

Secure Foundation for Electronic Health Records in Ambulatory Care Environments

Revised: May 27, 2009, OL-19314-01

The 2009 Stimulus Package has provided healthcare providers with a strong incentive to implement Electronic Healthcare Record (EHR) applications. Protected Healthcare Information (PHI)—or patient data—must remain secure and private as the healthcare industry deploys EHRs, as well as supporting infrastructure and tools.

This publication addresses Ambulatory EHR systems in the context of the following:

- The security threats facing ambulatory healthcare organizations deploying EHRs
- The steps that healthcare practitioners must take to secure PHI data that traverses the network
- Deployment scenarios for small, midsize, and large-scale provider based IT infrastructure

Executive Summary

Network-based applications have transformed virtually every industry—healthcare is no exception. Wireless, wired, and mobile solutions that allow access to EHRs, medical management systems, imaging, biomedical information, material management, patient accounting, admitting information, and online claims submissions are becoming increasingly common. Today, healthcare systems can merge these tools into a converged infrastructure to more effectively communicate and collaborate, reduce errors, and improve both the efficiency and quality of patient care. The end result is a lower cost for patient care through the various efficiencies gained.

As healthcare providers adopt EHRs, they also face new security threats. Internal employee violations and breaches, hackers, human error, and computer viruses present real dangers to provider-based healthcare networks.

Fortunately, many security breaches can be prevented, and there are numerous network security tools available that are easy to deploy and use. The Cisco Medical-Grade Network uniquely provides comprehensive protection for information, applications, and services.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2009 Cisco Systems, Inc. All rights reserved.

Building upon the industry-proven capabilities of Cisco Security solutions, the Cisco Medical-Grade Network integrates security services into the provider's IT-based network infrastructure. Each device has integrated security, providing the network with threat mitigation abilities, secure connectivity, and strong policy management. This enables providers to use modern, network-enabled technologies to help ensure uniform compliance with established security policies.

Healthcare Industry References

The solution design described in this publication addresses support for the following standards requirements and industry organizations:

Health Insurance Portability and Accountability Act (HIPAA)

Health Insurance Portability and Accountability Act (HIPAA) is a US law designed to provide privacy standards to protect patient medical records and other health information provided to (and shared by) health insurers, doctors, hospitals and other health care providers. HIPAA was developed by the Department of Health and Human Services (DHHS) to provide a framework to ensure the privacy of patient medical records and to allow greater control by patients with regard to how their personal health information is used and disclosed.

Health Information Trust Alliance (HITrust)



The Health Information Trust Alliance (HITrust) is a healthcare industry organization that aims to build greater trust between patients, physicians, organizations, government and technology companies by ensuring information security is a foundational pillar in the adoption of technology and the exchange of data.

American Hospital Association (AHA)



Cisco's wireless networking products have the exclusive endorsement of the American Hospital Association (AHA).

IronPort's secure messaging services have the exclusive endorsement of the American Hospital Association (AHA).

The American Hospital Association (AHA) represents and serves all types of hospitals, healthcare networks, patients, and communities. AHA members include nearly 5000 hospitals, healthcare systems, networks, and other care providers, as well as 37,000 individuals. AHA Solutions is a subsidiary of AHA with the sole purpose of finding products and services that help hospitals run more efficiently. AHA Solutions is uniquely positioned to understand the needs of the healthcare community and to identify ways to help its stakeholders achieve better patient care.

IronPort is the exclusive secure messaging provider endorsed by the AHA. This endorsement was established to provide a standardized, secure messaging solution compliant with stringent HIPAA regulations for patient and information privacy and security in the healthcare sector.

The Need For Network Security In Deploying EHR

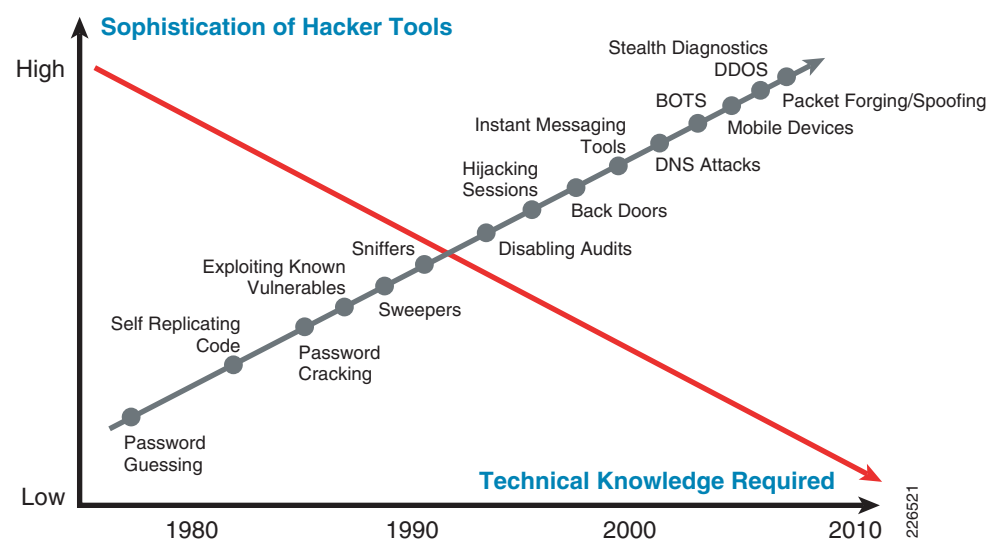
While information security is a top priority for any organization, healthcare providers must be especially diligent in protecting confidential patient data. In addition to the evolving threat posed by hackers and other intruders, government regulations—such as the U.S. Health Insurance Portability and Accountability Act (HIPAA)—establish privacy requirements for PHI. Merely deploying a network firewall is insufficient and does not by itself provide the necessary security measures. Instead, providers must apply a comprehensive approach to protecting patient information at every potential point of access—both inside and outside the network.

Escalating Security Threats

As healthcare organizations increasingly rely on networks to support core operations, they become vulnerable to nontraditional attacks. Compromised networks, applications and operations can disrupt critical business functions, interfere with patient care—even to loss of life, expose providers to substantial liabilities, and damage credibility and reputation of the organization.

Network attacks vary by systems and location in the network. Some attacks are elaborately complex with specific motives in obtaining access to PHI data, while others are simply malicious attacks without a specific purpose. Employee threats must also be considered and are too often overlooked. Though possibly unintentional, these threats can still cause significant damage and disrupt patient care. Intentional attacks by internal employees are the most common disruption. According to a survey by the U.S. Computer Security Institute/Federal Bureau of Investigation, attacks by insiders represented almost 50 percent of all attacks in 2008¹. Some of the security threats facing information networks today are summarized in Figure 1. Over time, the technical sophistication required to launch an attack has required less and technical skill. This is primarily due to hacking kits, which include fully functional utilities and tools, as well as source code used to self-author worms and other viruses.

