



Cisco Healthcare Security Perspectives:  
Protect Your Patients, Your Practice, Yourself  
Technical Implementation Guide

# Cisco Healthcare Security Perspectives: Protect Your Patients, Your Practice, Yourself

Contents

[Abstract](#)

[Executive Summary](#)

[The Need For Network Security In Healthcare](#)

[Considerations For Implementation](#)

[Designing The Network Architecture](#)

[Deployment Blueprints For Providers](#)

[Conclusion](#)

# Cisco Healthcare Security Perspectives: Protect Your Patients, Your Practice, Yourself

## Abstract

As the healthcare industry adopts network applications and tools, patient data must remain secure and private. This technical implementation guide describes:

- The security threats facing healthcare organizations
- The steps that healthcare practitioners must take to protect the network
- Deployment scenarios for small, midsize, and large-scale networks

Note: This paper is focused on small, midsize, and large remote locations and does not cover the main provider location. To do so would require larger scale architecture than is discussed here. The same concepts will apply and can be applied to a main site location. A different product solution set that is better positioned to handle the increased traffic and service load would be applied.

## Executive Summary

Network-based applications have transformed virtually every industry, and healthcare is no exception. Solutions that allow access to electronic medical records (EMRs), medical management systems, imaging, biomedical information, material management, patient accounting, admitting information, and online claims submissions are becoming commonplace in wireless, wired, and mobile scenarios. Today, healthcare systems can merge these tools into one infrastructure to more effectively communicate and collaborate, reduce errors, and improve patient care and efficiency. This results in lower cost for patient care.

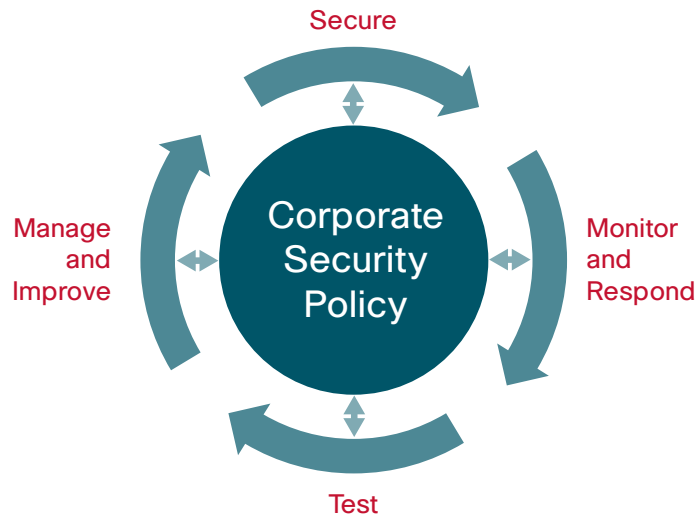
As healthcare providers adopt new technologies, they also face new security threats. Hackers, computer viruses, disaffected employees, and human error present real dangers to healthcare networks.

Fortunately, most 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 is unique in its capability to provide complete defense for information, applications, and services.

Security must be considered a process, not a product-based point solution. The first step an organization should take to establish a secure network infrastructure is to develop a formal security policy to define the roles, responsibilities, acceptable use, and security practices. After developing the policy, the organization should then monitor and assess, using established best practices as a benchmark. Providers should closely examine and test their network infrastructures to identify potential vulnerabilities, including physical security, to establish a vulnerability/risk matrix.

As the implementation continues, providers must continually evaluate each area of the network, determine potential threats, and implement appropriate security measures to mitigate them. If the provider does not have a technical security expert, Cisco and its qualified partners can assist in developing an appropriate architecture that will meet the established security policies of the healthcare organization.

**Figure 1.** The Security Wheel: A Continual, Multistage Process Focused on Incremental Improvement



Building upon the capabilities of the Cisco Self-Defending Network, the Cisco Medical-Grade Network provides security services that are integrated into a hospital's network architecture. These services are self-defending, with each device having integrated security, and offer threat control and containment, confidential communications, operational controls, and policy management. This enables healthcare providers to use modern, network-enabled technologies to help ensure uniform compliance with established security polices.

### The Need For Network Security In Healthcare

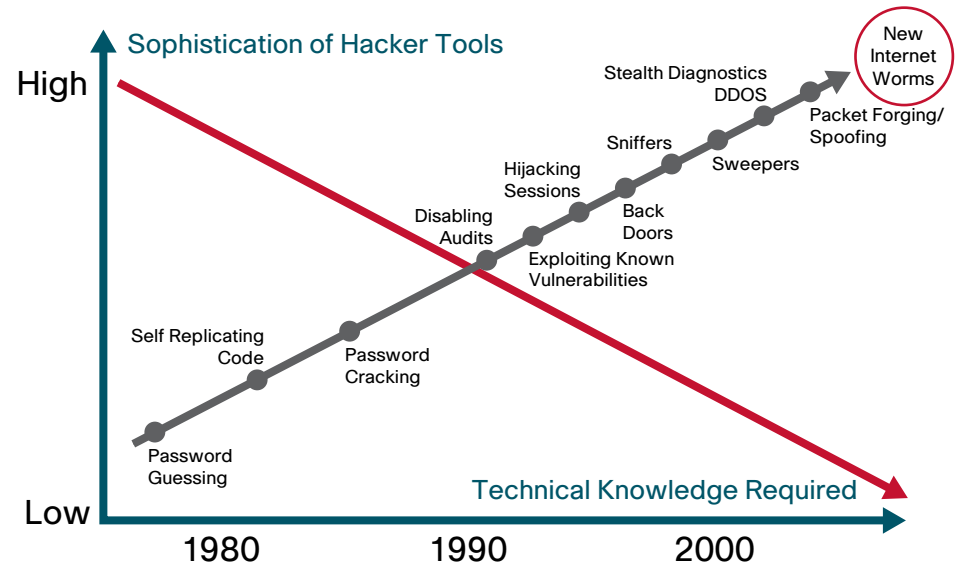
While information security is a top priority for any organization, healthcare providers must be especially diligent in protecting confidential patient data. In addition to the evolving threat posed by hackers and other intruders, government regulations such as the U.S. Health Insurance Portability and Accountability Act (HIPAA), establish privacy requirements for protected health information (PHI). Merely deploying a network firewall is insufficient. Instead, providers need to take 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 for their core operations, they become vulnerable to, nontraditional attacks. Compromised security can disrupt critical functions, interfere with a clinician's ability to treat patients, expose providers to substantial liabilities, and risk the loss of lives and reputations.

