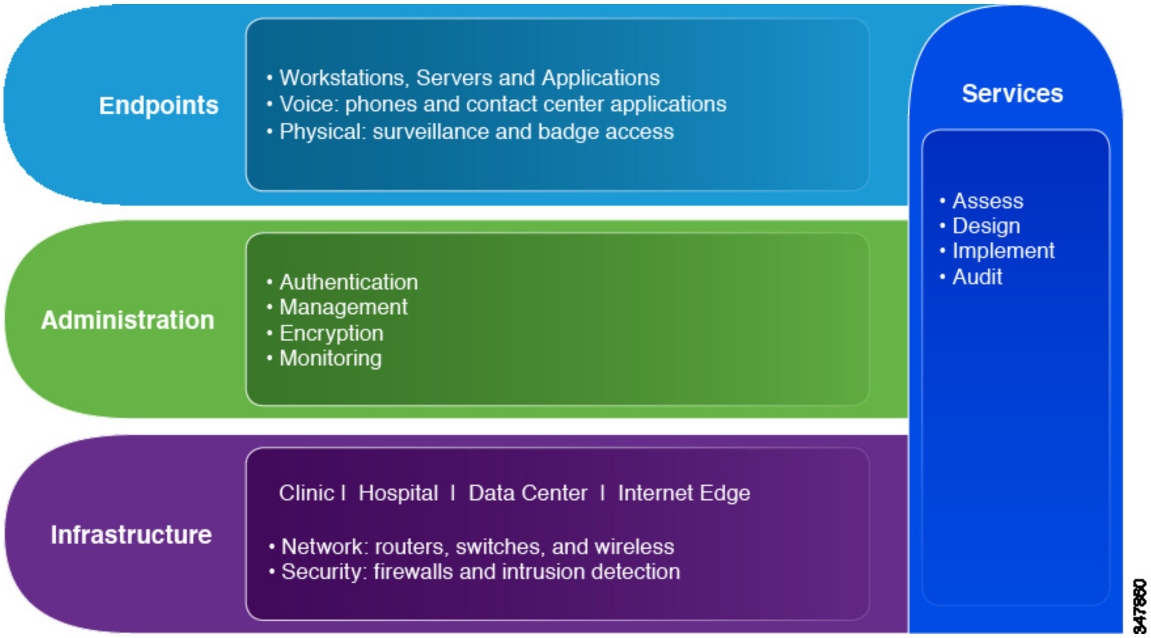
CHAPTER 3

Solution Architecture

Cisco's Compliance Solution for HIPAA Security Rule is a set of architectures, strategic principles, and tactical designs that provide a clarifying understanding of how the network can be used to address HIPAA requirements. Cisco's solution architecture is used as a baseline for demonstrating the range of places that typically exist within an enterprise healthcare provider. This chapter describes the solution architecture in detail so that the HIPAA Security Rule controls can be placed in context. The solution looks at an enterprise from an end-to-end perspective; from a clinic or hospital, where doctors use protected health information (PHI), to the back-end of the data center, where the PHI leaves the providers network to be handled by a business associate.

The Infrastructure layer of the framework shows enterprise locations such as the clinic, hospital, data center, and the Internet edge. The following sections in this chapter show the architectural design considerations of each of these locations. (See Figure 3-1.)

Figure 3-1 Solution Framework


Endpoints
• Workstations, Servers and Applications
• Voice: phones and contact center applications
• Physical: surveillance and badge access
Administration
• Authentication
• Management
• Encryption
• Monitoring
Infrastructure
Clinic I Hospital I Data Center I Internet Edge
• Network: routers, switches, and wireless
• Security: firewalls and intrusion detection
Services
• Assess
• Design
• Implement
• Audit
347660

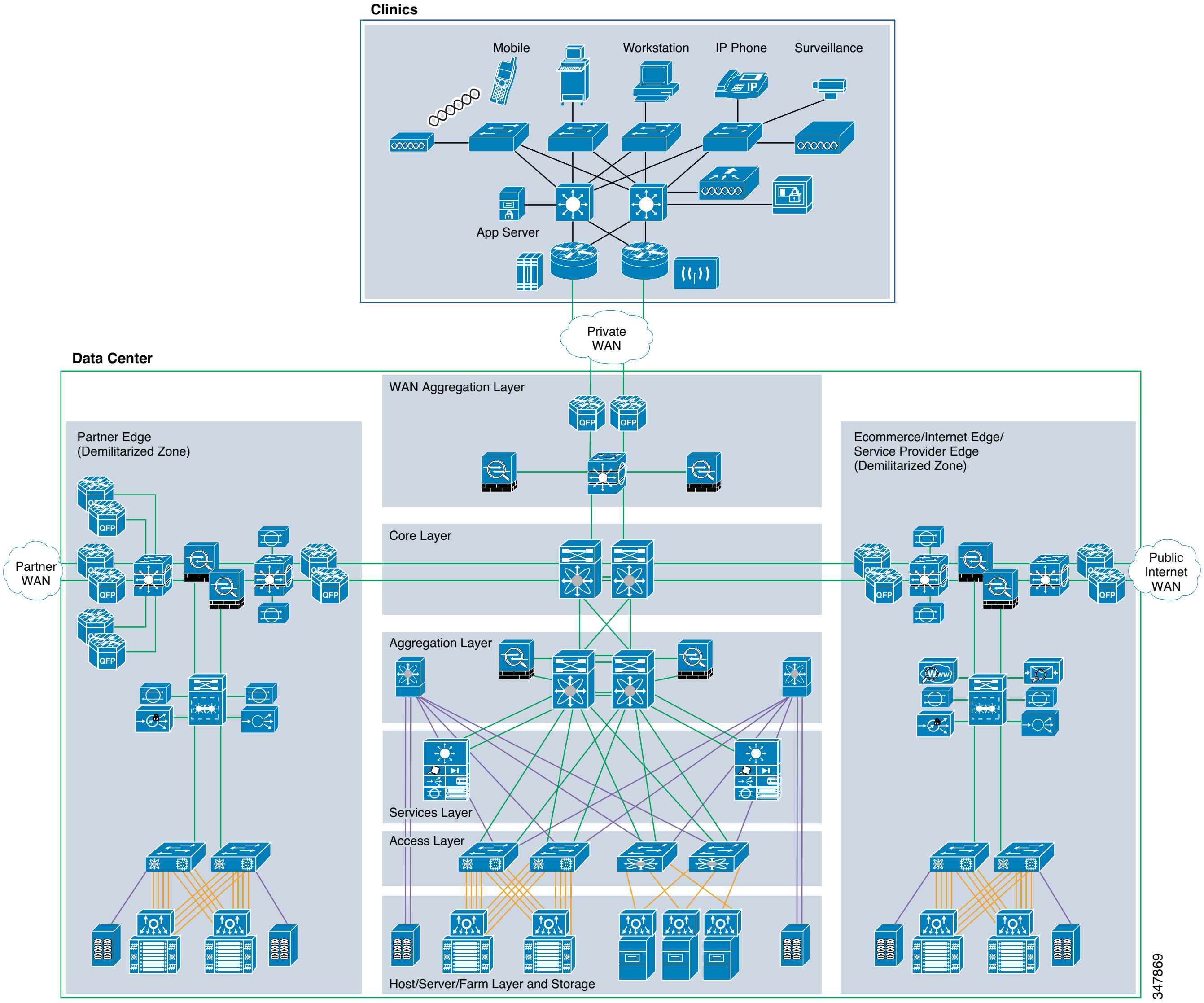
Enterprise Architecture and HIPAA Design Considerations

Healthcare Security control requirements that are derived from the HIPAA Security Rule safeguards apply universally to all sizes of healthcare organization, payer or provider (for example, covered entity), healthcare information clearing houses, Healthcare plans, and Business Associates. The implementation of a secure architecture scales from a single remote clinic to the largest healthcare corporation, with headquarters, regional administrative offices, multiple data centers, points of presence on the Internet, dozens of hospitals, and hundreds of clinics. Cisco's Compliance Solution for HIPAA Security Rule scales both vertically and horizontally to provide the building blocks to construct a compliant enterprise architecture.