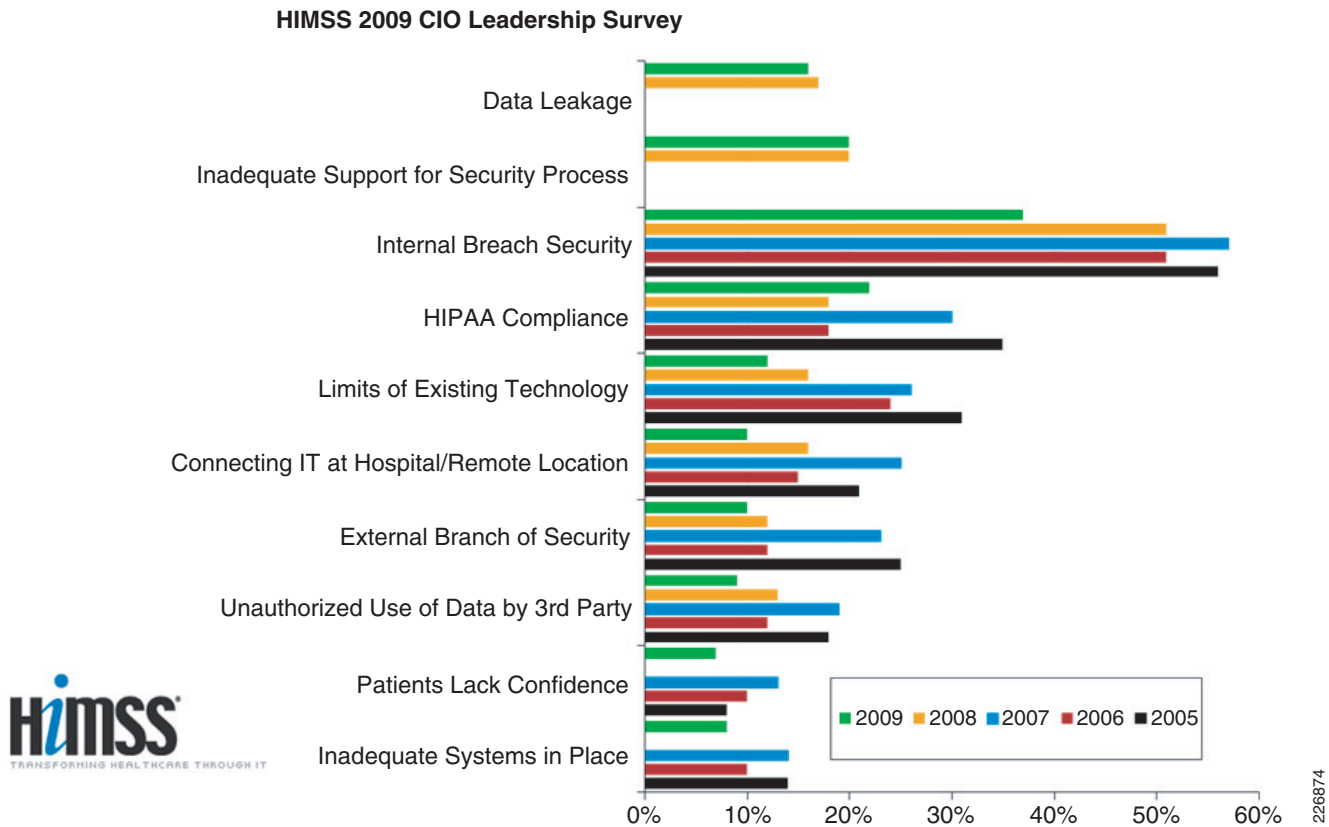
Figure 1 Security Threats



1. This information was derived from the Computer Security Institute publication at the following URL:
<http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2008.pdf>

According to a 2009 Chief Information Officer (CIO) survey published by the Healthcare Information and Management System Society (HIMSS), internal breaches have consistently represented the top security concern of members over the past five years. As shown in Figure 2, internal security breaches decreased in 2009, but this threat is still the primary concern of HIMSS-member CIOs. However, internal security breaches might not always be purely malicious in nature and might simply be the result of a curious internal user looking for information about a popular figure, a friend, or a neighbor.

Figure 2 Top Concern—Security of Computerized Medical Information



Historically, the Internet Protocol (IP) did not contain specific provisions for security in its design. As a result, healthcare providers must make sure that their IP-based network implementations take into account network security practices, services, and products that can mitigate the inherent risks facing today’s integrated healthcare information environment.

The Costs of Poor Security

Network security breaches can result in fines, legal liability, lost productivity for clinical and administrative staff, and the devastating loss of partner and patient confidence. In addition to the cost of repairing the network itself, the impact on a provider can include the following:

- *Disruption of clinical and administrative processes*—Network downtime and loss of critical server and application operations are common immediate effects of poor security. The more that providers rely on networks, EHR, practice management systems, and clinical information systems, the more an unavailable network can interfere with a provider’s ability to treat patients.

- *Loss of patient and partner confidence*—A practice that has been victimized by hackers might find it difficult to earn back trust and loyalty. Patients, insurers, and clinical partners are understandably reluctant to share private information with a practice that cannot protect it. Under HIPAA, business associate agreements prohibit the sharing of PHI to organizations that cannot ensure its confidentiality.
- *Financial costs*—Under regulatory requirements such as HIPAA, providers that fail to protect confidential patient data can face stiff penalties and liability from litigation. To combat these threats, providers need a consistent, scalable, enterprise-wide security solution that continually safeguards their networks.

The Benefits of a Secure Healthcare System

Healthcare providers that employ strong security do more than just protect patient data. They establish new capabilities for improving patient care and business operations. A secure EHR network can enable the following:

- *Access to information at the point of care*—A secure wired or wireless network allows clinicians to access and update clinical records directly from an examination room or lab, providing an up-to-date, comprehensive view of the patient where caregivers need it most. Within an ambulatory environment, having access to patient histories during a patient visit can often offer a higher level of care.
- *Increased mobility*—Secure wireless networks and virtual private networks (VPN) allow clinicians to access patient information, lab results, and medical libraries from notebook computers, PDAs, handheld devices, and portable phones, as well as from remote practices, hospitals and home offices.
- *Enhanced productivity and reduced costs*—Once a secure, reliable network is in place, healthcare providers can deploy applications that streamline resource-intensive back-office processes. Solutions can include business management applications, claims processing systems, and systems for finance and human resources management.
- *Improved patient care and safety*—Digital clinical applications and real-time information sharing enabled by a secure network provide a more unified, up-to-date view of the patient, which results in faster, more accurate, less redundant care. When clinicians can securely update records and digitally write orders and prescriptions at the point of care, they can substantially reduce errors associated with handwritten, paper-based systems.

The Cisco Medical-Grade Network

The Cisco Medical-Grade Network incorporates end-to-end blueprints for designing, implementing, and maintaining highly secure wired and wireless networks. These blueprints take an integrated, defense-in-depth approach to network security design, focusing on expected threats and their mitigation rather than on simple instructions for where to place point product solutions, such as a firewall or an intrusion prevention system (IPS). This strategy results in a layered approach to security, in which the failure of one system is not likely to lead to the compromise of network resources.

The security strategy behind the Cisco Medical-Grade Network is built around the following fundamental concepts of network protection:

- A true security solution is a *process*, not a product. An effective security solution must continually evolve and change to defend against new threats and to accommodate changing business requirements.

