Leveraging Cisco's VMDC Solution to Implement HIPAA Safeguards in a Data Center

October 25, 2013

Leveraging Cisco's VMDC Solution to Implement HIPAA Safeguards in a Data Center

Healthcare organizations in the US are mandated to implement measures to protect electronic Protected Health Information (e-PHI) of their patients in accordance with HIPAA requirements.

Many questions and concerns arise about data centers in the healthcare industry. What are the requirements? How do these requirements affect data center strategies? What best practices can be leveraged for designing these secure data centers? This document summarizes the HIPAA Security Rules safeguards that are relevant in a data center. Cisco's recommended solution, Virtualized Multiservice Data Center (VMDC) is introduced as a reference architecture for accelerating HIPAA implementation and preparation for audits. The VMDC architecture is shown to have elements that map to the HIPAA controls. This document discusses how the Cisco VMDC solution can help implement the safeguards mandated in the HIPAA Security Rule in a data center.

Target Audience

This whitepaper is intended for, but not limited to, sales engineers, field consultants, professional services, IT managers, Cisco channel partner engineering staff, and customers who wish to accelerate their design and implementation of data centers for HIPAA requirements.

Technology Trends

Today's healthcare organizations have keen interests to leverage their Information Technology infrastructure to gain competitive advantage. In particular, the following themes influence spending and investments decisions.

Bring Your Own Device (BYOD)

In favor of working more productively, healthcare employees are rapidly introducing new mobile devices onto the network. Some of these mobile devices are IT-approved, while others are IT-non-approved personal devices. They are sharing data with their patients and other healthcare providers. This new trend raises many questions and concerns for CIOs. How does BYOD impact your data center security strategy? How do you protect patient information stored in your data center if the mobile device is lost?

Explosion of Data

The amount of data produced especially by hospitals, insurance companies, and life science organizations is growing exponentially. The transition to Electronic Health Records (EHR) and enhanced imaging capabilities are just some of the contributing factors. This is a huge problem to solve. How will you provide the massive need for computing, networking, and storage? How do you address this quickly and grow or optimize your Data Center without investing in millions of dollars of new equipment? How will you provide this data for patient access on any device?

Telemedicine

Telemedicine allows healthcare providers to extend their services to patients virtually from a distance. This new trend offers much flexibility and efficiency in patient care, for both the served and under served. This modification of the traditional patient care experience requires extending the network architecture with new devices. Telemedicine, in practice, changes the patient care experience and raises new questions for the CIO. How do you use the Data Center to protect patient data when the information is stored or transferred between two locations? How do you address HIPAA requirements?

Next Generation Data Center

The traditional data center infrastructure was built during a different time addressing different business models and technology trends. Today's healthcare organization CIOs must assess whether the current data center can address new trends such as mobility, data explosion, telemedicine, just to name a few. The journey to a next generation data center or cloud can involve many deployment scenarios including Private Cloud, Public Cloud, Virtual Private Cloud, or Hybrid Cloud. Each of these have its own unique benefits that impacts how healthcare provider IT organizations manage their budgets, operations, and resources. The challenge for Healthcare IT organizations will be understanding a variety of data center designs that address both technology trends and business drivers, while meeting government mandated regulations, such as HIPAA.

Introduction to HIPAA Privacy and Security

The United States government introduced the Health Insurance Portability and Accountability Act of 1996 (HIPAA) with the aim of protecting privacy and security of health information. The Department of Health and Human Services (HHS) published what are commonly known as HIPAA Privacy Rule and Security Rule providing guidance and safeguards for protecting the privacy and security of health information.

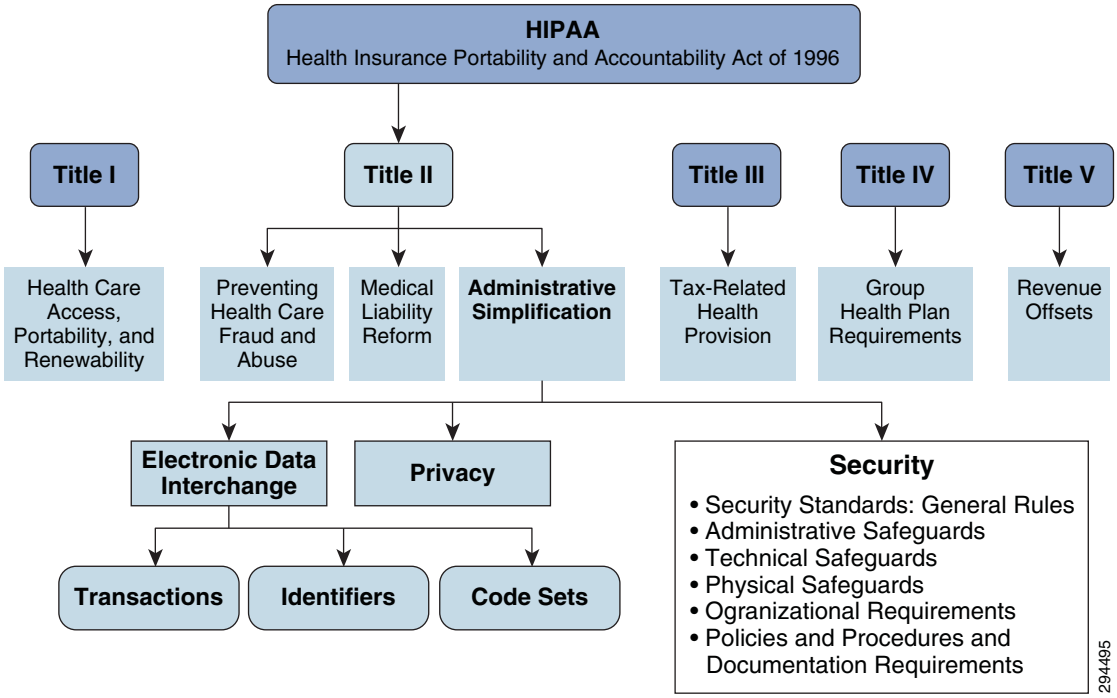
While the HIPAA Privacy Rule establishes privacy requirements for the individual's protected health information(PHI), the HIPAA Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals PHI.