Network attacks vary by systems and location in the network. Some attacks are elaborately complex with specific motives, while others are malicious. Employee threats must also be considered. 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 2003 survey by the U.S. Computer Security Institute/ Federal Bureau of Investigation, and are ten times as costly as an external attack.

Figure 2. Security Threats



In the beginning, Internet protocol did not contain specific provisions for security in its design. As a result, healthcare providers need to make sure that their IP implementations take into account the network security practices, services, and products that can mitigate the inherent risks associated with today's integrated healthcare. Common network threats include:

- **Packet sniffers:** Hackers can abuse this legitimate management tool to capture data that is transmitted over a network, such as usernames and passwords.
- **IP spoofing:** This occurs when a hacker inside or outside a network impersonates a trusted computer to gain access to network information.
- **Defacing:** For healthcare practices with a Web presence, defacing (the changing of files on a Web server) can damage patient and partner confidence in an organization's ability to protect sensitive data.
- **Denial of service (DoS):** Perhaps the most widely publicized form of attack, a DoS can be initiated using programs that are available on the Internet. It focuses on making a service unavailable for normal use, often by exhausting a resource on the network, operating system, or application.
- **Spam:** Another growing threat to network operations is spam (unsolicited mass e-mail), which slows mail servers, overruns storage space, and reduces user productivity by clogging mailboxes.
- **Man-in-the-middle attack:** Hackers who have access to packets that move across a wired or wireless network can initiate a man-in-the-middle attack. During this attack, hackers hijack a network session to gain access to private network resources, steal information, or analyze traffic to learn about a network and its users.
- **Viruses, Trojan horses, and worms:** End-user PCs and workstations are especially vulnerable to viruses and Trojan horse attacks. A virus is malicious software code that is attached to another program to execute an unwanted function on a user's PC. Trojan horse attacks are similar to viruses, but they disguise the application to look like something else. Worms are malicious replicating programs.

- **HTTP exploits:** HTTP attacks use a Web server application to perform malicious activities by exploiting the relatively insecure access to an organization's Web servers. If attackers can take control of a Web server, they can access resources that would otherwise be unavailable.
- **Application layer attacks:** Hackers can initiate application layer attacks using several different methods. One of the most common is to exploit well-known software weaknesses commonly found on servers—such as send-mail, HTTP, and FTP—to gain high-level administrative access to a computer.

### 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:

- **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, EMR, 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 may 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 like 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 Maintaining a Secure Healthcare Environment

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 healthcare network can enable:

- **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 a more up-to-date, comprehensive view of the patient where caregivers need it most.
- **Increased mobility:** Secure wireless networks and VPNs 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 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 detection system (IDS). 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 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.
- All aspects of the network, including applications, desktops, laptops, and 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. This integrated approach is the foundation of a self-defending 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 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 the 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.

### Considerations For Implementation

Security challenges are continually evolving, and deploying technology alone is not enough to combat them. Healthcare organizations must develop end-to-end strategies for combating security threats, including robust technologies, a comprehensive security policy, and in-depth evaluation of potential vulnerabilities. A sample analysis such as that shown below can be applied to determine where resources should be applied to mitigate the threat in any network location.

#### Threats (Targets)

- Type A: Targets Critical Infrastructures
- Type B: Targets Near-Critical Infrastructures
- Type C: Insignificant Targets, Minimal Impact

#### Vulnerabilities (Damage Potential)

- Type 1: Catastrophic Loss of Life and Money
- Type 2: Significant Loss
- Type 3: Everything Else

#### *Risk = Threat x Vulnerability*

Effective Security If and Only If:

$$\frac{\text{Prevention}}{T} + \frac{(\text{Detection} + \text{Response})}{t} > \text{Acceptable Risk}$$

T = Development/Deployment Time ~ Days, Months, Years

t = Reaction Time ~ Seconds, Minutes, Hours

Figure 3. Risk Matrix

		Vulnerability		
		1	2	3
Threat	A	More than 1000 lives and/or more than \$1B	More than 100 lives and/or more than \$500M	More than 10 lives and/or more than \$250M
	B	More than 10 lives and/or more than \$250M	More than 1 life and/or more than \$250M	Zero lives lost, more than \$100M
	C	Zero lives lost, more than \$10M	Zero lives lost, more than \$1M	Zero lives lost, less than \$10M

### The Components of a Healthcare Security Solution

While the threats to healthcare networks are real, protecting against those threats can be relatively easy and straightforward—even for smaller organizations without a large IT staff. Network security tools include:

- **Antivirus software packages:** These packages counter most virus threats, if updated regularly and maintained correctly.
- **Secure network infrastructure:** Switches and routers have hardware and software features that support secure connectivity, perimeter security, intrusion protection, identity services, and security management.
- **Dedicated network security devices and software:** Tools such as firewalls are essential for protecting internal systems from external threats over the Internet. IDS solutions monitor the network to detect and neutralize security breaches. Endpoint security software offers day-zero threat protection for network services and applications.
- **Identity services:** Authentication, authorization, and accounting services help to identify users and control their activities and transactions on the network. Services include passwords, digital certificates, and digital authentication keys.
- **Encryption:** Encryption helps ensure that data cannot be intercepted, tampered with, or read by anyone other than the authorized recipient.
- **Wireless security:** Advanced authentication and encryption tools allow physicians to access patient records with a wireless tablet or PDA without the risk of unauthorized users intercepting wireless transmissions.
- **VPNs:** Virtual private networks provide a highly secure, encrypted connection over a service provider network or the Internet. They enable physicians to securely connect to the network from virtually anywhere—a remote hospital or clinic, a conference site, or even from home.
- **Security management:** Includes the tools for monitoring and maintaining security. It is the control element for the other building blocks of a strong security solution.

None of these components on its own can fully protect healthcare systems, but when integrated, they are highly effective in keeping a network safe from attacks and other security threats.

### Creating a Security Policy

The first step in helping to ensure a secure environment is to develop a sound security policy that addresses all the requirements to protect people, processes, data, and technology. A security policy is a formal, publishable document that defines roles, responsibilities, acceptable use, and security practices for the organization. It is an essential component of a complete security framework, and it should be used to guide investment in security defenses.

### The Elements of a Security Policy

Since a security policy affects all aspects of a healthcare ecosystem, it should be created through a collaborative process that includes representatives of clinical, administrative, legal, and technology staff. A cross-functional team will help ensure that all interests of the provider are met while delivering a secure system. Developing a policy can take weeks, depending on the size of the organization.

The elements of a security policy include:

- **Policy statement:** A concise statement of the document's purpose, a policy statement should be specific to the individual organization or department and be auditable, controllable, and enforceable.
- **Scope:** The policy should include the type of information and resources covered by the policy (for example, whether it applies only to electronic resources or incorporates paper-based physical security or other forms of intellectual property).
- **Roles and responsibilities:** Policies must define the roles and duties of those managing security and information systems, as well as the responsibilities of clinical and administrative staff.
- **Security directives:** The policy should offer detailed security directives that must be followed. Directives should cover the types of hardware and software that employees can use, any third parties that will have access to the network, remote access, name and password management, IDSs, and other requirements.
- **Acceptable use policy (AUP):** The AUP addresses issues such as personal use of the Internet and prohibitions against accessing Internet sites that offer inappropriate content.
- **Incident response procedures:** Among the most important aspects of a security policy, incident response procedures define how notification will occur for various threats and the specific actions that are required for response.
- **Document control factors:** Organizations should define how updates to the security policy will occur and how often they should be reviewed and validated.

Providers may want to begin with a simplified, high-level security policy and refine it over time. Sample policies can be found at: [www.sans.org](http://www.sans.org). Cisco recommends that organizations postpone making any major security purchase decisions until a policy is in place. Administrative and clinical processes will likely change over time. Practices should create guidelines for continuous review of the security policy to incorporate new threats and organizational changes.

### Identifying Vulnerabilities

A typical healthcare network can have many potential vulnerabilities, including partner extranets, VPNs, "always-on" broadband connections, and WLANs. Organizations can identify potential vulnerabilities by reviewing aspects of the network architecture.

- **Do you have a firewall, and do you know what it is doing?**

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.

- **What types of remote access do you allow?**

Organizations should check VPNs, modem dialup lines, 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 a Web site?**

If you operate a 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 to evaluate and install security patches promptly. Endpoint security software (Cisco Security Agent, for example) can also offer prompt protection for Web and other application servers.

- **Do you have a comprehensive IDS solution?**

IDS solutions detect attempts to degrade or gain unauthorized access to a network. These solutions use a set of predetermined rules to manage intrusions automatically or to alert security and IT staff to manually address events.

## 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.

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:

[http://tools.cisco.com/WWChannels/LOCATR/jsp/partner\\_locator.jsp](http://tools.cisco.com/WWChannels/LOCATR/jsp/partner_locator.jsp)

## The Network Perimeter

Many small and midsize providers select economical broadband cable or DSL services for Internet access. While these high-speed services can usually support many health-care applications, they can pose a greater risk than leased-line services. For example, a single DoS attack on a provider's Web server can take up all the available bandwidth. Unlike leased lines, which service a single user, broadband connections are usually shared, creating the potential risk of users seeing each other's data.

## Firewalls

The best way to protect the perimeter is with a business-class firewall or an 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, may 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 to ensure that only appropriate information and personnel are allowed access to the provider's network and IT environment
- Block unwanted or dangerous transmissions from unauthorized users
- Filter the Internet content that users are allowed to view

Although a firewall is critical for any business connected to the Internet, implementing and maintaining one often tax the limited IT resources of many small and midsize providers. As a result, many of these organizations choose to outsource firewall implementation and management. Whether an organization implements a firewall itself or works with a partner, it should ask the following questions:

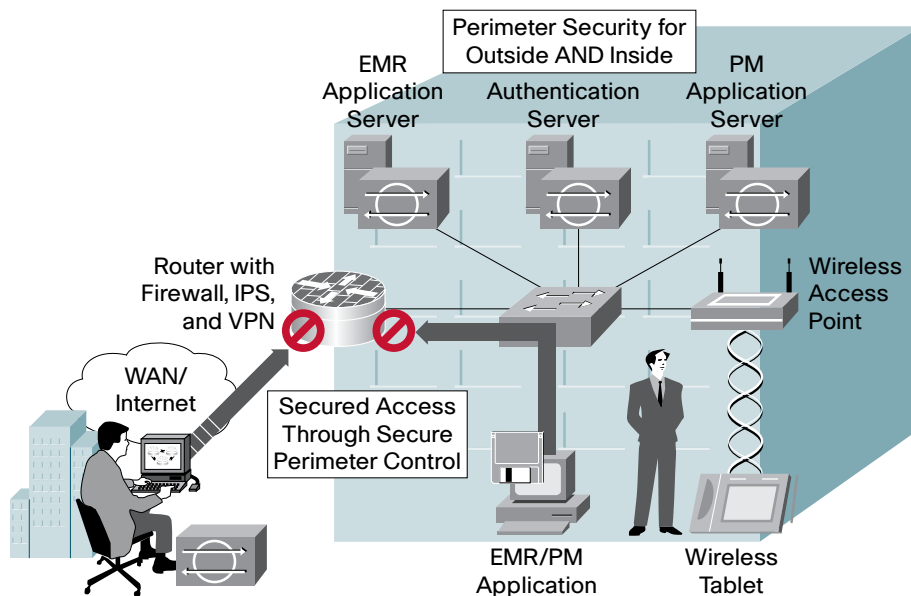
- **Does the firewall support our network security policy, or does it impose the vendor's policy?**

The most secure approach is to preset the firewall to deny all services except those expressly permitted. During installation, site personnel can switch on the required services.

- **Does the firewall perform at or above the expected levels of network traffic?**

Organizations should independently evaluate the firewall to confirm that the vendor's claims are valid. Depending on the provider's size and needs, the firewall should be able to handle a large number of user connections and move traffic quickly with security rules in place.

Figure 4. Firewall Security



### Intrusion Protection Systems

Intrusion protection system (IPS) solutions can also protect the network perimeter against hackers and unauthorized users. An IPS can identify attacks that firewalls cannot detect—for example, distributed denial of service (DDoS) attacks caused by floods of “legal” traffic—by monitoring Internet and extranet connections in real time to protect network resources. 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.

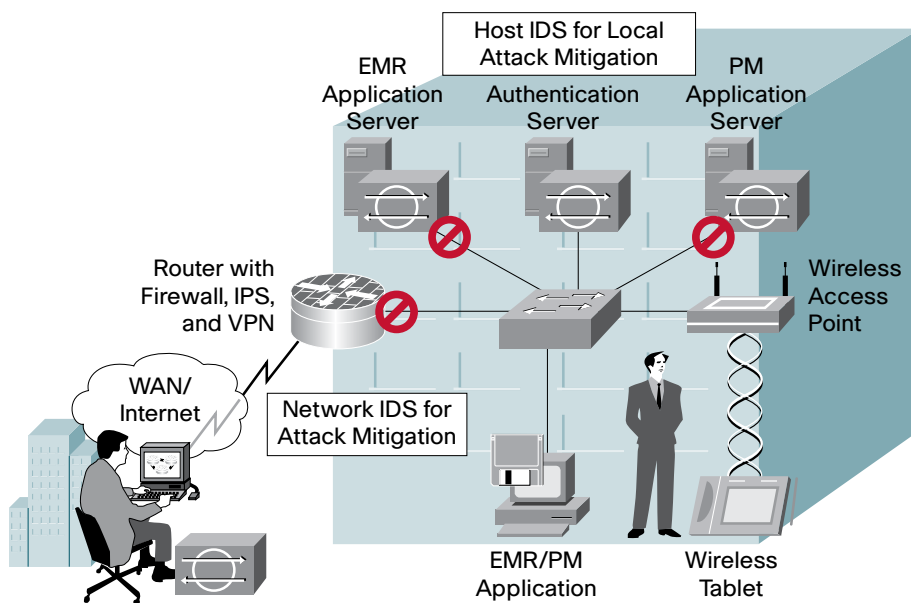
### Host Intrusion Protection Systems

Host intrusion protection systems (HIPSs) are typically loaded on each protected asset. These agents constantly collect information on system resources such as disk space, operating systems, applications, and system audit trails to determine if a security breach has taken place. HIPS agents are tailored specifically for host-related activity and can track events with a fine level of detail (such as reporting which user accessed which file at what time). HIPS agents can be self-contained, sending alarm information to the user of the specific asset being protected, or they can be managed remotely through a central management tool.

### Network Intrusion Protection Systems

Network intrusion protection systems (NIPSs) monitor activity on a specific network segment. A NIPS can be a dedicated platform or software in an access router. A NIPS appliance consists of a sensor that passively analyzes network traffic and a management system that alerts security personnel of potential events. NIPSs can work alongside HIPSs to provide strong, coordinated protection to both network segments and individual resources.

Figure 5. Intrusion Protection



### The Cisco Solution

Cisco offers a complete portfolio of integrated, comprehensive security offerings for the network perimeter. The Cisco 1700 Series Modular Access Router, Cisco 2600 XM Series Multiservice Platforms, and the Cisco 3700 Series Multiservice Access Router deliver fast, reliable network and Internet connectivity. They 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. The addition of Cisco Security Agent provides security capabilities to protect servers and other endpoints.

Large medical practices may require support for more simultaneous connections, higher bandwidth, and higher performance than a smaller practice. For smaller practices, a dedicated Cisco PIX® 500 Series Security Appliance offers enterprise-class firewalling and numerous customizable security services.