- Each element within a network—including applications, desktops, laptops, servers, and network devices (routers, switches, wireless access points, and appliances)—must play a part in protecting the organization from internal and external threats. Security must be integrated into the operations of the network and into the devices on the network.
- A successful security solution requires comprehensive, integrated safeguards throughout the network infrastructure—not just a few specialized security devices. Security solutions should be modular in order to keep costs down and ensure scalability and flexibility.
- A layered, in-depth defense strategy provides more complete protection and minimizes areas of potential vulnerability.
- Security should be integral to the overall architecture from the beginning—not considered later or as a separate “add-on” component.

A Modular Blueprint Based on Best Practices

Each security blueprint uses a modular approach that offers two main advantages. First, it allows network planners to address the security relationship between the functional blocks of the network. Second, it enables planners to evaluate and implement security on a module-by-module basis, instead of attempting to adopt and deploy a complete architecture in a single phase. Cisco has developed blueprints for small, midsize, and large networks that incorporate wired and wireless infrastructures, satellite locations, and remote connectivity.

These blueprints are based on years of experience developing security solutions for healthcare organizations of all sizes around the world. Organizations that use these blueprints can benefit from proven best practices for creating robust security solutions that protect both patients and healthcare organizations.

The Components of a Healthcare Security Solution

Threats to healthcare networks are real, and protecting these networks requires security tools which include:

- *Endpoint security software packages*—These packages counter most virus, spyware, and malware threats—if updated regularly and maintained. The use of endpoint security software on all hosts within the physician’s office is critical to keep a host from being compromised
- *Secure network infrastructure*—Hardware and software features that support secure connectivity, perimeter security, intrusion protection, identity services, VPN, and wireless. Because these devices comprise the infrastructure used to support the EHR system, enabling the corresponding security features native to each product will provide added protection to the overall EHR deployment
- *Security management*—Tools for provisioning, change management, monitoring and maintaining security, that provide centralized intelligence for managing the other components of a strong security solution.

No individual component can fully protect healthcare systems, but when integrated, these coordinated elements are highly effective in keeping a network safe from attacks and other security threats.

Identifying Vulnerabilities

A typical healthcare network can have many potential vulnerabilities, including partner extranets, unsecured VPNs, always-on broadband connections, internal unauthorized employee access, information theft, and wireless LANs (WLAN). Organizations can identify potential vulnerabilities by reviewing aspects of the network architecture. Key questions follow.

Do you have a firewall and do you know how it is protecting the practice and its valuable PHI data?

Even the most robust, feature-rich firewalls are of little use unless they are correctly configured and their appropriate features are enabled. Appropriate resources should be allocated on a routine basis to validate the operational effectiveness of each firewall against the security policy. Most EHR vendors can provide some guidance as to what security policy should be enabled in order to properly and most effectively secure their specific system.

What type of remote access to your network and EHR system do you allow?

Organizations should check VPNs, WLANs, PC-based remote control software, and other external connections to insurers, vendors, and partners to help ensure that only allowed systems are granted access—and that no unknown access points have been added to the network.

Do you have an Internet-accessible website used for scheduling or other patient communication purposes?

If you operate an Internet web server for patient or partner access, keeping the server safe from hackers requires specific attention. At a minimum, every web server's underlying OS should be configured to conform to the OS vendor security checklists. Providers should also develop a process for evaluating and installing security patches promptly in order to help eliminate any web-based application vulnerability.

Do you send and receive E-mail from your office?

Healthcare organizations that send and receive E-mail should ensure that all transmissions are safe and secure—in compliance with HIPAA regulations. There should also be safeguards in place to protect network resources from viruses, worms, and malware transmitted via E-mail. Do you exchange patient information via E-mail?

Designing the Network Architecture

When designing and deploying network architectures, healthcare providers must evaluate each area of the network, determine potential threats, and implement appropriate security measures. This is part of the business risk analysis and response that should be performed under HIPAA regulations. A healthcare provider's specific security implementation will depend on the size of the organization and, for HIPAA requirements, its risk tolerance. At a minimum, any secure network architecture should include protection for the network perimeter, the department/office LAN, teleworker connections, WLANs, and any satellite/remote locations.

All Cisco products include mechanisms to provide security in order to protect patient information. In the design discussions that follow, multiple security technologies are described as separate devices for the sake of discussion, but are actually integrated into a small number of devices that can be easily deployed within a practice.

Cisco Channel Partners, value-added resellers, and managed security service providers can be especially helpful in assisting small and midsize providers to implement cost-effective, systemic security at their locations. Each partner has its own areas of specialization. When considering a partner, be sure to

investigate its manufacturer certifications, which can ensure that the partner is qualified to install and configure network security solutions, and is up to date on the latest issues and technologies. To find a Cisco Certified Security Partner in your area, visit the following URL:

<http://www.cisco.com/go/partnerlocator>

The Network Perimeter

Many small and midsize providers select economical broadband cable or digital subscriber line (DSL) services for Internet access. While these high-speed services can usually support many healthcare applications, they pose a greater risk than private leased-line services. For example, a single Denial of Service (DoS) attack on a provider's web server can consume all the available bandwidth on the segment. Unlike leased-lines, which service a single provider, broadband connections are usually shared with neighbors and the like. As a result, the risk of impacting availability (and security) is much greater when using a shared broadband service.

Firewalls

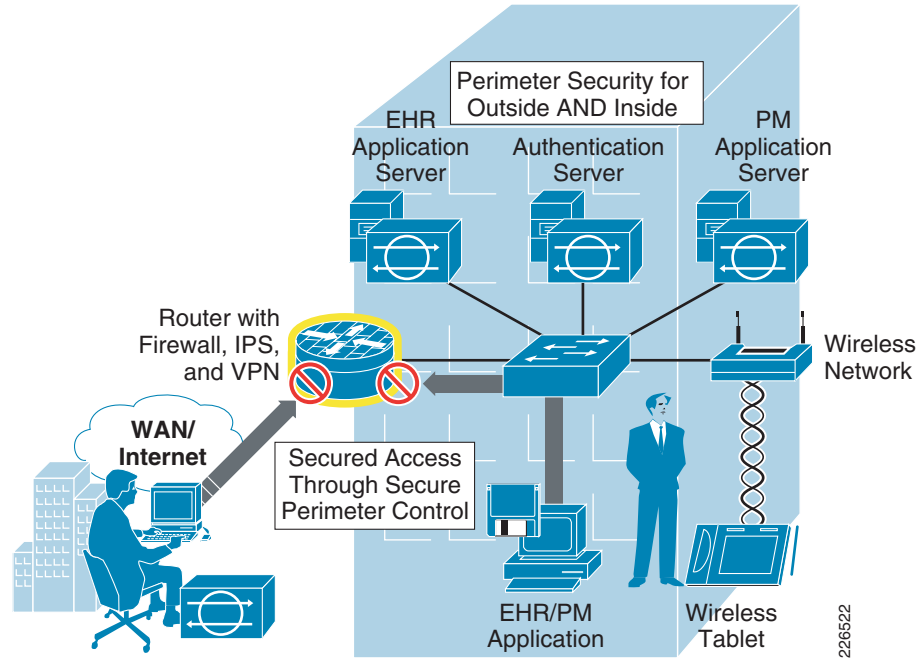
The best way to protect the perimeter is with a business-class firewall and access router with inspection firewall features. An integrated router can provide a manageable, cost-effective solution for smaller provider locations with limited IT budgets and staff. Larger providers, however, might require the increased capabilities of a dedicated firewall.