The HIPAA Security Rule focuses on the safeguarding of "electronic protected health information" (e-PHI) that is created, received, transmitted, or maintained by a covered entity.

The HIPAA Omnibus Rule, released January 2013, introduced some significant changes and updates. The changes include expanding the coverage of HIPAA to business associates of covered entities, like cloud/data center providers and increasing the civil penalties for data breach. At the same time, the 2012 audits concluded with some initial findings. The HIPAA Audit Results from the pilot of 115 audits may impact how healthcare enterprises store the e-PHI data and how the healthcare network maintained. Given these latest changes, it's imperative that healthcare organizations understand the impact this may have on the IT group and the network.

Figure 1 gives an overview of the rule and relevance of the same to information security.

Figure 1 HIPAA Components



All HIPAA covered entities and their business associates must comply with the Security Rule, which specifically focuses on protecting the confidentiality, integrity, and availability of e-PHI, as defined in the Security Rule. The e-PHI that a covered entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures.

Security Rule Objectives

As required by the "Security Standards: General rules" section of HIPAA Security Rule, each covered entity or its business associate must:

- Ensure the confidentiality, integrity, and availability of e-PHI that it creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats and hazards to the security or integrity of EPHI;
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

In complying with this section of the Security Rule, covered entities and their business associates must be aware of the definitions provided for confidentiality, integrity, and availability as given by § 164.304 of HIPAA Rule:

- Confidentiality is "the property that data or information is not made available or disclosed to unauthorized persons or processes."
- Integrity is "the property that data or information have not been altered or destroyed in an unauthorized manner."
- Availability is "the property that data or information is accessible and usable upon demand by an authorized person."

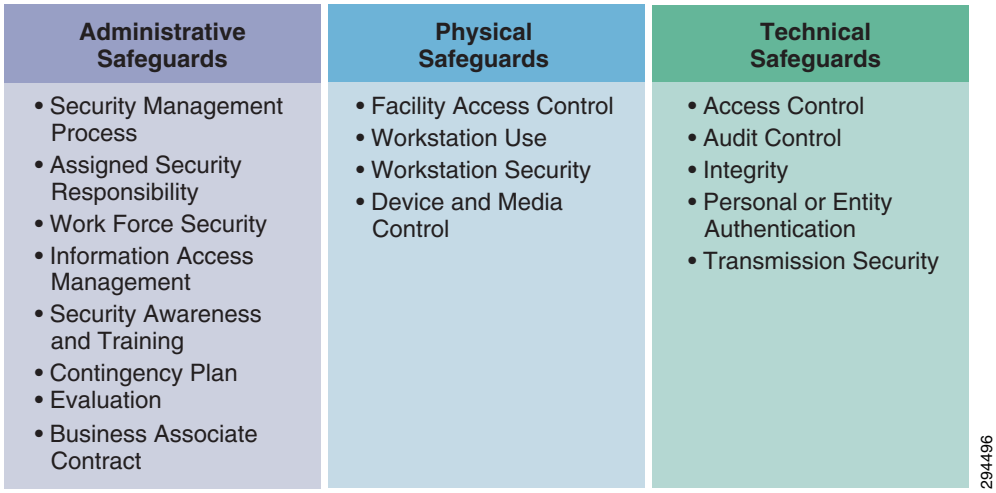
HIPAA Relevance in the Data Center

Protecting the confidentiality, integrity and availability of e-PHI is the key goal of the HIPAA Security Rule. Servers and systems storing and processing e-PHI are housed in the data center and hence, it is imperative that HIPAA security requirements be applied to a healthcare data center. In addition to any in-house data centers of healthcare organizations, the HIPAA requirements also apply to cloud service providers who handle e-PHI data.

Data centers need to adhere to administrative, physical and technical safeguards provided in the HIPAA Security Rule to be HIPAA compliant and to protect patient data.

Figure 2 gives an overview of the security rule and relevance of the same to data centers.

Figure 2 HIPAA Security Rule Components Relevant to Datacenter



Security Threats in the Data Center

The threats that IT security administrators face today have grown from relatively trivial attempts to wreak havoc on networks to sophisticated attacks aimed at profit and theft of sensitive corporate data. Implementation of robust data center security capabilities within a multi-tenant environment to safeguard sensitive healthcare applications and data is a cornerstone in the effort to secure healthcare networks.

The multi-tenant data center is exposed to threats from outside and from other tenants. Security threats from other tenants are an additional security risk that requires mitigation. Attack vectors have moved higher in the stack to subvert network protection and aim directly at applications. HTTP, XML, and SQL based attacks are useful efforts for most attackers because these protocols are usually allowed to flow through the enterprise network and enter the data center.

The following are some of the threat vectors affecting the multi-tenant data center:

- Unauthorized access
- Interruption of service
- Data loss
- Data modification

Unauthorized access can include unauthorized device access and unauthorized data access. Interruption of service, data loss, and data modification can be the result of targeted attacks. A single threat can target one or more of these areas. Specific threats can include privilege escalation, malware, spyware, botnets, denial-of-service (DoS), traversal attacks (including directory, URL), cross-site scripting attacks, SQL attacks, malformed packets, viruses, worms, and man-in-the-middle.

In addition to these threats, many new threats are entering the enterprise network through legitimate applications, such as E-mail or through the Web. Viruses, spam, and malware are examples of such threats. These threats can significantly decrease user productivity, lead to loss of data, and cause sensitive information to be compromised, such as e-PHI.

Hypervisor Compromise

The security of the entire virtual infrastructure relies on the security of the virtualization management system that controls the hypervisor and allows the operator to start guest OSs, create new guest OS images, and perform other management functions.