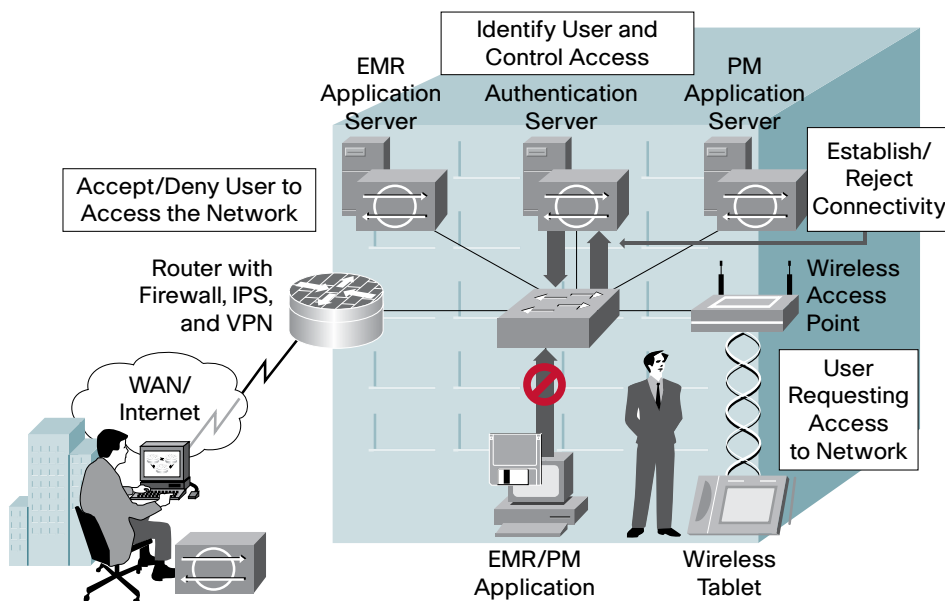
These Cisco routers and firewalls feature easy-to-use, Web-based configuration tools designed to meet the needs of smaller organizations. Even a practice with limited IT resources can deploy and manage perimeter security with confidence.

### The Departmental/Office LAN and Desktops

For most providers, the departmental or office LAN contains desktop PCs, file servers, and daily file backup systems and software. In smaller applications, most of the resources may be contained on a single file server, so it is critical that these resources be secure and available. Organizations should protect these assets with third-party software solutions, such as antivirus scanners and OS security patches, and be sure to update security software regularly. Cisco Security Agent complements third-party antivirus packages and offers day-zero threat protection for servers and other endpoints.

Practices should employ identity services to help identify users and control what they are permitted to do on the network. These should include RADIUS or TACACS+ services that authenticate users and restrict access to sensitive information and network resources.

Figure 6. Access Control



### The Cisco Solution

Secure Cisco LAN switches, such as Cisco Catalyst® 2940 and 2950 series switches, provide native support for most identity services, enabling providers to control switches from a central location and restrict unauthorized users from altering switch configurations. For larger applications, Cisco Catalyst 3550, 3750, and 4500 series switches deliver unparalleled network performance, scalability, and manageability. These switches include Cisco integrated security features, such as advanced user authentication and enhanced security administration tools.

To protect business-critical servers and other endpoints on the network, practices should use Cisco Security Agent, an endpoint protection agent that goes beyond conventional security systems with day-zero identification and prevention of malicious behavior. Cisco Security Agent's management tool is part of the CiscoWorks VPN/Security Management Solution (VMS).

### WLANs

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. However, 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.

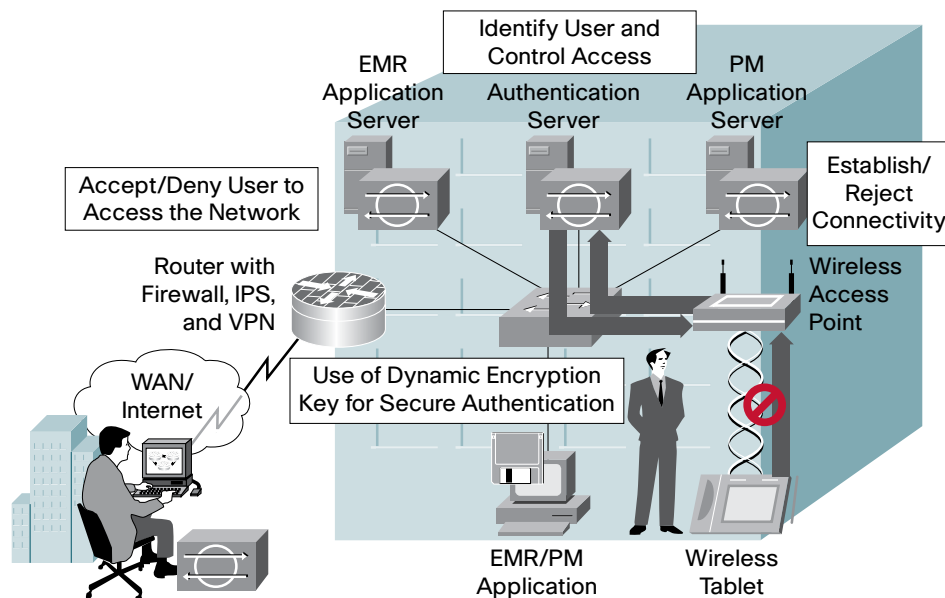
### Deploying WLAN Security

The two primary components of WLAN security are authentication and encryption. Authentication helps ensure that the user and the access point are who and what they say they are. Encryption helps ensure that data remains uncorrupted throughout transmission, and that anyone who might intercept data will be unable to read it.

Traditional WLAN security includes the use of Service Set Identifiers, open- or shared-key authentication, static Wired Equivalent Privacy (WEP) keys, and MAC authentication. This combination of services offers a basic level of access control and privacy, but it is not sufficient to protect sensitive data transmissions in a healthcare environment.