Cisco's solution does not guarantee compliance with HIPAA, the ownership of compliance always resides with the covered entity or business associate.

Figure 3-2 shows the enterprise-wide reference architecture and locations that commonly exist in enterprise domain.

Figure 3-2 Enterprise-wide Reference Architecture



Without this contextual reference, it is difficult to discuss specific controls. The following solution principles applied to this architecture reduce risk of losing control of PHI.

- Segmentation

  Within covered entities, the need to segment, separate, and isolate administrative and clinical functions and data is paramount to limiting the scope and depth of security controls that are applied to various forms of data. Generally, institutions that can effectively isolate PHI from other data are most effective at maintaining control over this information. By segmenting clinical information from administrative information, you are able to apply the appropriate controls to effectively protect the information based on its criticality. Enterprise addressing plans should take this into account by separating PHI onto its own address space. Whether in the data center, hospital, or clinic, segregating data leverages the power of the network to help support HIPAA Security Rule safeguards, and best manage risks to PHI and critical medical systems.

  There is an additional benefit beyond security that is a result of effective segmentation. Improved performance can be achieved by designing the architecture to restrict traffic within segments. With the large capacity files for imaging and streaming, this can have a large impact on the response time for healthcare professionals.

- Identity and Access Management

  Identity management, authentication, authorization, and access controls of users/systems to PHI is the central theme in the HIPAA Security Rule safeguards. A strong and manageable identity and access control solution is critical for warranting an assessment of low risk under a customer's risk management program. Effective identity and access management is critical to an organization's ability to meet the Accounting rule.

- Logging, Auditing, and Monitoring

  The need to log, audit, and monitor the access to PHI by users and systems is a critical requirement in the HIPAA Security rule. Centralized application/database/device access logging as well as support for auditing is critical to effectively supporting a covered entity or business associate's breach management strategy. Real-time intrusion detection and protective response within very large and complex networks is critical to identifying compliance issues before they turn into breaches. Logging, auditing, and monitoring are critical to an organization's ability to meet Accounting Rule 164.528, and can help identify whether a compromise has occurred that may lead to a breach notification.

- Encryption

  The ability to encrypt and decrypt PHI represents the most effective and organic control available to resist unwanted PHI data exposures. This applies to HIPAA Safeguard 164.312(a)(1)(2)(iv) Encryption and Decryption.

The following sections describe the major places affected by HIPAA compliance throughout the enterprise. Each section provides design considerations that are affected by HIPAA controls in more detail.

Hospital and Clinic Architectures

Hospitals and clinics provide in-patient and out-patient medical treatment and emergency medical treatment. Each involves creating, receiving transmitting, and maintaining PHI in the forms of electronic medical records, as well as patient treatment information in multiple formats (video, audio, converted photographic and x-ray images, and electronic imaging, and so on).

Design Considerations

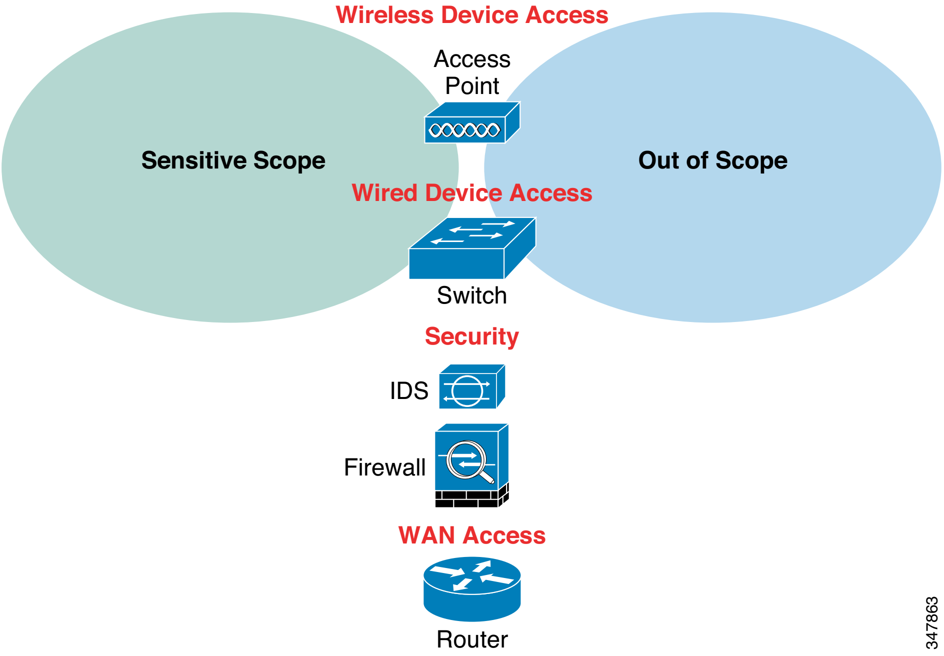
The process of segmenting the wired or wireless networks into *scopes* (that is, devices containing PHI from other devices) is fundamental to demonstrating control and knowledge of the location and use of PHI, as required under HIPAA's Risk Management requirement. The scope of the risk management program and cost of additive control for HIPAA is limited by controlling scope.

Clinics that do not collaborate or share patient data should be isolated from other clinics that do limit the unintentional flow of PHI between them. Consider the isolation of operating units from one another, and from non-required systems in the data center, and the grouping of like functions across segments (for example, LAN/WAN, Internet).

In addition to segmenting, separating, and isolating PHI from other data, VLAN capabilities establish device common "virtual rails" for medical devices, workstations, servers, mobile devices, physical security devices using IP transport, and so on, to simplify control policies between device types and devices.

Figure 3-3 shows the fundamental infrastructure components used within a healthcare location. These components are used in conjunction with each other to segment PHI data from other data.

Figure 3-3 Fundamental Infrastructure Components



Hospital or clinic component designs may scale or consolidate because of the relative size and complexity of the facility, but security functionality is maintained, and each device in the infrastructure is used for a different function.