The hypervisor or virtual machine monitor is an additional layer of software between an operating system and hardware platform that is used to operate multi-tenant virtual machines and is common to IaaS clouds. Besides virtualized resources, the hypervisor normally supports other application programming interfaces to conduct administrative operations, such as launching, migrating, and terminating virtual machine instances. Compared with a traditional, non-virtualized implementation, the addition of a hypervisor causes an increase in the attack surface. That is, there are additional methods (e.g., application programming interfaces), channels (e.g., sockets), and data items (e.g., input strings) an attacker can use to cause damage to the system.

The complexity in virtual machine environments can also be more challenging than in their traditional counterparts, giving rise to conditions that undermine security. For example, paging, check pointing, and migration of virtual machines can leak sensitive data to persistent storage, subverting protection mechanisms in the hosted operating system intended to prevent such occurrences. Moreover, the hypervisor itself can potentially be compromised. A compromise of the hypervisor could result in the compromise of all systems that it hosts.

A hypervisor can control all aspects of all VMs that run on the hardware, so it is a natural security target.

Virtual Network Vulnerability

Most virtualization platforms have the ability to create software-based switches and network configurations as part of the virtual environment to allow virtual machines on the same host to communicate more directly and efficiently. For example, for virtual machines requiring no external network access, the virtual networking architectures of most virtualization software products support same-host networking, in which a private subnet is created for intra-host communications. Traffic over virtual networks may not be visible to security protection devices on the physical network, such as network-based intrusion detection and prevention systems. While some hypervisors allow network monitoring, their capabilities are generally not as robust as those in tools used to monitor physical networks. Organizations should consider the risk and performance trade-offs between having traffic hidden within the hypervisor versus exposing that traffic to the physical network for monitoring.

Administrative Rights

A side effect of virtualized environments is the potential loss of separation of duties between existing administration roles in an organization. For example, in traditional computing environments, computer administrators typically do not configure network security components, such as intrusion detection and prevention systems and firewalls. Network security administrators, on the other hand, can configure such

devices, but typically do not have administrative rights on hosts to grant system access. In virtual environments, the distinct roles of computer and network security administrators can collapse into a single role of a virtual infrastructure administrator. Other distinct roles, such as that of storage administrators, can be similarly affected. Management and operational controls may be needed to compensate a lack of technical controls in virtual environments for maintaining separation of duty.

Cisco Virtualized Multiservice Data Center (VMDC)

The Cisco® Virtualized Multiservice Data Center (VMDC) solution provides design and implementation guidance (available to general public) for deploying private cloud, public cloud, and virtual private cloud. The Cisco VMDC solution reference architecture has proven value for enterprises, service providers, and public-sector organizations that are integrating networking, computing, storage, and management building blocks into a cohesive architecture.

With Cisco VMDC, IT departments have flexibility to deploy physical and virtual applications on a common platform, while preparing to accommodate emerging applications and technology trends, such as big data, hosted collaboration, hybrid cloud and high-performance computing (HPC). The Cisco VMDC mitigates risk through extensive testing and validation of reference guidelines by Cisco.

VMDC Benefits for HIPAA Compliance

Consider the following VMDC benefits for HIPAA Compliance.

Accelerate HIPAA Compliance

Cisco VMDC design options are available for small, medium, or large-sized data centers. Each design has been rigorously tested in Cisco's labs. Integration of the Cisco VMDC solution will help organizations mitigate operational impacts on two levels as a set of guidelines to follow to help organizations with HIPAA compliance. First, adopting organizations will be capable of implementing pre-defined configurations which are designed to be compliant and more importantly, secure. The second level of impact exists where organizations will be capable of integrating the Cisco VMDC solution into a secure environment and adopt existing operational and management controls.

Facilitate HIPAA Audits with VMDC

Cisco VMDC design principles are mapped to HIPAA's Security Rule controls and implementation specifications (discussed in further detail later in this document). IT departments building data centers based on Cisco VMDC to address HIPAA requirements can continuously audit themselves to minimize security breach risks. When there is an audit, the Cisco VMDC design principles can help show areas that are already compliant with HIPAA technical requirements. Retaining control of the operational and management controls while capitalizing on the thought leadership of the Cisco VMDC technical controls will better position the organization for HIPAA audits.

How to Implement

Many of the HIPAA Technical controls can be implemented by integrating the Cisco VMDC solution within data center infrastructure. Cisco VMDC has been widely adopted in enterprise, public sector, and service provider segments worldwide, in both modular and full-scale deployments. Cisco VMDC can be leveraged for HIPAA requirements in new data center deployments or in existing data center expansions. Cisco Advance Services and Channel Partners have extensive experience with Cisco VMDC implementations and can support customizing these reference designs.

VMDC Architecture

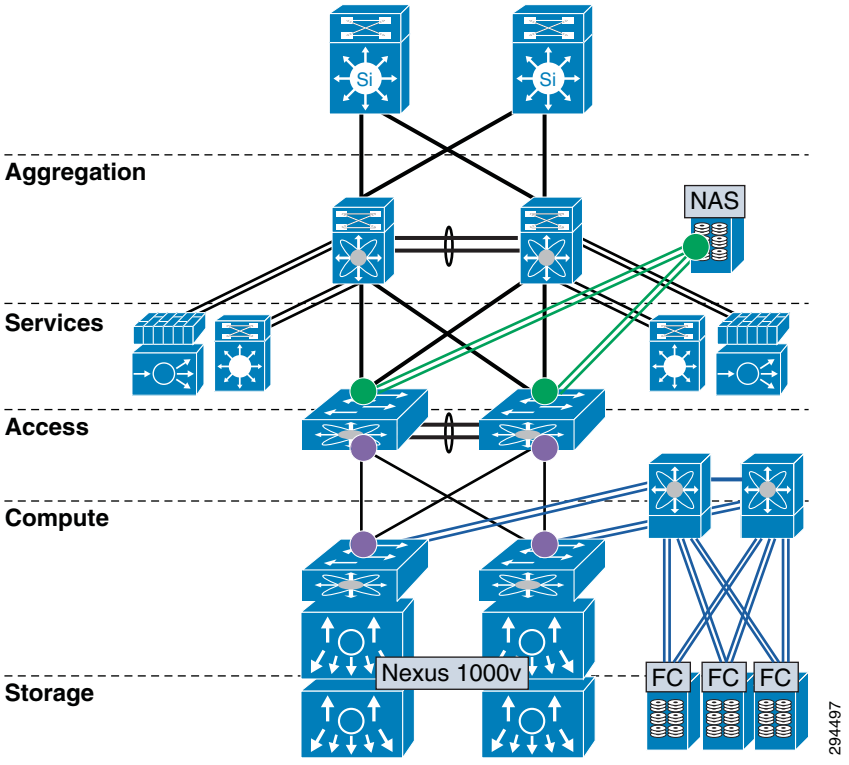
The following VMDC functional layers are detailed.

