

MEDICAL-GRADE NETWORKS—CISCO PROTECTED HEALTHCARE SOLUTIONS FOR PHYSICIAN GROUPS AND CLINICS

INTELLIGENT NETWORKS. SMART MEDICINE

ABSTRACT

As physician practices adopt 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 physician practices must take to protect the network
- Deployment scenarios for small, midsize, and large practices

EXECUTIVE SUMMARY

Network-based applications have transformed virtually every industry, and healthcare practices are no exception. Solutions like wireless access to electronic medical records (EMRs), practice management systems, and online claims submissions are no longer just the domain of large hospitals and health systems. Today, even small medical practices can use these tools to more effectively communicate and collaborate, reduce errors, and deliver better overall patient care.

As smaller healthcare practices adopt new technologies, however, they also face new security threats. With hackers, computer viruses, disaffected employees, and even human error presenting real dangers to healthcare networks, a locked file cabinet or office door is no longer sufficient to protect confidential patient information.

Fortunately, most security breaches can be prevented and numerous network security tools are now available. These tools are easy to deploy and to use, even for smaller organizations such as physician groups. Cisco[®] Protected Healthcare Solutions for Physician Groups and Clinics provide scalable, comprehensive security that enables small and midsize physician practices to combat threats just as effectively as a large hospital or health system.

The first step in establishing a secure network infrastructure is the development of a formal security policy to define roles, responsibilities, acceptable use, and security practices for the organization. After developing the policy, the practice may consider conducting an assessment, using established best practices as a benchmark. Practices should closely examine their existing network infrastructures to identify potential vulnerabilities—including physical security.

As they move forward to design, upgrade, and install secure network architectures, physician practices must evaluate each area of the network, determine potential threats, and implement appropriate security measures. If the practice does not have a technical expert, Cisco Partners are trained to help develop and implement a comprehensive security solution. To locate a Cisco Partner, visit:

http://tools.cisco.com/WWChannels/LOCATR/jsp/partner_locator.jsp

Cisco and its partners offer multitiered solutions to provide robust protection to every portion of the data infrastructure, from the desktop to the network perimeter, enabling physician practices to use modern, network-enabled technologies with confidence.

THE NEED FOR NETWORK SECURITY IN HEALTHCARE

While information security is a top priority for any organization, healthcare practices must be especially diligent about protecting confidential patient data. In addition to the evolving threat posed by hackers and other intrusions, government regulations, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA), set privacy requirements for Protected Health Information (PHI). Simply deploying a firewall in the network is not sufficient—practices need to take a comprehensive approach to protecting patient information at every potential point of access, inside and outside the network.

Escalating Security Threats

As healthcare practices digitize systems and records, they increasingly rely on networks for their core operations—making them even more vulnerable to attacks. Compromised security can disrupt critical practice functions, interfere with a clinician's ability to treat patients, expose practices to substantial fines and legal liability, and risk the loss of reputation.

Network attacks can be as varied as the systems that they attempt to penetrate. Some attacks are elaborately complex. Other threats might be unintentional security breaches by employees; although unintentional, these threats can still cause significant damage. Security attacks by internal employees are the most common, according to a 2003 survey by the U.S. Computer Security Institute/Federal Bureau of Investigation (CSI/FBI), and are 10 times as costly as an external attack.

To understand potential attacks, it is important to be aware of some of the inherent limitations of TCP/IP. When the Internet was formed, it linked various government entities and universities to one another to facilitate learning and research. Because the original architects of the Internet never anticipated its widespread commercial adoption, security was not built into the IP specification. As a result, most IP implementations are inherently insecure. Cisco Systems® has dedicated significant resources to designing networking solutions that can protect your network.

Because specific provisions for IP security were not designed from the outset, physician practices need to make sure that their IP implementations include network security practices, services, and products that can mitigate the inherent risks of the protocol. Common network threats include:

- *Packet sniffers*—A packet sniffer is a legitimate management tool that can be abused by hackers to capture data transmitted over a network, such as usernames and passwords.
- *IP spoofing*—An IP spoofing attack occurs when a hacker inside or outside a network impersonates a trusted computer to gain access to network information.
- *Defacing*—Defacing attacks focus on changing the files on a Web server. For practices that maintain a Web presence, defacing 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 attack can be initiated using programs that are available for download on the Internet. They focus on making a service unavailable for normal use, often by exhausting a resource on the network, OS, or application.

- *Spam*—Another growing threat to network operations is spam, or unsolicited mass e-mail, which slows mail servers, overruns storage space, and reduces user productivity by clogging individual mailboxes.
- *Man-in-the-middle attack*—A man-in-the-middle attack is initiated by hackers who have access to network packets that move across a wired or wireless network. 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 disguise the application to look like something else. Worms are malicious programs that replicate themselves.
- *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 to perform malicious activities, 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 exploiting well-known software weaknesses commonly found on servers, such as sendmail, HTTP, and FTP, to gain access to a computer with a high level of administrative access.

The Costs of Poor Security

Network security breaches can be devastating to physician practices, risking fines, legal liability, lost productivity of clinical and administrative staff, and loss of confidence of patients and partners. Small practices are especially vulnerable because they often lack the staff and budget needed to respond effectively to a security breach. In addition to the costs of repairing the network itself, the impact on a physician practice can include:

- *Disruption of clinical and administrative processes*—A common immediate effect of poor security is network downtime and loss of critical server and application operations. The more that physicians rely on wireless networks, EMR and practice management systems, and clinical information systems, the more an unavailable network can interfere with a practice's ability to treat patients. Network-based applications for managing office functions and processing claims can be unavailable for days at a time while a security breach is repaired.
- *Loss of patient and partner confidence*—A practice that has been victimized by hackers can 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, practices that fail to protect confidential patient data could face stiff penalties and liability from litigation.