- The router function can be used for the following:
  - Accessing the WAN
  - Routing between VLANs
  - Providing basic isolation via access control lists (ACLs)

    Routing and access control lists provide segmentation between authorized and unauthorized access on the network. This applies to the HIPAA requirement for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i); and protecting ePHI from parts of an organization that are not authorized such as Isolating Healthcare Clearinghouse Functions 164.308(a)(4)(i). Segmentation also provides for protection against malicious software 164.308(a)(5)(ii)(B) and can modify the accessibility as described in Access Establishment and Modification 164.308(a)(4)(ii)(C).
- The firewall can be used for the following:
  - Filtering inappropriate network packets (data, service requests, service acknowledgements, and so on) via a stateful firewall and supporting security policy controls at the boundary edge; for example, limiting inappropriate clinic-to-clinic cross traffic.
  - Routing between VLANs

    The firewall filtering and routing provide segmentation between authorized and unauthorized access on the network. This applies to the HIPAA requirement for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i); and protecting ePHI from parts of an organization that are not authorized such as Isolating Healthcare Clearinghouse Functions 164.308(a)(4)(i). Segmentation also provides for protection against malicious software 164.308(a)(5)(ii)(B).
  - Detecting and preventing intrusions; (IPS/IDS devices can also be separate appliances) based on the same security policy; for example, detecting and preventing access attempts from non-clinic personnel.

    The IPS/IDS identifies and notifies appropriate individuals that suspicious activity is occurring. This applies to the HIPAA requirement for identifying and responding to suspected or known security incidents (164.308(a)(6)(ii)).
- Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS) monitor for anomalous behavior on the network and alerts administrators (for example, of issues or attacks that are across multiple servers in a hospital or multiple clinics).
  - The IPS/IDS identifies and notifies appropriate individuals that suspicious activity is occurring. This applies to the HIPAA requirement for identifying and responding to suspected or known security incidents (164.308(a)(6)(ii)).
- The switch can be used for the following:
  - Segmenting via VLANs

    This applies to the HIPAA Safeguard for guarding against malicious software as described in 164.308(a)(5)(ii)(B).
  - Accessing wired devices
- The access point can be used for the following:
  - Filtering between authorized and unauthorized access on the network. This applies to the HIPAA requirement for preventing, detecting and containing security violations as listed in the Security Management Process 164.308(a)(i).
  - Supporting wireless segmentation to match the security policy being asserted in the wired network. Segmentation also provides for protection against malicious software 164.308(a)(5)(ii)(B).

  - Accessing wireless devices

The function of each of these devices can be virtualized and consolidated for simplicity, depending on the space and management requirements of the facility footprint. For example, many clinics that occupy leased space are not in control of their IT closet, and may have several power, wiring closet, rack, and cabling restraints that benefit from virtualized devices that reduce the physical footprint of the infrastructure.

Identity and Access Management should be centralized, as is discussed in the data center section. However, when connectivity is lost to the centralized services, local identity and access management should be configured for emergency access.

Logging should be centralized and is discussed in the data center section. However, local device logging should be enabled if centralized connectivity fails. This ensures that auditing and monitoring can be used.

Encryption of PHI across networks is necessary as described in the HIPAA Security Series published by HHS: Covered entities must consider the use of encryption for transmitting ePHI, particularly over the Internet. As business practices and technology change, situations may arise where ePHI being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis shows such risk to be significant, a covered entity must encrypt those transmissions under the addressable implementation specification for encryption; there should be application layer encryption, but additional consideration should be given when PHI leaves the clinic over Internet service provider (VPN) or wireless networks (WPA2).

Conversely, in clinics that own their own space, are moderate size, or have a number of clinical subsystems and technology tools, each of these devices can be increased in number depending on the resiliency and redundancy requirements of the business. For example, if clinic connectivity is a business priority, using redundant routers for redundant WAN access might be a requirement to ensure that connectivity is maintained.

Clinics routinely have minimal space for the technology infrastructure. The ability to implement the technological components securely in minimal space is an advantage.

Regardless of how the IT infrastructure is designed from an ownership and scale perspective, the same types/locations of controls should be consistent and available across the various configurations.

From a control prospective, most health groups "home run" their Internet access from the remote clinics and connected hospitals into their central data center to more effectively manage Internet access, filter content, and enforce data loss prevention, control email connectivity and provide for email filtering in both directions.

This perimeter is typically secured as a demilitarized zone (DMZ) using firewalls and IDS/IPS. Whenever you introduce any type of untrusted network (wireless, Internet, microwave, satellite, cellular, and so on) into the healthcare environment, you have effectively created a new external perimeter that must now be secured with a firewall and intrusion detection/prevention system. Table 3-1 defines the types of factors that affect clinic controls and requirements.

Table 3-1 Healthcare Services and Corresponding Compliance Controls Located at Facility

Hospital/Clinic Service Types	Controls Recommended	Relevant Solution Products
Electronic medical records (EMR) systems	Data encryption/decryption Auto-log-off controls Passwords	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x Switch
Wired and wireless medical devices	Data encryption/decryption Auto-log-off controls Passwords	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x Switch

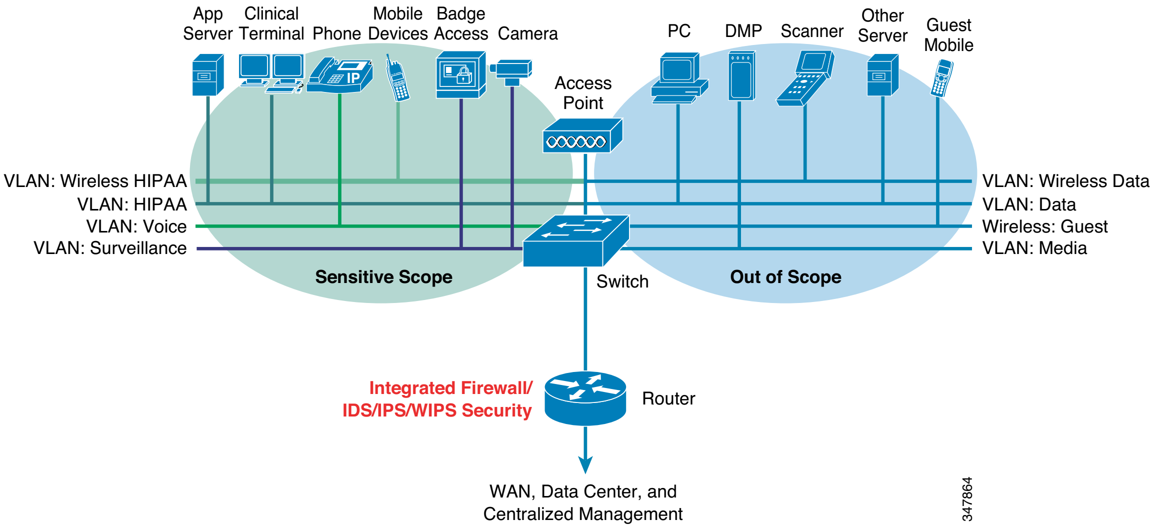
Table 3-1 Healthcare Services and Corresponding Compliance Controls Located at Facility

Imaging systems	Data encryption/decryption Auto-log-off controls Passwords	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x Switch
Wireless tablets and roll-around carts	Data encryption/decryption Auto-log-off controls Passwords	Cisco ISR, Cisco ASA, Cisco IPS appliance, Cisco Unified Wireless
Hospital/clinic LAN/WAN	Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS Appliance
Patient registration workstations Nurse station workstations	Authentication controls Passwords	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x Switch
Internet demarcation	Data encryption/decryption Firewall, IDS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS Appliance

The fundamental reference architecture assumes that a covered entity or business associate may eventually need to scale to these levels of services, but not necessarily immediately. From a facility perspective, Cisco's Integrated Services Router (ISR) performs each of the functions listed in Table 3-1. This allows a provider to grow with its investment by purchasing a router that can scale by different license keys for different services without having to rip and replace. For example, a clinic can purchase an ISR for basic WAN connectivity. When the business wants to introduce wireless to the facility, the merchant can unlock the firewall/IPS/IDS feature set with a license.