VMDC Functional Layers

As shown in Figure 3, the VMDC architecture can also be functionally classified into these different categories.

- **Aggregation**—Provides routing connectivity between the data center and the users outside the data center
- **Services**—The Services layer comprises network and security services such as firewalling, server load balancing, SSL offload, intrusion prevention, network analysis, and gateway functions
- **Access**—The access layer provides connectivity between compute appliances and other segments of the data center and beyond.
- **Compute**—The compute layer comprises of computing resources such as servers and hypervisors, and virtual appliances.
- **Storage**—The Storage layer provides storage resources to all servers and virtual machines
- **Management**—The Management layer consists of the "back-end" hardware and software resources required to manage the multi-tenant infrastructure

Figure 3 VMDC Architecture Functional Classifications

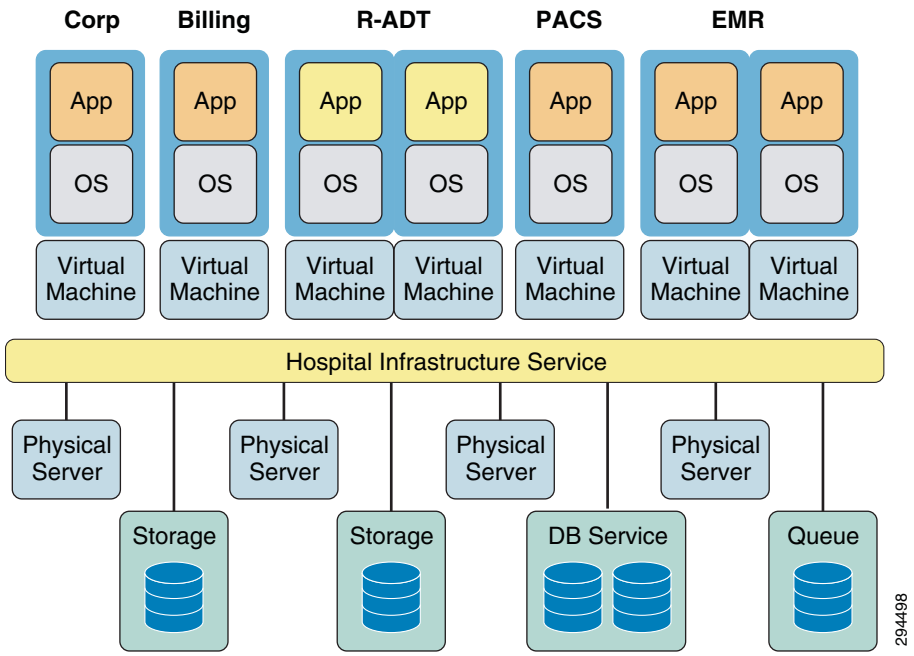


Multi-Tenancy within Healthcare Organizations

Virtualization of compute and storage resources enables sharing across an organizational entity. In contrast, virtualized multi-tenancy, a concept at the heart of the VMDC reference architecture, refers to the logical isolation of shared virtual compute, storage, and network resources. In essence, this is "bounded" or compartmentalized sharing. A tenant is a user community with some level of shared affinity. For example, within an Enterprise, a tenant may be a business unit, department, or workgroup. Depending upon business requirements or regulatory policies, a tenant "compartment" may stretch across physical boundaries, organizational boundaries, and even between corporations.

The multi-tenancy framework of VMDC can be mapped seamlessly to healthcare organizations such as hospitals. Many healthcare organizations are divided into various functional groups that need to be securely separated from other groups. It goes without saying that due to the sensitive nature of patient data, policy enforcement, secure separation, visibility and compliance requirements are critical elements for consideration of data center architecture adoption. Within a healthcare organization, such a hospital, residing wholly within their private cloud, may extend from the tenant's Enterprise to the provider's facilities within a public cloud. The VMDC architecture addresses all of these tenancy use cases within healthcare organizations through a combination of secured data path isolation and a tiered security model. Figure 4 shows the implementation of multi-tenancy within the a typical healthcare organization.

Figure 4 Multi-Tenant Implementation in a Typical Healthcare Organization

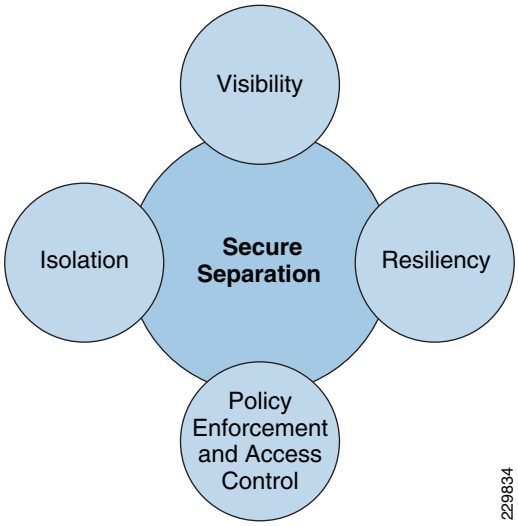


VMDC Security Architectural Framework

Secure separation is the partition that prevents one tenant from having access to another's environment and also prevents a tenant from having access to the administrative features of the cloud infrastructure. The following briefly describes the main security principals that are implemented in this architecture.