A more secure solution is the IEEE 802.1X standard for authentication on wired and wireless networks. This standard provides strong, mutual authentication for wireless clients and authentication servers. 802.1X provides dynamic, per-user, per-session WEP keys, eliminating the need to manually monitor and change static WEP keys. Several 802.1X authentication types exist, each providing a different approach to authentication while relying on the same framework and the Extensible Authentication Protocol (EAP) for communication between a client and a wireless access point. With 802.1X authentication, the credentials used for authentication, such as a password, are never transmitted over the wireless medium without encryption.

Figure 7. WLAN Security



### The Cisco Solution

Cisco Aironet® 1100 and 1200 series access points deliver highly secure, high-performance wireless connectivity using the IEEE 802.11a and IEEE 802.11b standards. The Cisco Wireless Security Suite, included with Cisco Aironet products, provides robust WLAN security services that closely match the security available in a wired LAN.

The Cisco Wireless Security Suite takes advantage of the EAP framework for user-based authentication to support all 802.1X authentication types, including Cisco EAP (Cisco LEAP), which enables local authentication within individual access points. While Cisco LEAP offers an ideal solution for smaller networks with a limited number of access points, larger networks may prefer to manage wireless authentication centrally. For these organizations, the Cisco Secure Access Control Server (ACS) platform delivers the full range of authentication services for wireless and wired networks.

### Teleworking and Remote Access

Many providers have adopted remote connectivity solutions that give clinicians remote access to necessary 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 their home. As remote connectivity becomes a standard healthcare tool, practices need to provide remote connectivity solutions that are as highly secure and reliable as the wired and wireless office network. Any 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.

Providers should implement remote connectivity solutions that support several options. For example, although DSL may be the practice's broadband technology of choice, some physicians may have access only to a dialup Internet service. Regardless of the access method, the provider network must help ensure proper routing, encryption, and access control.

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 their suppliers and partners, providing limited access to specific portions of the network for collaboration and coordination.

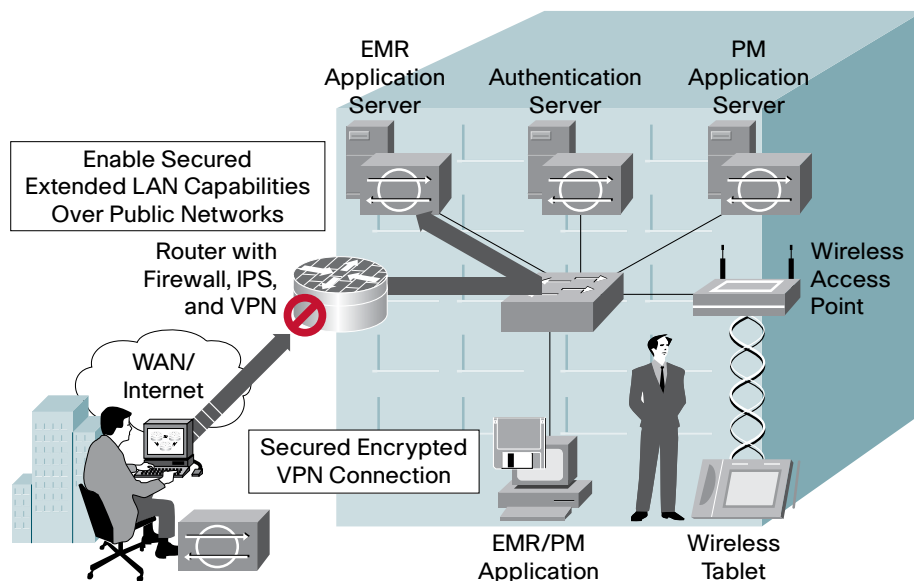
A healthcare VPN solution must include all of the security features needed to keep VPN traffic private and secure. VPNs use a tunneled connection to carry encrypted data between the remote user and the provider network. Providers should make sure that their VPN solutions support primary tunneling protocols, including IP Security (IPSec), Layer 2 Tunneling Protocol, and generic routing encapsulation.

### 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.

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 connectivity 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, Cisco Security Agent has firewall capabilities and complements any type of remote-access VPN.

Figure 8. IP VPN Security



### The Cisco Solution

Cisco offers VPN connectivity solutions for providers of all sizes. Cisco 1700 Series modular access routers, Cisco 2600 XM Series multiservice platforms, Cisco 3700 Series multiservice access routers, and Cisco PIX 500 Series security appliances provide native VPN support, enabling smaller locations to terminate and manage remote VPN sessions without having to deploy a separate appliance. 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 800 Series routers, Cisco uBR 10012 Series cable access routers, and Cisco VPN 3002 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.

### Satellite Locations

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

Providers have two options for connecting the satellite locations—private WAN links and public links. Private WANs—such as Frame Relay, ISDN, T1, and Fractional T1—enable greater control of network traffic, including quality of service (QoS) support and traffic prioritization. Dedicated WAN links are more private, in that they are not shared connections; however, private WANs do not provide inherent security, since the traffic is not encrypted. This alternative typically costs more, with increased operating and ownership expenses. Public shared links, such as cable and DSL, are less expensive but less secure. To address this, IPSec VPNs use encrypted VPN connections over a service provider network or the Internet to support WAN connectivity. A provider should take HIPAA into account when making WAN choices; encrypted IPSec VPNs offer considerably more privacy protection.

### The Cisco Solution

Cisco 1700 Series modular access routers, Cisco 2600 XM Series multiservice platforms, and Cisco 3700 Series multiservice access routers offer built-in support for site-to-site 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.

### 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. Good management tools allow administrators to view and control activity on the network at any time, and to access all network devices through a single interface.