The fundamental healthcare reference architecture in Figure 3-4 shows the solution framework endpoints/applications within the context of the fundamental healthcare component's infrastructure.

Figure 3-4 Fundamental Reference Healthcare Architecture



In-scope devices can include the following:

- Medical devices and imaging subsystems
- Mobile video/audio carts and wireless tablets
- Physical access, ID, and surveillance subsystems for the facilities
- Clinical and administrative workstations
- Primary EMR servers

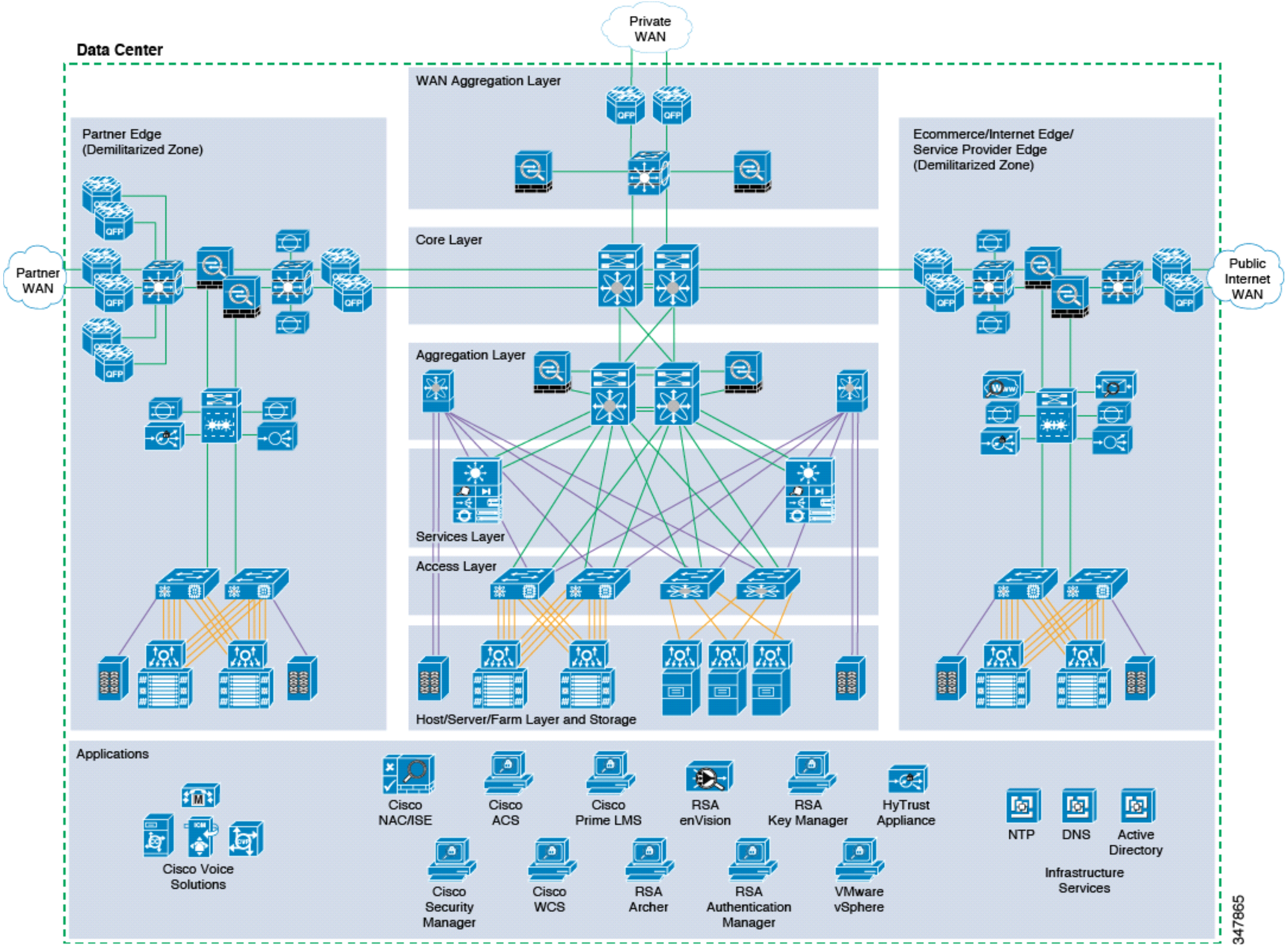
In general, an additional VLAN for management of infrastructure should be distinctly defined. The remaining devices at the facility level are considered *out-of-scope* and do not need to be audited, given that they are on their own network and segmented via firewall/IPS/IDS from the sensitive networks.

The HIPAA facility model and its controls were applied to multiple healthcare formats ranging from clinics to hospitals and are shown in Chapter 4, "Solution Implementation," in detail. This section provides sample addressing plans used. Many designs can be extracted by understanding and using the Healthcare Reference Architecture shown above, but the overall functions are essentially the same.

Data Center

The data center provides a covered entity or business associate with the ability to centralize, aggregate, consolidate, share, maintain, and control their storage of PHI. (See Figure 3-5). The data center is also the place where management systems are deployed. The data center provides centralized control from an administrative perspective because administrative and management tools can span across the data center servers, hospital systems, and remote clinic systems. This minimizes operational overhead and enforces the security policy.

Figure 3-5 Data Center Architecture



Design Considerations

Data centers can house many types of functions and the term itself can encompass narrow and broad aspects. For the purposes of this guide, data centers include the following functions:

- WAN aggregation layer—Aggregates the clinic and hospital WAN connections to the core
- Core layer—Highly available, high-speed area that is the central point of connectivity to all data center areas
- Aggregation layer—Aggregates the services of one area and connects that area to the core
- Services layer—Data treatment and manipulation occurs between access layer and aggregation layer
- Access layer—Server-level access and connectivity between hosts/servers to the services and aggregation layers, depending on the nature of the application
- Host/server farm—Physical servers, virtualized servers, and appliances' host applications
- Storage—Storage area networks (SANs)
- E-commerce/Health—Internet-based transactions for prescription renewals, payment of bills
- Internet/service provider edge demilitarized zone (DMZ)—Secure connectivity to the Internet
- Partner edge DMZ—Secure segmented connectivity to partners

Common data center security features include, but are not limited to, the following:

- Standardized equipment and software images that are deployed in a modular, layered approach simplify configuration management and increase the systems availability.
- The highly available data center design permits highly resilient access from clinics to core data and storage services.
- WAN aggregation alternatives allow flexible selection of service provider network offerings.
- The service aggregation design allows for a modular approach to adding new access layers and managing shared network services (for example, firewall, IDS, application networking, wireless management)
- Firewall, IDS, and application networking services are available at the service and aggregation layers of the data center.
- Scalability accommodates shifting requirements in data center compute and storage requirements.
- WAN access speeds are typically the limiting factor between the clinic network systems and the WAN aggregation layer.
- Backup network connections from remote facility networks to the data center are recommended when PHI is transported via the WAN.