- **Isolation**—Isolation can provide the foundation for security for the multi-tenant data center and server farm. Depending on the goals of the design, it can be achieved through the use of firewalls, access lists, VLANs, virtualization, storage, and physical separation. A combination of these can provide the appropriate level of security enforcement to the server applications and services within different tenants.
- **Policy Enforcement and Access Control**—Within a multi-tenant environment, the issue of Access Control and Policy Enforcement looms large and requires careful consideration. Capabilities of devices and appliances within each layer of the architecture can be leveraged to create complex policies and secure access control that can enhance secure separation within each tenant.
- **Visibility**—Data centers are becoming very fluid in the way they scale to accommodate new virtual machines and services. VMDC leverages the threat detection and mitigation capabilities that are available at each layer of the network to gather alarm, data, and event information.
- **Resiliency—**Resiliency implies that end-points, infrastructure, and applications within the multi-tenant environment are protected and can withstand attacks that can cause service disruption, data enclosure, and unauthorized access. Figure 5 shows the security architecture framework implemented within VMDC.

Figure 5 Security Architecture Framework in VMDC



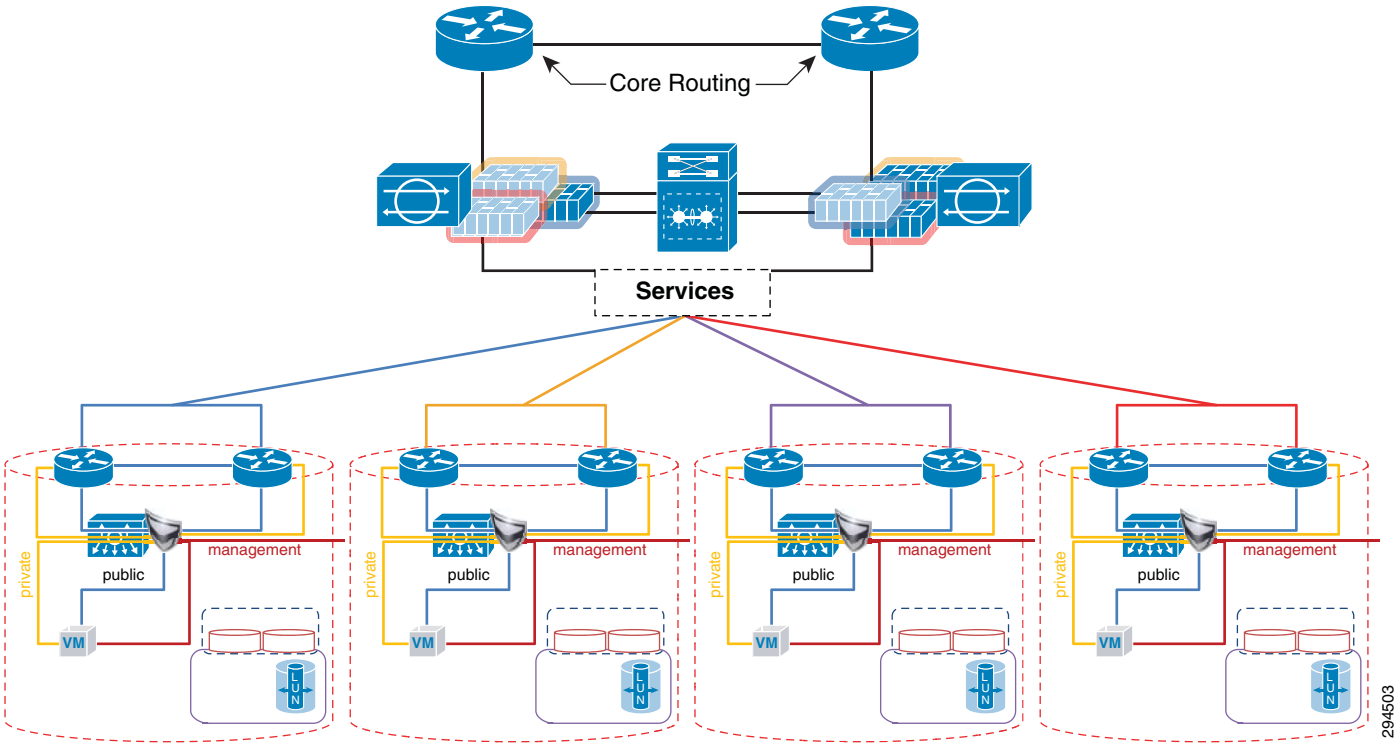
Integration and Implementation of HIPAA Controls using VMDC

VMDC's architectural framework can assist network and security architects to seamlessly implement the various pertinent HIPAA controls. The container construct within VMDC provides the secure overlay of services, a separate management container and flexible service containers that can be leveraged to implement HIPAA controls.

Secure Overlay of Applications and Services

A typical health care organization may deploy different classes of applications or services. As an example, organizations may deploy Unified Communications voice services, Video Surveillance infrastructures, or Medical Records application software and its associated databases within their network infrastructures. VMDC's container model can be leveraged to overlay different applications and services to its own separate container as shown in Figure 6.

