibility and ability to see any and all traffic in and out of the data center.

This security architecture provides network visibility to monitor and detect the threat of malware spreading throughout a multi-tenant data center. Detecting threats and illegal activity within a network is an essential part of any security framework and architecture.

Real-Time Operational Intelligence—Event Monitoring and Logging

Event monitoring and logging is essential in any security framework and architecture. However, in a multi-tenant cloud data center deployments, it is difficult to identify security events in a timely manner and re-mediate them efficiently.

In VMDC Cloud Security 1.0, Splunk a technology partner virtual appliance is used that provide ability to monitor, search, analyze, visualize and act on the massive streams of machine data generated by the network and security appliances. It also perform monitoring of IT systems and infrastructure in real time to identify issues, problems and attacks before they impact your customers, services and revenue.

Site-to-Site Virtual Private Networks

Until recently, implementing site-to-site virtual private networks (VPNs) required additional hardware, such as an Aggregation Services Router (ASR) 1000 Series router, which increases OPEX and CAPEX. Now, Cisco Adaptive Security Appliance (ASA) products can implement site-to-site VPN inside ASA firewalls.

Incorporating site-to-site design inside ASA firewalls reduces network complexity for site-to-site VPN deployments on multi-tenant data centers significantly. It also reduces CAPEX.

Related Publications

The following design and implementation guides are available for respective iterative releases.

VMDC 2.x System Releases

In the data center portion of the architecture, VMDC 2.x designs centered on traditional hierarchical infrastructure models incorporating leading Cisco platforms and Layer 2 (L2) resilience technologies, such as virtual port channel (vPC), network containers and tenancy models of different sizes, and service profiles, along with network based services, orchestration, and automation capabilities for cloud providers and consumers.

- VMDC 2.3 Design Guide
- VMDC 2.3 Implementation Guide

VMDC 3.x System Releases

VMDC 3.x systems releases introduced Cisco FabricPath for intra-DC networks as an L2 alternative to hierarchical vPC-based designs. FabricPath eliminates the complexities of Spanning Tree Protocol (STP) to enable more extensible, flexible, and scalable L2 designs.

- VMDC 3.0.1 Design Guide
- VMDC 3.0.1 Implementation Guide

VMDC Virtual Services Architecture (VSA) System Releases

VMDC VSA is the first VMDC release dealing specifically with the transition to NFV (Network Function Virtualization) of IaaS network services in the data center. Such services comprise virtual routers, virtual firewalls, load balancers, network analysis and WAN optimization virtual appliances.

- VMDC VSA 1.0 Design Guide
- VMDC VSA 1.0 Implementation Guide