Whether hardware- or software-based, a firewall encircles a provider's network and acts as a secure buffer between it and an "untrusted" network, such as the Internet. When deployed at the network perimeter, firewalls can help do the following:

- Ensure that only appropriate PHI information and personnel are allowed access to the provider's network and EHR system
- Block unwanted or dangerous transmissions from unauthorized users
- Filter the Internet content that users are allowed to view including secure E-mail

In [Figure 3](#), the router shown has an imbedded firewall that protects against Internet-based attacks and controls access to the EHR from inside the practice.

Figure 3 Firewall Security



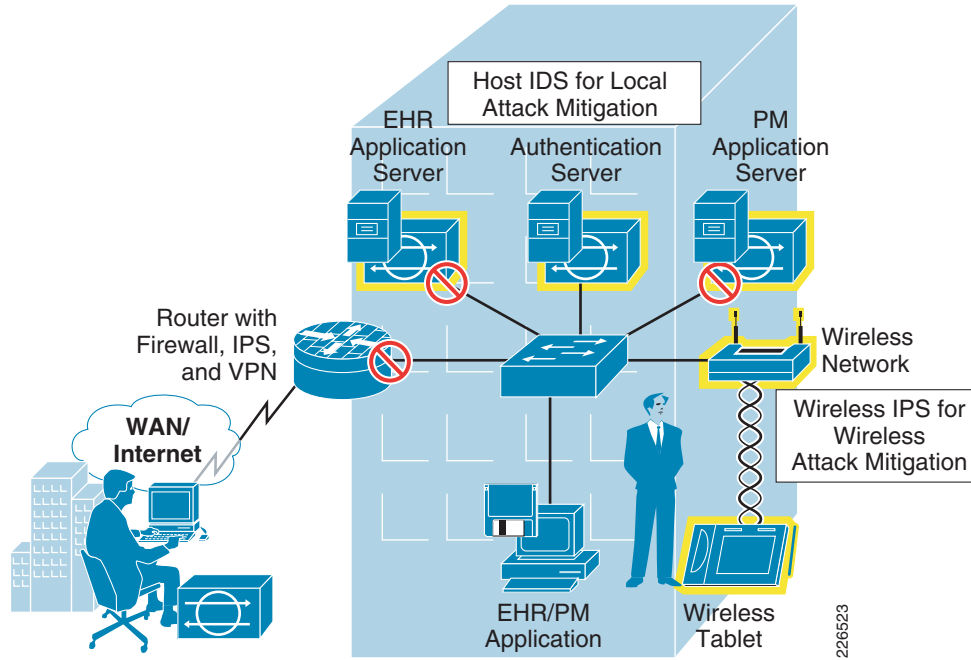
Intrusion Prevention Systems

As shown in [Figure 3](#), the Intrusion Prevention System (IPS) can also protect the network perimeter against hackers and unauthorized users. An IPS can identify attacks that firewalls cannot detect—for example, identifying attacks targeted at the EHR system, and alerting personnel. IPS capabilities can alert administrators, cut off hackers, and even dynamically reconfigure the network to help prevent future attacks. IPS solutions can be network-based systems (appliance-based sensors or a feature set in access router software) or host-based software agents.

Wireless Intrusion Prevention Systems

Wireless intrusion prevention systems (wIPS) monitor the RF environment for a given building. These systems look for wireless-specific attacks, such as rogue wireless infrastructure access points and clients, denial of service (DoS) attacks, and others. Even if there is no active wireless network in place, organizations should strongly consider placing a wIPS system in place to ensure that employees have not placed insecure wireless infrastructure elements on the network that can provide a backdoor into the corporate infrastructure. [Figure 4](#) highlights the placement of wIPS sensors within the network. Again, if desired, the wIPS function can be enabled within the wireless access point—directly reducing the number of standalone devices within the practice.

Figure 4 Wireless Intrusion Prevention



Secure E-mail

E-mail has become the mainstay in business communication today. Within healthcare, the use of E-mail to communicate with a patient—as well as among physician practices—is becoming increasingly common. Outside of the normal patient E-mail communication, there are other sources of E-mail that are even more pervasive. Some examples include correspondence with insurance companies, referring physicians, and the casual office employee E-mail. Since the nature of the information often includes medical information regarding the patient under care, the need for a consistent security policy to safeguard PHI is critical and must comply with HIPAA regulations.

The Cisco IronPort family of products allows the safe and secure transmission of E-mail by providing encryption for all outbound E-mail. It operates transparently and does not require senders to deliberately mark messages for encryption. Policy-based message filtering capabilities determine which messages should be encrypted and message routing policies determine delivery methods for identified messages.

By using a pre-configured HIPAA security policy on the IronPort family of products, E-mail becomes a trusted messaging platform by eliminating the transmission of patient information without the use of encryption. In addition, Ironport will reduce spam and other E-mail related virus activity—thereby helping to eliminate the likelihood of a virus spreading throughout the practice.

Protecting the Network Perimeter—The Cisco Solution

Cisco offers a complete portfolio of integrated, comprehensive security offerings for the network perimeter. The Cisco Unified Communications 500 Series for small business, Cisco 1800 Series Modular Access Router and Cisco 2800 Series Multiservice Platforms deliver fast, reliable network and Internet connectivity.

These Cisco products support the full suite of Cisco router-based security services, including stateful firewall, IPS, and integrated VPN for connecting individual remote users or satellite offices. If the practice desires a dedicated firewall appliance, the Cisco Adaptive Security Appliance (ASA) 5505 supports firewall, IPS, and integrated VPN capabilities.

The Cisco Unified Communication 500, Cisco 1800, and Cisco 2800 Series products offer fast, reliable communication, and add Unified Communications and wireless capabilities. With Cisco Unified Communications capabilities, a physician's office can take advantage of voice over IP (VoIP) which offers lower cost voice service based on the Session Initiation Protocol (SIP). Other features include voicemail, Interactive Voice Response (IVR) and 802.11 wireless. The 802.11 wireless can be used for voice services based on any of the Cisco VoIP wireless handsets, as well as data services allowing access to the EHR system in the exam room.

Cisco Unified Communication coupled with an EHR systems available on the market today can enhance the office workflow by providing automated patient reminder outcalls, EHR screen pop-ups for all inbound patient calls, and remote access to the EHR system using encrypted an secure VPN technology.

These Cisco products feature easy-to-use, web-based configuration tools designed to meet the needs of smaller organizations. Even a practice with limited IT resources can deploy and manage perimeter security, voice communication, and remote access with confidence.

Wireless LANs (WLAN)

Perhaps no industry has benefited more from wireless networking than healthcare. Clinicians can now use wireless-enabled handheld devices to access clinical information systems, medical records, imaging systems, and other resources—right from the patient's bedside. WLANs also present unique security considerations.

Since overall network security is only as strong as its weakest link, providers need to be as certain as possible that WLANs are providing the same level of access control and privacy as wired LANs. In contrast to a wired LAN, in which a physical connection controls access to the network, WLANs broadcast data through the air. Any wireless-enabled device in the area—such as a patient's laptop in a waiting room or a wireless PDA in a neighboring office—presents a potential security threat.