Figure 6 VMDC Container Model

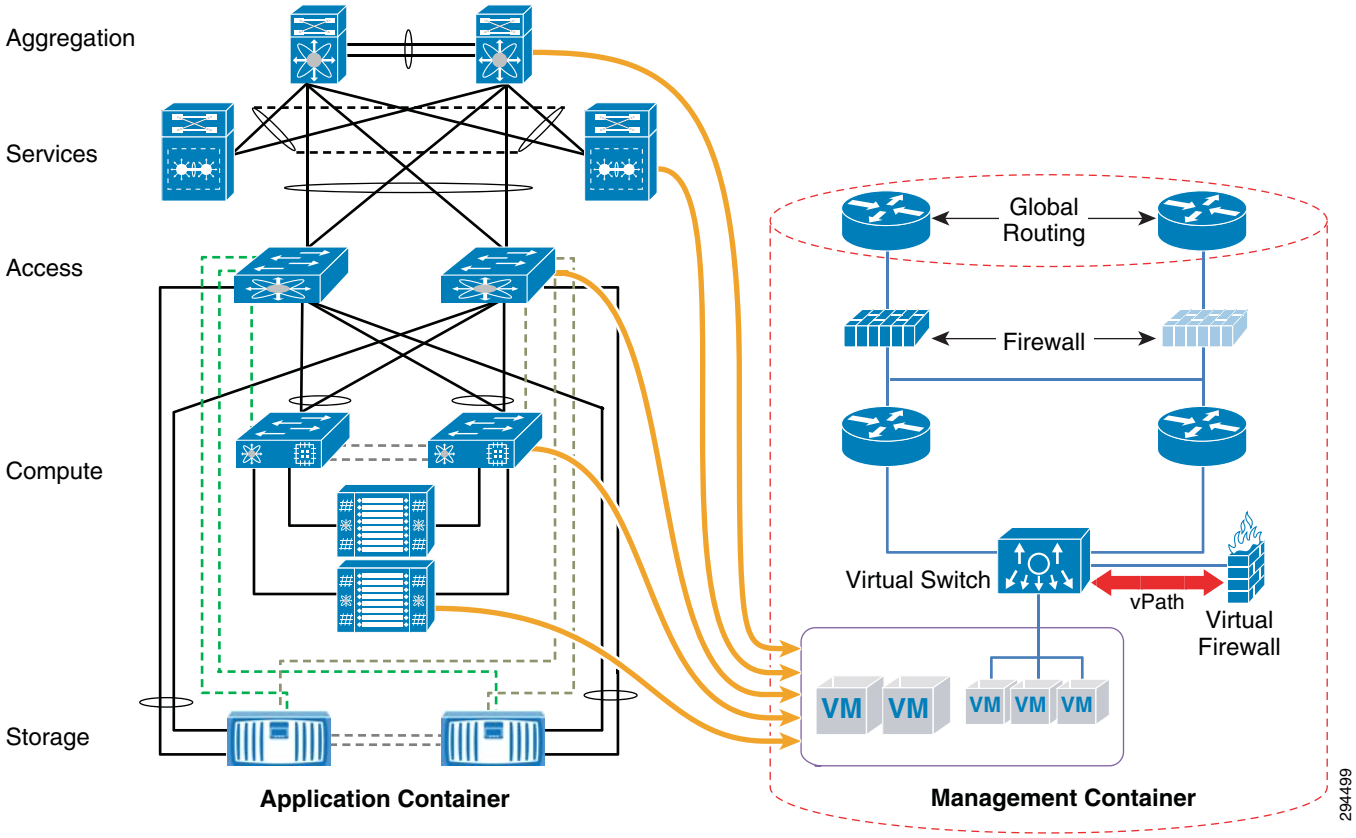


The mapping of services or applications to its own container securely separates them from other segments of the network, and allows for deployment of application-based security policies at the Domain Services Node. In addition, a separate application container provides for secure management of these services that are essential when implementing HIPAA technical controls.

Deployment of a Separate Management Container

A separate management container eases the implementation deployment of access control policies, allows for secure monitoring of network and applications against attacks, and integration of auditing and network analysis tools that is essential for meeting many of HIPAA's technical controls. Figure 7 illustrates the implementation of management container within VMDC.

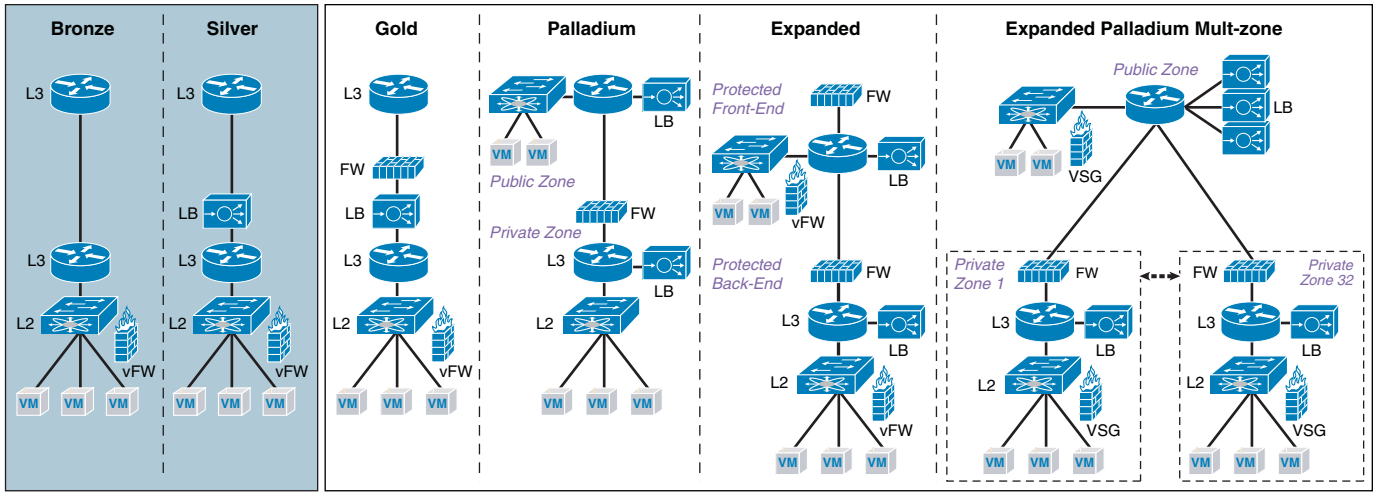
Figure 7 Management Container Implementation in VMDC



Flexible Service Containers

Healthcare organizations deploy a variety of different network applications and services. Each application or service has its own characteristics and needs its own network services, like load balancing or firewalls. VMDC's flexible network containers provide the ability to utilize a variety of network services ,and secure sensitive medical applications and medical data, while at the same time allow less sensitive workloads to only use services that they need. Figure 8 shows the different classes of containers supported within the VMDC architecture.