Related to segmentation between clinical and other systems, clinical data should be, to the extent possible isolated to reduce the risk of copying PHI on to non-PHI data sets, databases, file, file shares, or system drives and backups. Isolation can be accomplished at both the system and network levels by organizing clinical systems in separate VLANs from other systems, and by enforcing access restrictions between dissimilar system/server functional groups. HIPAA 164.308(a)(4) Isolating Clearinghouse Functions requires that covered entities must create separation of PHI from the larger organization, which can be accomplished through router/switch segmentation functionality or through the use of firewalls to more effectively manage a uniform segmentation "policy" across multiple devices and interfaces. Consideration should be given to isolating PHI traffic between servers to a common and small (for example, controllable) set of VLANs, to the exclusion of other systems.

Related to segmentation between internal data center systems and Internet-exposed components, an organization must have policies and procedures in place for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i). Additionally, HIPAA §164.312(c)(1) Data Integrity mandates procedure (or technical controls) to protect PHI from improper alteration or destruction. The use of firewalls as a demarcation and access management point allows the customer to establish and manage a common security policy for data flows between data center and Internet-exposed devices/systems to support maintaining data integrity around PHI. Along with strong application and system controls, the use of network restrictions aligns with the defense-in-depth strategy. Obfuscate internal addressing schemes to the public, especially addresses of PHI storage devices and backups. Consider the use of enterprise-class firewalls to provide a unified security policy management framework to manage critical network boundaries between the covered entity/business associate and the rest of the Internet.

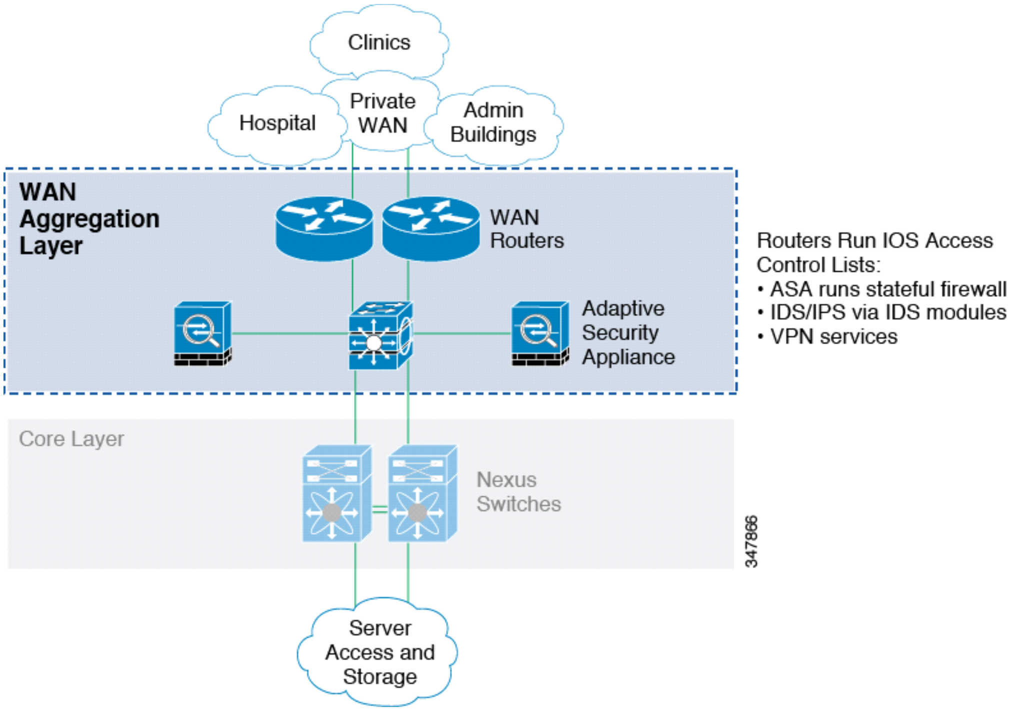
Identity management, authentication, and authorization of users and systems to PHI; and access controls between users/systems and PHI is critical to enforcing HIPAA safeguards. Having the ability to individually grant or deny access to a user or by system at the network (device) and/or system (server) levels provides the granularity of control necessary to support HIPAA safeguards. Consider leveraging centralized identity and access management functions across health groups, and within hospitals and clinics to best support restriction of users and systems to PHI. Ensure that the ability to control access during both routine and emergency access is supported. 164.312.(a)(1) Access Control requires that technical policies and procedures be implemented to allow access only to persons or software programs that are authorized.

An ability to seamlessly encrypt and decrypt PHI and to share encrypted files across the network provides opportunities for real-time PHI sharing and collaboration to improve patient care. The ability to seamlessly exchange PHI or various types, all in encrypted form, reduces the potential places where PHI can be breached. Encrypt PHI (and all operating data if possible) while in transit across the enterprise and when transiting the Internet or other public networks. Consider leveraging encryption management and engines to encrypt/decrypt all PHI when stored. Providing the capability to encrypt traffic sent over public networks helps an organization meet the HIPAA requirement for Transmission Security 164.312(e)(1), Integrity 164.312(e)(2)(i), and Encryption 164.312(e)(2)(ii).

WAN Aggregation

The WAN aggregation layer is a transit network that aggregates the connections from the healthcare locations, backstage locations, and offices, as shown in Figure 3-6.

Figure 3-6 WAN Aggregation Layer


Clinics
Hospital
Private WAN
Admin Buildings
WAN Aggregation Layer
WAN Routers
Adaptive Security Appliance
Routers Run IOS Access Control Lists:
• ASA runs stateful firewall
• IDS/IPS via IDS modules
• VPN services
Core Layer
Nexus Switches
347866
Server Access and Storage

Design Considerations

Segmentation is used at the WAN aggregation layer to minimize the PHI scope from sites that do not have PHI. The WAN aggregation layer needs Layer 3 filters to restrict PHI data from crossing into sites that do not have the need for PHI data.

Two options are possible at this layer for Layer 3 filters at the WAN aggregation layer:

- Firewall appliance—Interior to the WAN edge routers, a dedicated firewall appliance is used to secure incoming WAN traffic and to terminate remote facility VPN connections. This design provides the highest scalability. When managed centrally over several firewalls, a unified security policy can be exerted over the organization with the minimum of administrative overhead, and in a repeatable way that supports effective risk management. The firewall provides multiple safeguards to help a healthcare organization meet HIPAA safeguards. The firewall filtering and routing provide security between authorized and unauthorized traffic from an unsecured network. This is extremely important when connecting the organization to external networks such as the Internet or a business associate. This helps an organization meet the HIPAA requirement for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i).