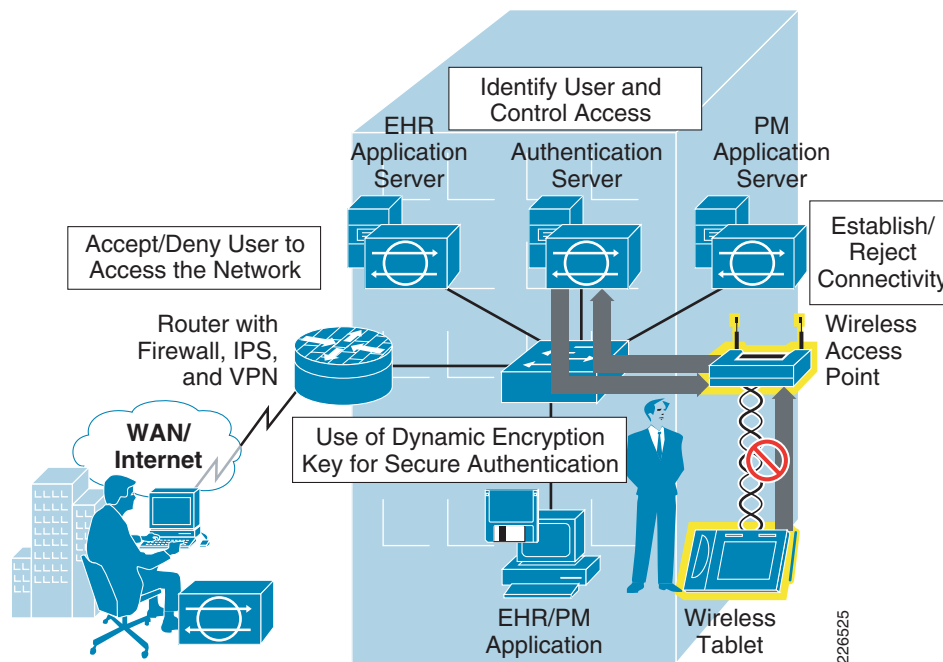
WLAN—The Cisco Solution

Cisco Aironet 1100 and 1200 Series Access Points deliver highly secure, high-performance wireless connectivity using the IEEE 802.11a, IEEE 802.11b/g, and 802.11n standards. Cisco Aironet products and the Cisco Unified Wireless Network provide robust WLAN security that closely match the security available in a wired LAN. Cisco also offers the Cisco Secure Services Client (CSSC), which provides a single supplicant for VPN, wired, and wireless access.

Beyond base encryption and authentication support, Cisco offers an extensive wireless intrusion prevention system called the Cisco Adaptive Wireless Intrusion Prevention System (wIPS). Cisco Adaptive wIPS provides wireless-specific network threat detection and mitigation against malicious attacks, security vulnerabilities, and sources of performance disruption. Cisco Adaptive wIPS provides the ability to visualize, analyze, and identify wireless threats, and to centrally manage mitigation and resolution of security and performance issues. Cisco Adaptive wIPS uses the entire WLAN infrastructure to provide security including Aironet access points to monitor for radio frequency (RF) threats, the Cisco Mobility Services Engine for centralized analysis and recording of event forensics, and the Cisco Wireless Control System which serves as a central management console for WLAN operations and security management. Cisco Adaptive wIPS can also collaborate with technologies from the wired

network security portfolio to create a layered approach to wireless security. Figure 5 shows the wireless security features available throughout the practice, providing secure access to the EHR within the exam room.

Figure 5 WLAN Security Environment



Voice over IP (VoIP)

The WLAN is often considered a *data-only* service. Using any Cisco 802.11 WLAN product enables the physicians practice to leverage the investment through the use of 802.11-based wireless phones. The Cisco Unified IP Phone 7921G and 7925G wireless handsets utilize all of the robust authentication and encryption features available, thereby providing an extremely secure and robust communications environment.

Many physician practices use consumer grade wireless phones which do not offer the privacy needed for secure voice communication. By leveraging the Cisco Unified Communication 500 Series product, Cisco’s enterprise-ready wireless phones can be deployed providing robust encryption for each voice conversation. In addition, the full set of features are extended to the Cisco wireless phone, including voice mail, conference calling, call-hold, and more.

Through the integration with an EHR system, access to schedules, patient records, patient contact information, and text-based messaging are all available to staff members no matter where they are within the office. The result is improved office efficiency coupled with higher patient and staff satisfaction.

Teleworking and Remote Access

Many providers have adopted remote connectivity solutions that give clinicians remote access to necessary clinical and scheduling applications. Using VPNs, clinicians can now use highly secure connections to access patient and clinical information from any remote location, including satellite facilities—and even from home. As remote connectivity becomes a standard healthcare tool, practices must provide remote connectivity solutions that are as secure and reliable as the wired and wireless

office network solutions. Any remote access solution must account for the sensitivity of the information as well as the access method. Access may be denied based on any number of parameters in order to enforce security policies and maintain patient confidentiality.

Today, VPNs are the most popular and versatile remote-access solution. VPNs enable users to securely connect to provider resources over a public network, using any access method. Providers can use extranet VPNs to connect to suppliers and partners, providing limited access to specific portions of the network for collaboration and coordination.

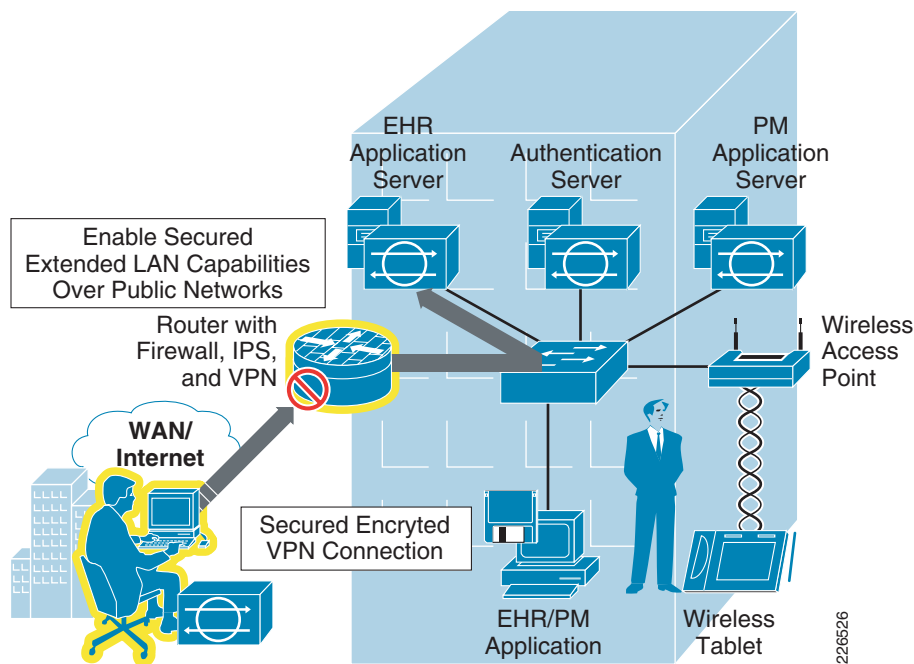
VPN Hardware and Software Client

Remote clinicians can use software or hardware VPN clients to connect with the provider. They can take advantage of Secure Sockets Layer (SSL) VPNs or “clientless” VPNs that require only a web browser. For clinicians who will use the solution while traveling or working from a remote location, the software client or SSL VPN makes the most sense. However, when using a software client, information on the clinician’s PC is protected only while connected to the VPN tunnel. Information on the laptop is not inherently protected while a clinician is surfing the Internet if he or she is not connected to the VPN tunnel.