Figure 8 Container Classes Supported in VMDC



Mapping HIPAA Controls with VMDC Solution

Figure 9 provides VMDC security control mapping to HIPAA controls. Guidelines on how to implement pertinent HIPAA controls are given below.

Figure 9 HIPAA VMDC Security Control Mapping

Security Principles	HIPAA Requirements	Network	Compute	Storage
Secure Isolation of Users, Application and Storage Arrays	164.308(a)(3) 164.308(a)(4) 164.312(a)(1) 164.312(a)(2) 164.312(e)	• ASA/ASASM Firewall Services and virtual contexts • Nexus 1000v Security Features	• vSphere/vCenter • VSG and ASA 1000v	• Vblock, • NetApp Data ONTAP • MultiStore, IPSpaces and VLAN interfaces
Policy Enforcement and Access Control of Patient Data	164.308(a)(3) 164.308(a)(4) 164.312(a)(1) 164.312(1)(2) 164.312(d)	• Cisco ACS device management services • ASA/ASASM Firewall Services and virtual contexts • Security Group Tag • Active Directory Services	• vSphere/vCenter • VSG and ASA 1000v • RBAC and Access Control capabilities	• Vblock, • NetApp Data ONTAP LDAP • Microsoft Active Directory support with RBAC
Visibility and Attack Mitigation	164.308(a)(1) 164.308(a)(5) 164.308(a)(6) 164.308(a)(8) 164.312(b)	• Netflow, ERSPAN, Syslog • ASA/ASASM/IPS Event Notifications • ASA/ASASM/IPS Telemetry Data Export	• UCS Manager • VNMC • DCNM	• Vblock • NetApp Data ONTAP audit logs
Resiliency from Attacks	164.308(a)(1) 164.308(a)(4) 164.308(a)(5)	• Device Hardening • Nexus 1000v QoS • Load balancing and Offload Services	• Device Hardening • VSG and ASA 1000v	• Vblock • NetApp ONTAP advanced settings

Secure Isolation of Users, Applications and Storage Arrays

Protection of medical data records is essential to any security framework used within healthcare organizations. This protection requires the secure separation of unauthorized personnel, isolation of network containers that store sensitive data and prevention of unauthorized access to storage arrays. The technical controls that pertain to secure isolation can be implemented within the VMDC framework using the following general guidelines:

- Placing sensitive servers and applications within a VMDC container that contains a virtual firewall. Security at the application layer (where databases that store sensitive medical data) can be achieved by using an additional virtual firewall. A virtual firewall can protect sensitive data from intra-container (east-west) traffic and even between different components of the same application.
- Additional client-server (North South traffic) traffic flow enforcement can be achieved by utilizing the edge firewall contexts within the VMDC container construct. In addition the VLAN implementation within Nexus 1000V virtual switch and the load balancer within the VMDC containers provides additional separation of traffic.
- Utilizing the appropriate features within the storage appliances in providing isolation of records data. VMDC architecture has been validated with various features used by various storage vendors that provide isolation of storage data.

Policy Enforcement and Access Control of Patient Data

Protection of patient data is at the heart of HIPAA. The technical controls that pertain to policy enforcement and access controls can be implemented within the VMDC framework using the following general guidelines:

- Placing policy enforcement component such as Active Directory within the separate management container.
- Management software such as Active Directory, etc can access the various applications, storage arrays and servers by using the VMDCs back-end management network. Using the VMDC's design, a separate management out-of-band network provides means to configure and monitor these appliances while at the same time guard these appliances against attacks.
- Sensitive servers and applications can be placed in a VMDC container that contains a virtual firewall. A virtual firewall can provide an additional enforcement point at the compute layer.

Visibility and Attack Mitigation

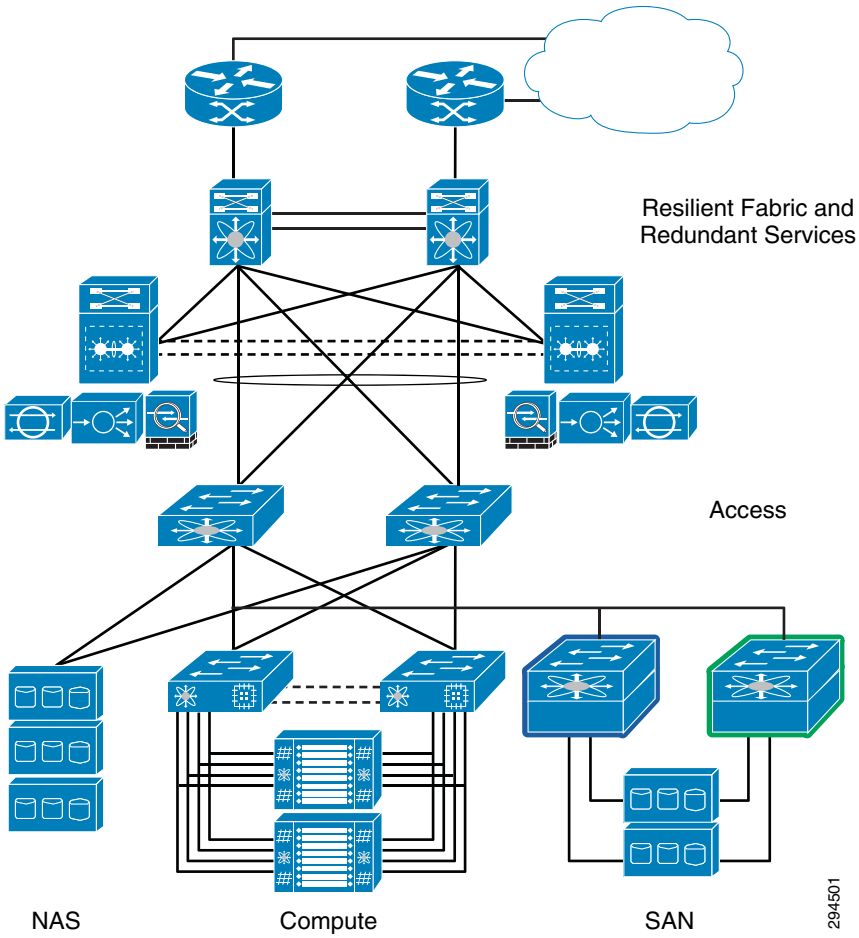
Many Cisco appliances deployed within VMDC architecture can be configured to export network status information to a centralized logging console. The edge and virtual firewalls can send event notification if they detect anomalies within the network. Netflow and ERSPAN features within Cisco routers and virtual switches can be configured to export network telemetry information, and system logging can be enabled on most appliances and storage appliances that enables logging of any aberration on network activities.