- Cisco IOS Software firewall routers—Many Cisco routers also support the Cisco IOS security software option that includes a firewall feature. Cisco recommends the use of the Cisco IOS Security feature set in hospitals, branches, and teleworker deployments, because of a much lower number of users and connection rates than at the Clinic WAN aggregation head end location.

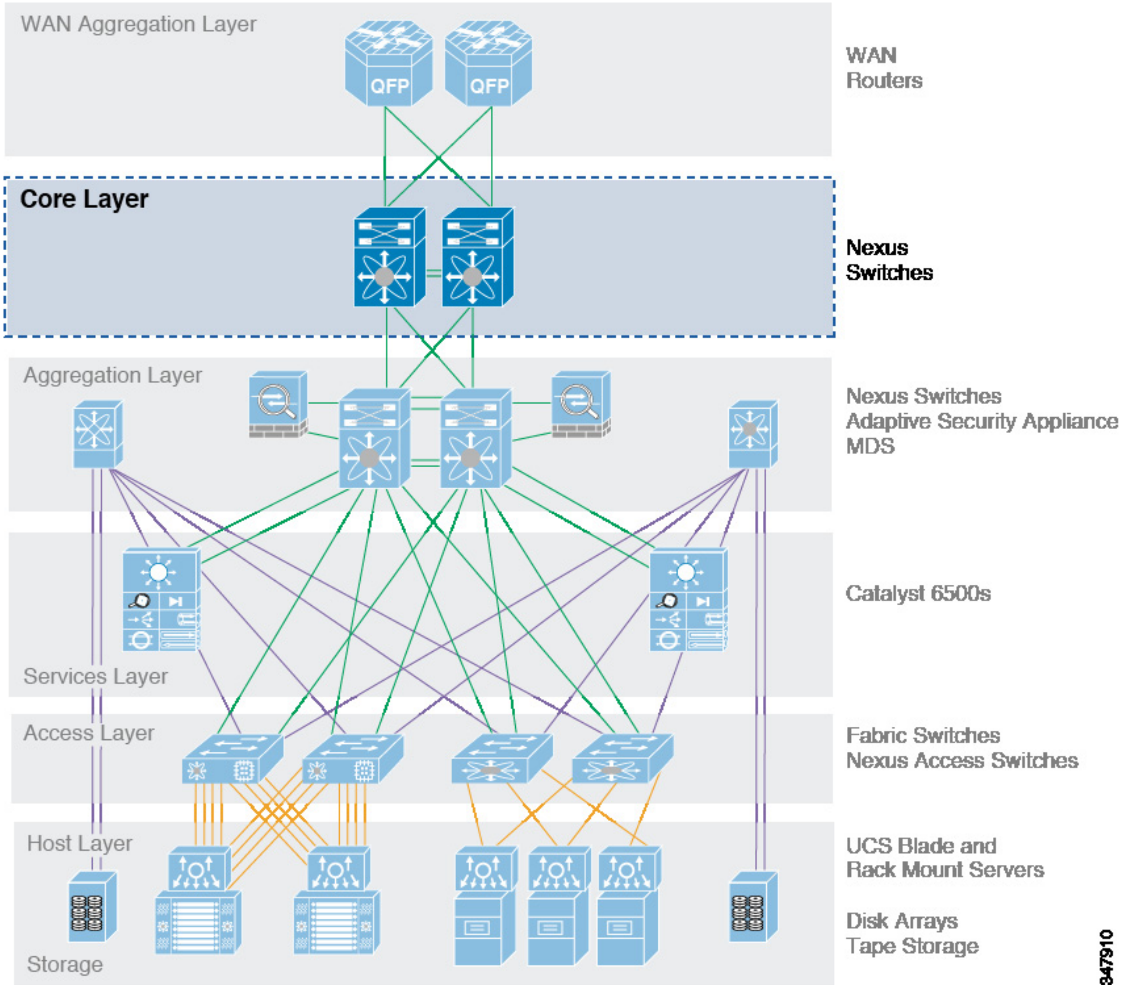
There are two typical WAN speed categories for a WAN aggregation network: less than and up to OC3 (155 Mbps), and OC12 (622 Mbps) and above. The choice of these two network speeds determines the platform set to select from Cisco. In addition, this design creates two profiles for each WAN speed. These profiles are designed to provide guidance when designing a WAN edge network, regardless of which enterprise WAN architecture is selected. The profiles for each WAN speed investigate integrated versus dedicated chassis for each functionality component, as highlighted in the previous section. Some customers prefer a highly integrated solution where most, if not all, of the WAN edge functions described in this document reside on a single or very few network devices. Other customers prefer the granularity and scalability of these same functions separated across multiple network devices.

The WAN aggregation architecture is based on the *Infrastructure Protection and Security Service Integration Design for the Next Generation WAN Edge v 2.0*, which can be found at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/IPSNGWAN.html

Core Layer

The core layer provides the high-speed packet switching backplane for all flows going throughout the data center, as shown in Figure 3-7.