The Cisco Secure Desktop feature provides the ability to prevent PHI data from being stored on a computer. The Cisco Secure Desktop automatically creates a protected environment that is automatically destroyed when the VPN user terminates the VPN session. This prevents data from being cached or stored locally on the computer, thereby meeting HIPAA-mandated regulatory and information security (InfoSec) policies.

For a clinician’s home office, a hardware client, such as a firewall appliance or a broadband router with firewall features, provides a more-secure, always-on solution. In a small satellite location with more than one user, the office router or firewall can also act as a VPN client, providing highly secure remote access for all users behind it and eliminating the need for each user to launch a VPN software client. In addition to day-zero threat protection, CSA has firewall capabilities and complements any type of remote-access VPN. [Figure 6](#) illustrates an example VPN environment.

Figure 6 IP VPN Security



VPN—The Cisco Solution

Cisco offers VPN connectivity solutions for providers of all sizes. Cisco 880, Cisco 1800, and Cisco 2800 Series modular access routers and Cisco Unified Communication 500 Series products all provide native VPN support—enabling smaller locations to terminate and manage remote VPN sessions without having to deploy a separate appliances. Larger locations that require support for more than 50 simultaneous VPN tunnels can deploy a more scalable Cisco ASA 5500 Series Adaptive Security Appliance behind the router or firewall.

For remote small and home offices, Cisco 880 Series routers and Cisco ASA 5505 hardware clients provide a highly secure, high-performance teleworker solution. Traveling clinicians can use Cisco VPN Client software, a highly secure, intelligent software client included with all Cisco VPN solutions, or the SSL VPN currently available with the Cisco ASA 5500 Series Adaptive Security Appliance.

Remote Office Locations

A healthcare provider’s remote office locations may function as independent, autonomous networks with their own local servers and user workstations or may rely on central processing resources. The remote office should include the same components, design principles, and considerations as security solutions discussed in the preceding sections.

The Cisco 880, Cisco 1800 Series modular access router, Cisco 2800 Series multiservice platform, Cisco Unified Communications (UC) 500 Series, and the Cisco ASA 5505 offer built-in support for site-to-site IP Security (IPSec) VPN WAN connectivity. These solutions combine enterprise-class network and Internet access to local users, advanced firewall protection, and highly secure, cost-effective WAN connectivity in a single, highly manageable form. While not modular, the Cisco UC 500 Smart Business Communications System provides voice, data, voicemail, Automated Attendant, video, security, and wireless capabilities—while integrating with existing desktop applications such as calendar, E-mail, and customer relationship management (CRM) programs.

Secure WLAN services can be delivered into remote office locations using the Cisco Hybrid Remote Edge Access Point (H-REAP) architecture. In this architecture, access points are centrally managed at a core facility. Authentication is handled by a central Authentication, Authorization, and Accounting (AAA) server. In the event a WAN link is lost, Cisco Aironet access points can provide limited authentication for known clients.

Managing a Secure Network

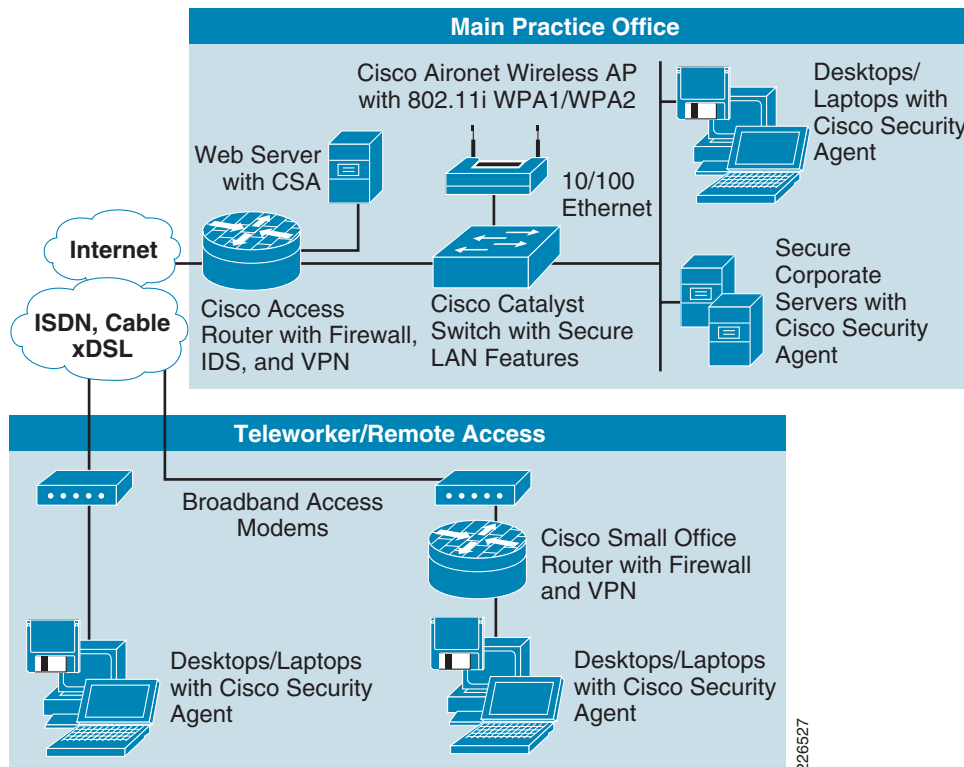
Strong healthcare security requires more than just the right network design, hardware, and software. System administrators must also be able to effectively monitor and manage the network with its integrated security system. Implementing the right management tools will allow administrators to view and control activity on the network at any time and to access all network devices through a single interface.

Small Office Blueprint

This deployment blueprint supports a location with approximately 10 total employees. The Cisco 880 or Cisco 1800 Series modular access routers, or the Cisco UC 500 Series, can provide all of the connectivity services required for the location. Either option will support 802.11 b/g/a wireless, firewall, IDS, and VPN services in a single, manageable device. Both systems provide voice services coupled with Power over Ethernet (PoE) to power a number of endpoint devices—such as VoIP phones, security cameras, and access points. For areas that require additional wireless coverage, the Cisco Series 1100 or Cisco 1200 Series access points can be configured to support the 802.11a/b/g and 802.11n wireless connectivity and can provide enterprise-ready authentication and encryption mechanisms.

Teleworkers connect with the networked locations using VPNs managed with the practice's Cisco 1800 or UC 500 Series system. Remote users can use Cisco VPN client software, Cisco 1800 Series router with firewall features, or a Cisco Adaptive Security Appliance (Cisco ASA 5505 firewall) from a home office. [Figure 7](#) illustrates an example environment for about 10 employees.