### The Cisco Solution

The CiscoWorks Small Network Management Solution (SNMS) is designed specifically for small and midsize networks. It provides a powerful set of services to address the complete network lifecycle, including Web-based configuration management and troubleshooting tools for Cisco devices and most third-party assets. For larger networks, CiscoWorks VMS offers enterprise-class security features and services for managing larger networks.

## Deployment Blueprints For Providers

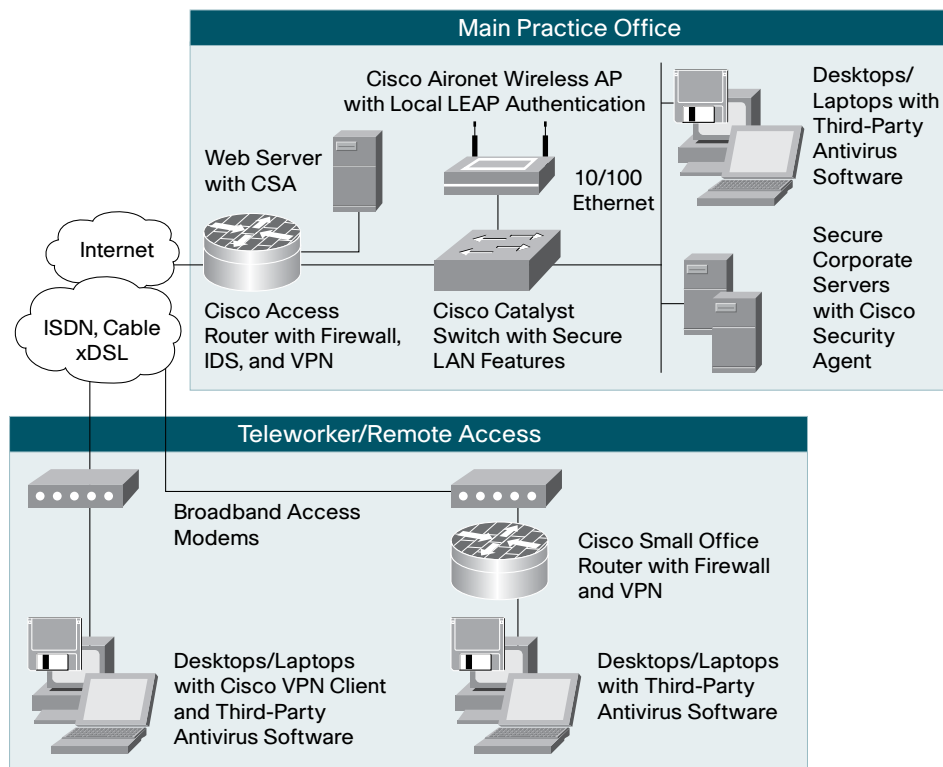
The following blueprints illustrate sample network architectures for small, midsize, and large provider locations.

### Small Location

This deployment blueprint supports a location with approximately 25 total employees. A Cisco 1700 Series Modular Access Router provides all of the connectivity services required for the location, and it supports firewall, IDS, and VPN services in a single, manageable device. A Cisco Catalyst 2940 or 2950 series switch manages bandwidth across the network and delivers applications to local users. Third-party servers running Cisco Security Agent manage authentication services. Cisco Aironet 1100 Series access points are configured to support either the 802.11a or 802.11b standard and provide Cisco LEAP authentication of wireless users.

Teleworkers connect with the networked locations using VPNs managed with the practice's router. Remote users can use Cisco VPN Client software or a Cisco 800 Series Router with firewall features from a home office.

Figure 9. Small Location Deployment Blueprint



### Midsized Location

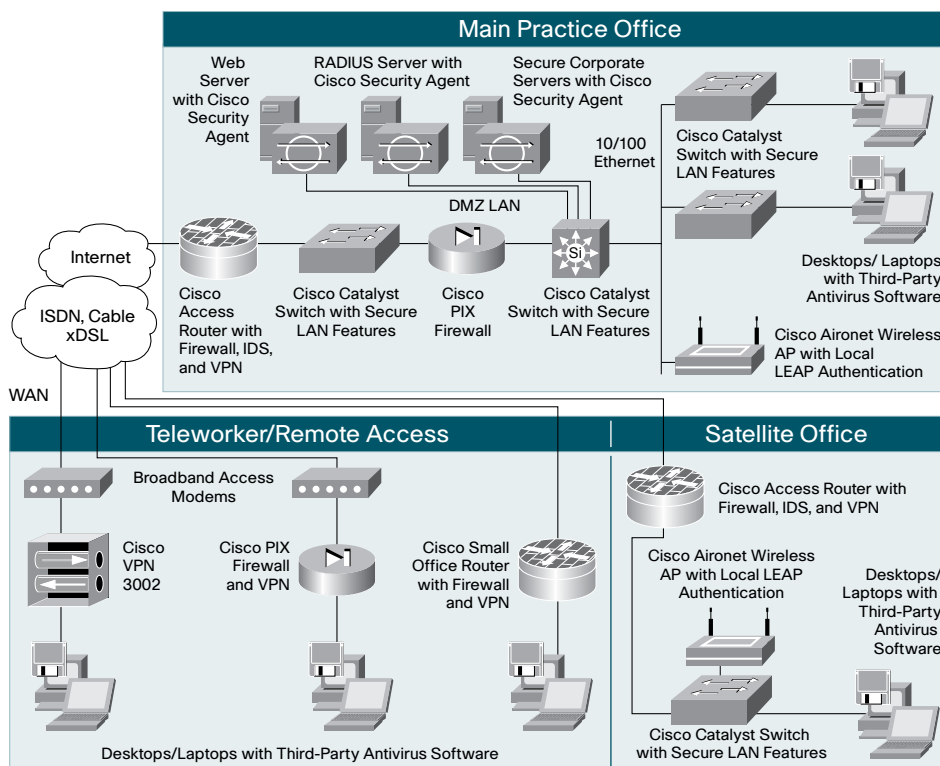
This deployment blueprint supports a practice of approximately 250 employees. In this blueprint, a Cisco 1700 Series Modular Access Router at the location provides connectivity, firewall, IDS, and VPN services at the network perimeter. A Cisco PIX 500 Series Security Appliance has been deployed to provide additional protection for internal network resources. A Cisco Catalyst 2950 Series Switch is deployed between the router and the firewall to support Web servers or other servers accessible to external parties. A Cisco Catalyst 3550 Series Switch links the servers with the 10/100 Ethernet LAN, and Cisco Catalyst 2950 Series switches connect local users.