Figure 3-7 Core Layer



Design Considerations

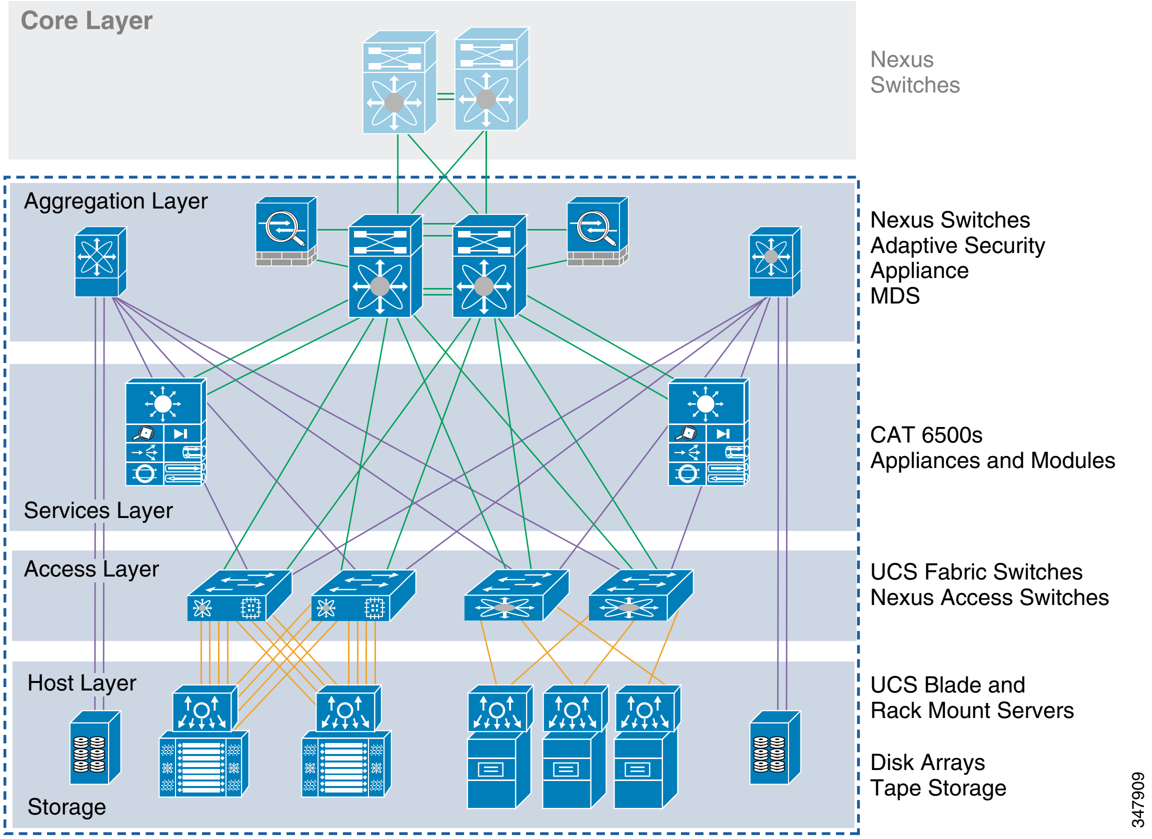
Depending on the risk management strategy, high availability may be a requirement. The core is the fundamental layer of an enterprise architecture that provides high availability and connectivity between all other layers. The core layer provides connectivity to multiple aggregation layers and provides a resilient Layer 3 routed fabric with no single point of failure. The core layer runs an interior routing protocol, such as Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing Protocol (EIGRP), and load balances traffic between the core and aggregation layers using the Cisco Express Forwarding (CEF)-based hashing algorithms. The core is not a perimeter; no security filtration should be performed at this layer. The core layer support the efficient transport of clinical, imaging, and administrative data without throughout issues or bottlenecks, thereby ensuring the highest patient care through data availability to the care team.

The core, services aggregation, and server access tiers of the multi-tier data center architecture was based on the design documented in the *Cisco Data Center Infrastructure Design Guides*, which can be found at the following URL:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns994/landing_dc_infrastructure.html

Aggregation Block

An aggregation block is a combination of the aggregation, services, and access layer systems. It represents a repeatable, implementable template for scaling applications and services within the data center. (See Figure 3-8.)

Figure 3-8 Aggregation Block



Design Considerations

Segmentation can occur at this layer by separating entire aggregation blocks or within the block. These blocks can be zoned by function or compliance types. For example, an organization that has sensitive healthcare information may be zoned away from the payment card sensitive information. Zones are a best practice to isolate applications and services based on their individual policy requirements. You can securely mix in-scope and out-of-scope applications and services within a single aggregation block but you may use entire aggregation blocks separately to ease administration as policies change over time. The aggregation layer uses Layer 3 filters to segregate and protect the edge of the scope of compliance.

In the services layer, server load balancing and wide-area application services (WAAS) are used at this layer to optimize applications. Using these devices to support HIPAA-relevant applications brings these devices into scope and susceptible to the same safeguards. For more information on understanding these safeguards and controls, consult [Chapter 5, "Component Assessment."]

In the access layer, switches provide both Layer 2 and Layer 3 topologies to enable segmentation within the aggregation block. The solution management servers connect to the network in this layer. They are centralized, segmented from other business application servers, and protected by firewall services from the service aggregation layer above.

In the storage layer, a combination of disk encryption provided by the Cisco MDS encryption card, fibre-channel zoning, and logical unit (LUN) masking/zoning were used in the storage implementation of this solution. By deploying zoning within a Fibre Channel fabric, device access is limited to devices within the zone. This allows the user to segregate devices based on access to a particular storage device (disk array). This applies to HIPAA Safeguard 164.312(a)(1)(2)(iv) Encryption and Decryption. This is a requirement in a data center environment in which multiple file servers in the data center server farm are connected to the same SAN fabric, and access to PHI data must be restricted to a subset of servers. LUN masking takes zoning beyond the Fibre Channel switchport level by restricting access to specific LUNs on a given disk array. Only specific devices belonging to the LUN zone are able to access those sections of the disk. Applications can be grouped by PHI use/storage, with encryption support on some devices but not necessarily on all arrays. Encryption keys for storage are managed by Cisco Key Manager and RSA Data Protection Manager. This provides a uniform method to control encryption keys across the enterprise. Key management can be structured by organizational unit, so the multiple business units can be supported under the same key management scheme, and the potential to intermix or misroute PHI (when encrypted) can reduce the potential for breach. This measure can mean the difference between losing PHI when other security controls are intentionally compromised, and maintaining control over that data.

In the host layer, server virtualization technology can be used to further establish separation between applications containing PHI and other applications, and to organize process-intensive applications into demand-groups to ensure timely file retrieval and update. Individual blades within a blade server chassis can be used to segment sensitive and non-sensitive applications because they run independent hypervisors. Because hypervisors are considered insecure, when mixing sensitive applications with non-sensitive applications (mixed-mode) across the same hypervisor, the non-sensitive applications are now in scope.

While meeting the central focus of this design guide by recommending an architecture that meets the HIPAA Safeguards, additional QoS parameters can increase performance using the recommended segmentation strategies.

For more information, see the following URL:
http://www.cisco.com/en/US/partner/solutions/ns340/ns414/ns742/ns743/ns1050/landing_vmdc.html

The host layer/server farm is where the centralized applications are deployed for managing and enforcing the segmentation policy, logging, auditing, monitoring, identity authentication and authorization.

Table 3-2 lists descriptions of applications for administrators.