Resiliency from Attacks

All Cisco appliances utilized within VMDC can be hardened against Denial of Service(DoS) attacks. Intrusion prevention appliances deployed within VMDC containers provide security against, worms, Trojans, viruses and DOS attacks. Load balancers can shield application servers by preventing the overload of servers by a malicious user.

In addition, the redundant nature of VMDC architecture provides end-to-end high availability and resiliency against the failure of any appliance or switch which was made inoperable during an attack. Figure 10 highlights the redundant design and relevant features deployed within all layers of VMDC that provides high availability.

Figure 10 Redundancy within VMDC



Conclusion

Cisco's Virtualized Multiservice Data Center architecture provides the architectural framework that can help IT architects accelerate HIPAA compliance. VMDC technical framework would also facilitate performing HIPAA audits and provide guidance necessary to implement various HIPAA technical controls.

References

HIPAA Privacy Rule

http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

HIPAA Security Rule

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

HIPAA Omnibus Rule

http://www.hhs.gov/news/press/2013pres/01/20130117b.html

Cisco Virtualized Multiservice Data Center

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/landing_vmdc.html

Cisco VMDC Overview

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns743/ns1050/solution_overview_c22-714480.html

Cisco VMDC Framework

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns743/ns1050/white_paper_c11-714729.html

Cisco Medical Grade Network

http://www.cisco.com/web/strategy/healthcare/cisco_medical-grade_network.html

Cisco Cloud Computing for Healthcare

http://www.cisco.com/web/strategy/healthcare/cloud_healthcare.html

Cisco Compliance Solution for HIPAA Security Rule

http://www.cisco.com/go/compliance

Glossary

HIPAA Health Insurance Portability and Accountability Act
R-ADT Radiology Technology/ Radiography
EMR Electronic Medical Record
PACS Picture Archiving and Communication System
VMDC Virtual Multiservice Data Center
e-PHI Electronic Protected Health Information

Acknowledgements

Axel Nadimi

Alex Nadimi, Solutions Architect, Systems Development Unit (SDU), Cisco Systems

Alex has been with Cisco for the past 15 years and is currently working as a Solutions Architect in Cisco's Systems Development Unit. Prior to this role, he worked as a Technical Marketing Engineer in the Cisco Central Marketing Organization. He has developed solutions and technical guidance on various technologies such as security, VPN networks, WAN transport technologies, data center solutions, and virtualization. Prior to Cisco, he has worked at Hughes LAN Systems and Northern Telecom. He holds a masters of science in electrical engineering from Louisiana State University.

Johnny Tung

Johnny Tung, Product Manager Engineering, Systems Development Unit (SDU) Marketing, Cisco Systems

Johnny Tung has worked as the Solution Go-To-Market Manager for Cisco's Virtualized Multiservice Data Center, Cloud Orchestration BMC CLM, Cloud Service Assurance, and BYOD architectures. He has helped enable Cisco field and partners sell CVD-based solutions. Prior to this role, he was a Market Development Manager and drove Europe switching sales for Catalyst 6500 and 4500 product families. He has led over 20 products and solutions to market and accelerated their adoption amongst enterprise customers. He holds an MBA degree from USC Marshall School of Business and bachelor of science degree in Applied Math from UCLA.

Terri Quinn

Terri Quinn, Security Solutions Manager, Security Business Group, Cisco Systems

Terri has been with Cisco for 18 years and is currently working as a Security Solutions Manager in Cisco's Security Business Group. She focuses on PCI and HIPAA compliance validated solutions. During her tenure at Cisco, Terri has worked in Advanced Services Product Management, Technical Marketing Engineering with focuses on campus design, cable providers, mobility and security; Research Tech Center working on emerging Powerline solutions, and Security Marketin. Prior to Cisco, she worked at SynOptics as a Systems Test Engineer, TAC and Product Manager.

Ramakrishnan AP

Ramakrishnan AP, Solutions Architect, Healthcare Solutions and Services Practice, Cisco Systems

Ramakrishnan Ayyappan Pillai is a Solutions Architect with Cisco Healthcare Solutions and Services Practice and has been engaged in security consulting and assessments in Cisco for six years. He has more than 19 years of broad systems experience, including IT architecture, enterprise and service provider networks, security architecture and IT Governance, Risk and Compliance Frameworks. In the current role, Ramakrishnan's focus is on building compliance and security solutions and services for Cisco's healthcare customers. Ramakrishnan also contributed to development of Cisco Security Control Framework, Cisco Security Assessment Services and created the Cisco Security Control Framework for Healthcare. Ramakrishnan is CISSP, CRISC and ITIL certified and holds a BS Degree in Information Systems from BITS, Pilani, India.

Vinodh Venugopal

Vinodh Venugopal, Network Consulting Engineer, Healthcare Solutions and Services Practice, Cisco Systems

Vinodh Venugopal is a Network Security Consultant with Cisco Healthcare Solutions and Services Practice and has been engaged in security consulting in Cisco for over 5 years. Vinodh has more than 12 years of experience in multiple architectures and systems and has provided security consulting for large customers in APJC and EMEAR. His expertise includes enterprise and service provider architectures and is an expert in assessing complex network architectures for security best practices. In the current role, Vinodh is responsible to assess, design and implement security solutions for healthcare customers and also contributed to the development of Cisco Security Control Framework for Healthcare. Vinodh is a CCIE (Security) and holds Bachelor degree in Engineering from Madras University, India.

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.