Figure 7 *Small Location Deployment Blueprint for About 10 Employees*



Midsize Office Blueprint

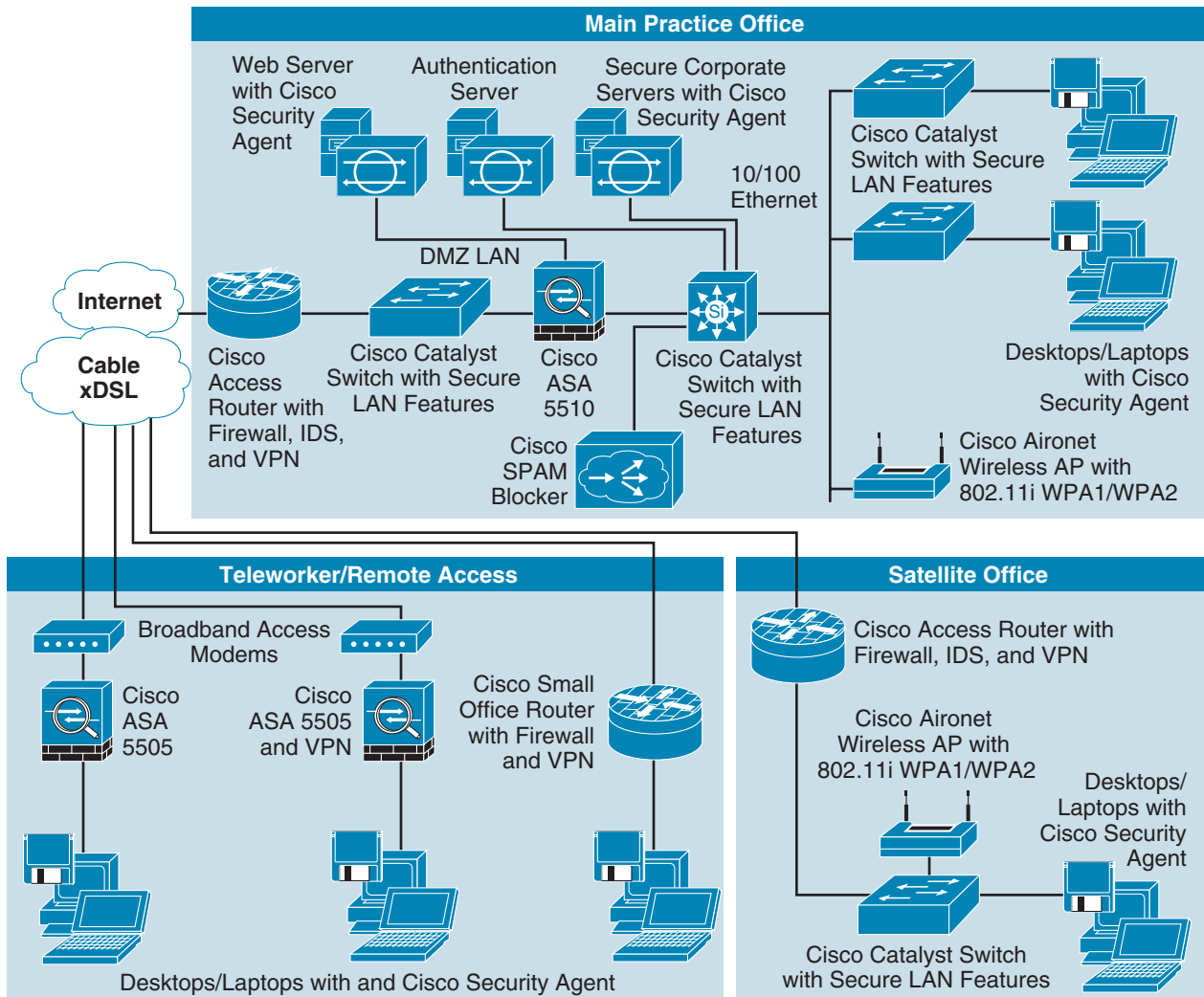
The midsize office deployment blueprint supports a practice of approximately 20 employees. In this blueprint, a Cisco 1800 or Cisco 2800 Series modular access router, or a Cisco UC 500 Series system provides connectivity, firewall, IDS, and VPN services at the network perimeter. Either the Cisco 1800 or 2800 Series modular access router, or the Cisco UC 500 can provide both voice and wireless services. A Cisco ASA 5505 or Cisco ASA 5510 Series security appliance can be deployed to provide additional protection for internal network resources. Through the use of the Cisco ASA Phone Proxy, remote users can utilize a Cisco VoIP phone and can be provided services from the main practice. A Cisco Catalyst 2960 Series switch is deployed between the router and the firewall to support web servers or other servers accessible to external parties. A Cisco Catalyst 3750 Series switch links the servers with the 10/100/1000 Ethernet LAN and Cisco Catalyst 2960 Series switches with PoE to connect local users and powered devices.

Midsize locations might use Cisco Aironet 1100 or 1200 Series access points for local wireless access. Cisco access points can be deployed if the location needs to support both the 802.11a/b/g and 802.11n standards in a single access point. Locations of this size may still use any number of enterprise-ready authentication and encryption models within the access points to control access to the wireless network.

Teleworkers based out of a midsize location can use Cisco VPN client software or clientless SSL-based VPN. A Cisco router with firewall features, or a dedicated VPN hardware client (such as a Cisco ASA 5505 or Cisco 880 Series access router hardware client) can, as an alternative, be used. This approach works well when sharing printers between offices.

In this deployment, the main office also connects with a satellite office. The satellite deployment is identical to the architecture used for a small office. WAN connectivity is delivered through an IPSec VPN tunnel between the main office and the satellite clinic, and is managed with the IPSec VPN features of Cisco routers. Figure 8 illustrates an example environment for about 20 employees.

Figure 8 *Midsize Location Deployment Blueprint for About 20 Employees*



226528

Large Office Blueprint

The large office deployment blueprints illustrates a location with more than 20 total users.