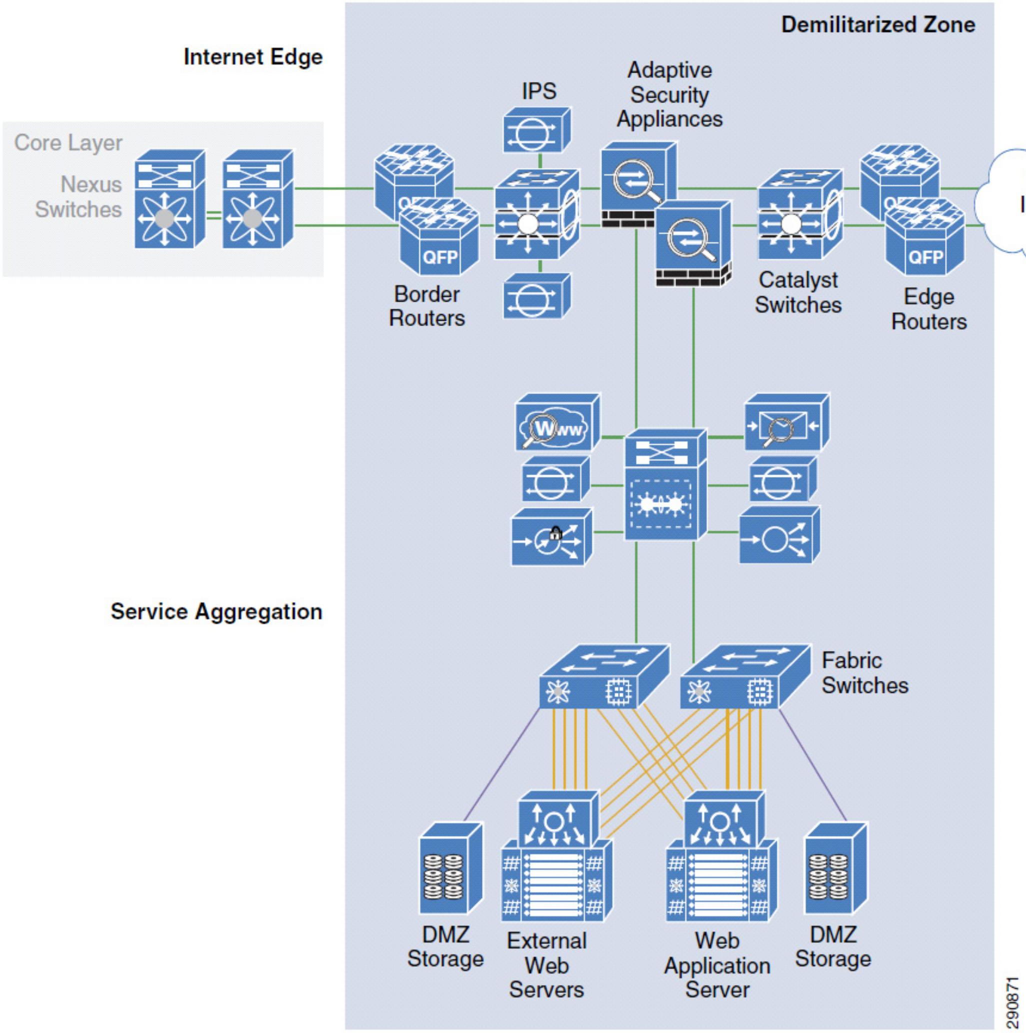
Table 3-2 Centralized Toolkit for Administrators

Function	Solution Component Options
Physical Security	
Closet to building access	Cisco Physical Access Manager
IT space intrusion detection	Cisco Physical Access Manager
Video surveillance	Cisco Video Surveillance Manager
Identity Management, Authentication, and Access Controls	
Device AAA	Cisco Secure ACS, Cisco ISE
Two-factor remote	RSA Authentication Manager
Directory services	Microsoft Active Directory
Logging, Auditing and Monitoring	
Event correlation	RSA enVision
Policy enforcement	Cisco Prime LAN Management Solution (LMS)
Corporate policy	RSA Archer
Virtualization	EMC Unified Infrastructure Manager, VMware vSphere
Encryption	
Storage	Cisco Key Manager, RSA Data Protection Manager
Remote access/VPN	Cisco Security Manager, Cisco AnyConnect VPN
Network Management	
Device configuration	Cisco Prime LMS
Security configuration	Cisco Security Manager
Wireless configuration	Cisco WCS

E-commerce/Internet Edge/Service Provider Edge/Partner Edge

The solution uses a collapsed Internet edge and extranet network to support Internet connectivity and business partner connectivity, as shown in Figure 3-9.

Figure 3-9 E-commerce/Internet Edge/Service Provider Edge



Design Considerations

The primary segmentation of the perimeter of the enterprise occurs at the edge.

The design does the following:

- Provides an enterprise connection to the Internet.
- Secures the Internet edge design using Cisco firewall and intrusion detection systems.
- Provides a dual-threaded design for network resiliency.

- Provides a collapsed Internet edge and extranet network for a highly centralized and integrated edge network.
- Provides remote VPN access to enterprise users/telecommuters.

This design takes into account best practices from the *Data Center Networking: Internet Edge Design Architecture Design Guide* (http://www.cisco.com/go/designzone) and customizes these recommendations for Internet edge and extranet networks. The edges connect Internet services to the complete enterprise environment from hospitals to Internet service providers and clinic office connections that use a Cisco secure VPN to connect to data centers. The collapsed design provides highly centralized and integrated edge networks, and transports the aggregated traffic through various service modules (Cisco ACE, Cisco ASASM, and Cisco IDSM2) within a pair of Cisco Catalyst 6500 switch chassis. The Internet edge provides the following security functions:

- Secure configurations and management.
- IP anti-spoofing.
- Access control lists (ACLs) provide explicitly permitted and/or denied IP traffic that may traverse between inside, outside, and DMZ. Routing and access control lists provide segmentation between authorized and unauthorized access on the network. This applies to the HIPAA requirement for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i); and protecting ePHI from parts of an organization that are not authorized such as Isolating Healthcare Clearinghouse Functions 164.308(a)(4)(i). Segmentation also provides for protection against malicious software 164.308(a)(5)(ii)(B) and can modify the accessibility as described in Access Establishment and Modification 164.308(a)(4)(ii)(C).
- Stateful inspection provides the ability to establish and monitor session states of traffic permitted to flow across the Internet edge, and to deny traffic that fails to match the expected state of existing or allowed sessions. The firewall filtering and routing provide segmentation between authorized and unauthorized access on the network. This applies to the HIPAA requirement for preventing, detecting, and containing security violations as listed in the Security Management Process 164.308(a)(i); and protecting ePHI from parts of an organization that are not authorized such as Isolating Healthcare Clearinghouse functions 164.308(a)(4)(i). Segmentation also provides for protection against malicious software 164.308(a)(5)(ii)(B).
- Intrusion detection using Cisco IDSM2 provides the ability to promiscuously monitor traffic across discrete points within the Internet edge, and to alarm and/or take action after detecting suspect behavior that may threaten the enterprise network. The IPS/IDS identifies and notifies appropriate individuals that suspicious activity is occurring. This applies to the HIPAA requirement for identifying and responding to suspected or known security incidents (164.308(a)(6)(ii)).
- Applications servers that need to be directly accessed from the Internet are placed in a quasi-trusted secure area (DMZ) between the Internet and the internal enterprise network, which allows internal hosts and Internet hosts to communicate with servers in the DMZ.
- All public-facing web applications should be developed using the security best practices to prevent known attacks, and must be reviewed annually or after changes.

The Internet and Partner Edge provides multiple safeguards to help a healthcare organization meet HIPAA safeguards. The firewall filtering and routing provide security between authorized and unauthorized traffic from an unsecured network. This is extremely important when connecting the organization to external networks such as the Internet or a business associate. This helps an organization meet the HIPAA requirement for preventing, detecting. and containing security violations as listed in the Security Management Process 164.308(a)(i).

The firewall also provides encryption capability to encrypt traffic sent over public networks. This helps an organization meet the HIPAA requirement for Transmission Security 164.312(e)(1), Integrity 164.312(e)(2)(i), and Encryption 164.312(e)(2)(ii).

The IPS/IDS identifies and notifies appropriate individuals that suspicious activity is occurring. This helps an organization proactively address security incidents. This applies to the HIPAA requirement for identifying and responding to suspected or known security incidents (164.308(a)(6)(ii)).