Midsized locations may use Cisco Aironet 1100 Series access points for local wireless access. Cisco Aironet 1200 Series access points can be deployed if the location needs to support both the 802.11a and 802.11b standards in a single access point. Locations of this size may still use Cisco LEAP authentication within the access points to control access to the wireless network.

Teleworkers based out of a midsized location can use Cisco VPN Client software, a Cisco 800 Series Router with firewall features, or a dedicated VPN hardware client such as the Cisco VPN 3002 Hardware Client or a Cisco PIX 500 Series Security Appliance with VPN features.

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, managed with the IPSec VPN features of Cisco routers.

Figure 10. Midsized Location Deployment Blueprint



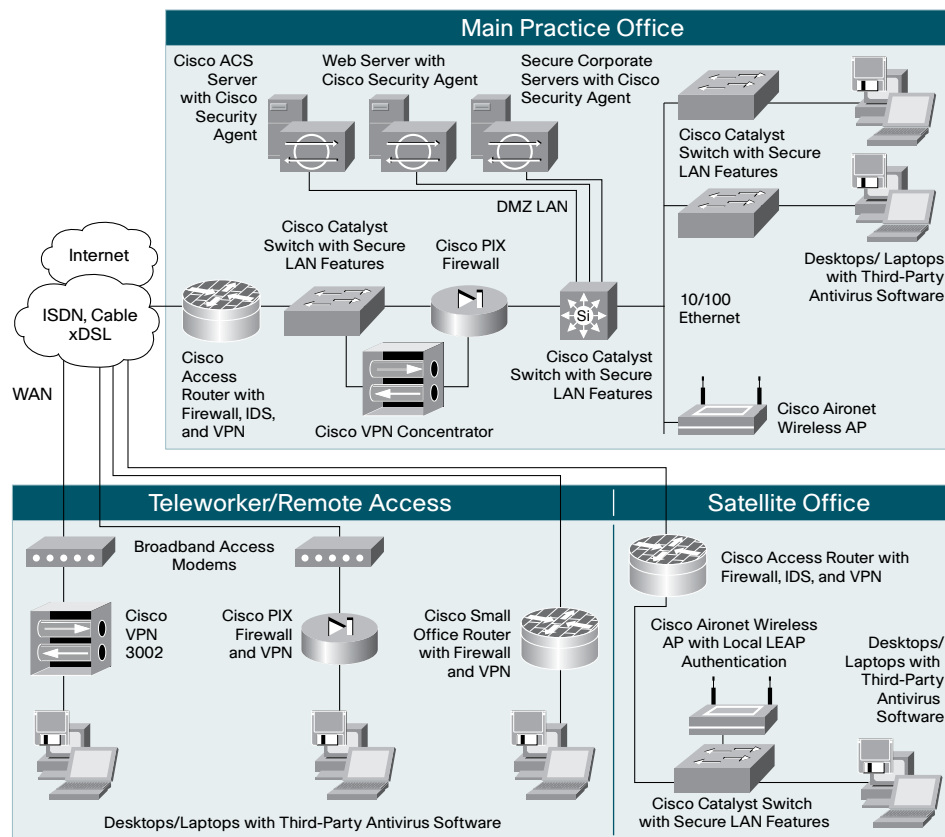
### Large Location

This deployment blueprints illustrates a location with more than 500 total users. In this blueprint, the location uses a Cisco 2600 XM Series Multiservice Platform or 3700 Series Multiservice Access Router to deliver enterprise-class connectivity, firewall, IDS, and VPN services. A Cisco Catalyst 3550 or 4500 series switch is at the core of the network, delivering high levels of performance and network traffic control. Large locations can still use Cisco Catalyst 2950 Series switches to support local users.

Cisco Aironet 1200 Series access points deliver wireless services to local users; however, the access points no longer manage wireless authentication locally. Instead, Cisco Secure ACS provides a more scalable solution for managing all wired and wireless authentication services across the network.

Satellite clinic and teleworker configurations are identical to those used by midsize locations, with one exception. Instead of terminating remote-access VPN tunnels with the Cisco router, a Cisco ASA 5500 series adaptive security appliance provides a more scalable, manageable solution for supporting more than 50 simultaneous VPN connections.

Figure 11. Large Location Deployment Blueprint



## Conclusion

As the risks and security concerns for healthcare networks grow, providers should take a systematic, multitiered 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.

Cisco Protected Healthcare Solutions for Providers offer a comprehensive, modular approach to security—one that can evolve as a provider's needs change. This approach encompasses every aspect of the data infrastructure, from the desktop to the WLAN to the network perimeter and the teleworker—and all areas in between.

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, healthcare 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.



**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100

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](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0705R)