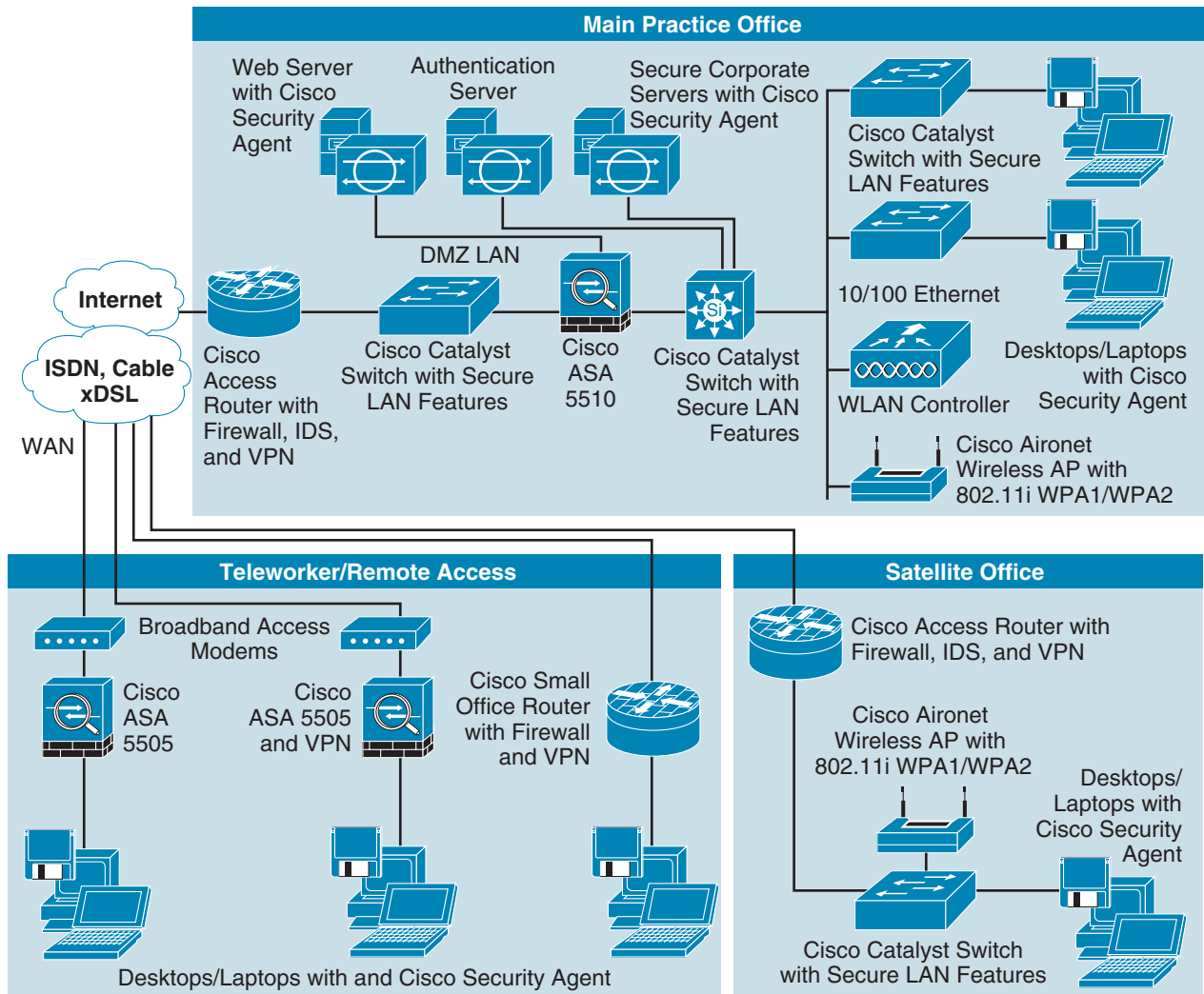
In this blueprint, the main office location uses a Cisco 2800 or Cisco 3800 Series multiservice platform to deliver enterprise-class connectivity, firewall, voice services, IDS, VPN, and wireless services—as well as video surveillance. A Cisco Catalyst 3750 or Cisco Catalyst 3560 Series switch is at the core of the network—delivering high levels of performance and network traffic control. If additional wireless access is required due to the shape or size of the main practice, Cisco access points can be used to deliver wireless services to the entire practice. However, in this deployment model, the access points no longer

manage wireless user authentication locally. Instead, a Cisco Secure Access Control Server (ACS) provides a more scalable solution for managing all wired and wireless authentication services across the network.

The remote office clinic and teleworker configurations are identical to those used by midsize locations—with one exception. Instead of terminating remote-access VPN tunnels at a Cisco router, a Cisco ASA 5510 series Adaptive Security Appliance provides a more scalable, manageable solution for supporting up to 250 simultaneous VPN connections which can be used to secure access to payers and ancillary lab services. WLAN services can be handled by either a WLAN controller located in the satellite office or via H-REAP—depending on the number of users in the remote office.

Figure 9 illustrates an example large location deployment example.

Figure 9 Large Location Deployment Blueprint for More than 20 Employees



226529

Conclusion

The Cisco Protected Healthcare Solution for Providers offers a comprehensive, modular approach to security—one that can evolve as a provider’s needs change.

While security measures must be comprehensive, they need not be difficult to deploy and manage. Cisco offers numerous security solutions designed specifically for small and midsize locations with limited IT staff and expertise. With so much at stake, health-care organizations cannot risk compromising the trust of patients and partners. Cisco offers hands-on experience and intimate knowledge of best practices gained from working with healthcare organizations around the world. Cisco can help providers deploy highly secure network services with confidence.

When deploying EHR applications and tools, providers should take a systematic, multi-tiered approach to planning and deploying a highly secure network infrastructure. This approach should include a careful evaluation of each area of the network, identification of potential threats, development of a practice security policy, and implementation of network security technologies.

Solution Product Listing

Table 1 provides a summary of Cisco products featured in this solution, organized by implementation environment.

Table 1 Summary of Implementation Environments and Corresponding Cisco Equipment

Implementation Environment	Applicable Cisco Systems Equipment
Teleworker/ Satellite Office (about 3 Employees)	Cisco 880, Cisco 1800 Integrated Services Router (ISR), Cisco ASA 5505
Small Clinic (about 10 employees)	<p>Cisco 1800 ISR or Cisco 2800 ISR</p> <ul style="list-style-type: none"> • AIM IPS/IDS Module • WLAN • Voice services (Cisco 1800 only) • VPN access <p>Cisco Unified Communications 500 Series</p> <ul style="list-style-type: none"> • Voicemail • WLAN • VoIP-enabled phones • EHR integration using appropriate third-party middleware • VPN access <p>Cisco Catalyst 2960 Series 10/100 switch</p> <p>Cisco Security Agent (with antivirus)</p>

Table 1 Summary of Implementation Environments and Corresponding Cisco Equipment (continued)

Implementation Environment	Applicable Cisco Systems Equipment
<p>Midsize Clinic (about 20 employees)</p>	<p>Cisco 1800 ISR</p> <ul style="list-style-type: none"> • AIM IPS/IDS Module • AIM VPN Module • Voice services • VPN access • Voicemail <p>Cisco Unified Communications 500 Series</p> <ul style="list-style-type: none"> • Voicemail • VoIP-enabled phones • EHR integration using appropriate third-party middleware • VPN access <p>Cisco Security Agent with antivirus</p> <p>Cisco ASA 5505, Cisco ASA 5510</p> <p>Cisco Catalyst 3560, Cisco Catalyst 3750 Series Switches</p> <p>Cisco 1100 and 1200 Series access points</p>
<p>Large Clinic (more than 20 Employees)</p>	<p>Cisco 2800 and Cisco 3800 ISRs</p> <p>Cisco ASA 5510 Adaptive Security Appliance</p> <p>Cisco 2100 series WLAN Controller</p> <p>Cisco 1100 and 1200 Series access points</p> <p>Cisco Wireless Control System</p> <p>Cisco Security Agent v. 5.0 with antivirus</p> <p>IronPort C150</p> <p>Cisco Catalyst 3560, Cisco Catalyst 3750 Series switches</p> <p>Cisco Unified Communications 500 Series</p> <ul style="list-style-type: none"> • Voicemail • VoIP-enabled phones • EHR integration using appropriate third-party middleware • VPN access <p>Cisco 4400 Series WLAN Controller (should be sourced for 802.11n connectivity)</p> <p>For Cisco Adaptive wIPS, add Cisco 3310 Mobility Services Engine.</p>

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