To combat these threats, practices need a consistent, scalable, corporate-wide security solution that enables them to continually safeguard their networks.

Benefits of Maintaining a Secure Healthcare Environment

Physician practices that employ strong security do more than just protect patient and practice data. In fact, once healthcare networks are secure, organizations can deploy many state-of-the-art technologies that enhance patient care and make it easier for clinicians to do their jobs. A secure healthcare practice network can enable:

- *Access to information at the point of care*—A secure wired or wireless network allows physicians 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 physicians to access patient information, lab results, and medical libraries from tablet computers, PDAs, mobile phones, and remote and home offices.
- *Enhanced productivity and reduced costs*—Once a secure, reliable network is in place, healthcare practices can deploy applications that streamline resource-intensive back-office processes. Solutions can include practice management applications, claims processing systems, and systems for finance and human resources processes.
- *Improved patient care and safety*—Digital clinical applications and real-time information sharing enabled by a secure network result in a more unified, up-to-date view of the patient, and in faster, more accurate care. When physicians can securely update records and write prescriptions digitally and at the point of care, they can substantially reduce the errors associated with hand-written, paper-based systems.

CISCO PROTECTED HEALTHCARE SOLUTIONS FOR PHYSICIAN GROUPS AND CLINICS

Cisco Protected Healthcare Solutions for Physician Groups and Clinics are based upon end-to-end blueprints for designing, implementing, and maintaining 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 a firewall or intrusion detection system (IDS). This strategy results in a layered approach to security, where the failure of one security system is not likely to lead to the compromise of network resources.

The security strategy behind Cisco Protected Healthcare Solutions for Physician Groups and Clinics is built around some 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, as well as network devices such as routers, switches, wireless access points and appliances, must play a part in protecting the organization from both 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.
- In order to keep costs down and ensure scalability and flexibility, security solutions should be modular.
- A layered, in-depth defense strategy provides more complete protection and minimizes areas of potential vulnerability.

A Modular Blueprint Based on Best Practices

Each Cisco Protected Healthcare Solutions for Physician Groups and Clinics blueprint uses a modular approach offering two main advantages. First, it allows network planners to address the security relationship between the various 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 physician practices that incorporate wired and wireless infrastructures, satellite locations, and remote connectivity.

Cisco Protected Healthcare Solutions for Physician Groups and Clinics 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.

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 regularly updated and correctly maintained.
- *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 healthcare 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 (AAA) 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*—VPNs provide a 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*—This includes the tools for monitoring and maintaining security. It holds together 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

As the first step in ensuring a secure environment, organizations need a sound security policy that addresses all of a practice's people, processes, and technologies. A security policy is a formal, published 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.

Elements of a Security Policy

Since a security policy affects all aspects of a physician practice, it should be created through a collaborative process that includes clinical, administrative, legal, and technology staff. The individual in charge of a practice's physical security is often the best choice to lead the team. Developing a policy can take up to several weeks, depending on the size of the practice.

The elements of a security policy include:

- *Policy statement*—A concise statement of the purpose of the document, a policy statement should be specific to the individual practice 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*—Security 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 security 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 who gets the first alert for various threat levels and the specific steps required for response.
- *Document control factors*—Organizations should define how updates to the security policy will occur.

As practices develop a security policy, they may want to begin with a simplified, high-level security policy and refine it over a year-long period. Sample policies can be found at:

<http://www.sans.org>

which is a good starting point. 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 continually reviewing the security policy to incorporate new threats and organizational changes.

Identifying Vulnerabilities

A typical physician practice network can have many potential vulnerabilities, including partner extranets, VPNs, “always-on” broadband connections, and WLANs. Potential vulnerabilities can be identified 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. Small and midsize practices should budget for yearly, proactive reviews of firewall configurations.

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

Organizations should check VPNs, modem dialup lines, and remote control software, as well as other external connections to insurers, vendors, and partners.

- *Do you have a Web site?*

If you operate a Web server for patient or partner access, keeping the server safe from hackers requires considerable effort. At a minimum, every Web server’s underlying OS should be configured to conform to OS vendor security checklists. Practices should also develop a process to evaluate and install security patches within a week of the OS vendor’s distribution. Endpoint security software (Cisco Security Agent, for example) can also offer day zero 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 practices 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. The specific security implementation will depend on the size of the practice and, for HIPAA requirements, the practice’s risk tolerance. Minimally, any secure network architecture should include protection for the network perimeter, the office LAN, teleworker connections, WLANs, and any satellite locations.

Cisco Channel Partners, VARs, and managed security service providers (MSSPs) can be especially helpful to small and midsize physician practices, which generally lack the staff or expertise of larger healthcare institutions. 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

The Network Perimeter

Most small and midsize physician practices choose economical ISDN, digital subscriber line (DSL), or broadband cable for Internet access. While these high-speed services are usually more than sufficient to support practice applications, they can pose a greater risk than leased-line services. For example, a single DoS attack on a practice's Web server can take up all of the available bandwidth. And, unlike leased lines that service a single user, broadband connections are usually shared connections, creating the potential risk of users seeing each others' data.

Firewalls

The best way to protect the perimeter is with a business-class firewall, or an access router with stateful inspection firewall features. For smaller practices with limited IT budgets and staff, an integrated router can provide a manageable, cost-effective solution. Larger practices, however, may require the increased capabilities of a dedicated firewall.

Whether hardware- or software-based, a firewall encircles a practice'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 practice's network and IT environment
- Lock unwanted or dangerous transmissions from unauthorized outsiders
- Filter the Internet content that users are allowed to view

Although a firewall is critical for any business connected to the Internet, implementation and maintenance often tax the limited IT resources of most small and midsize physician practices. 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:

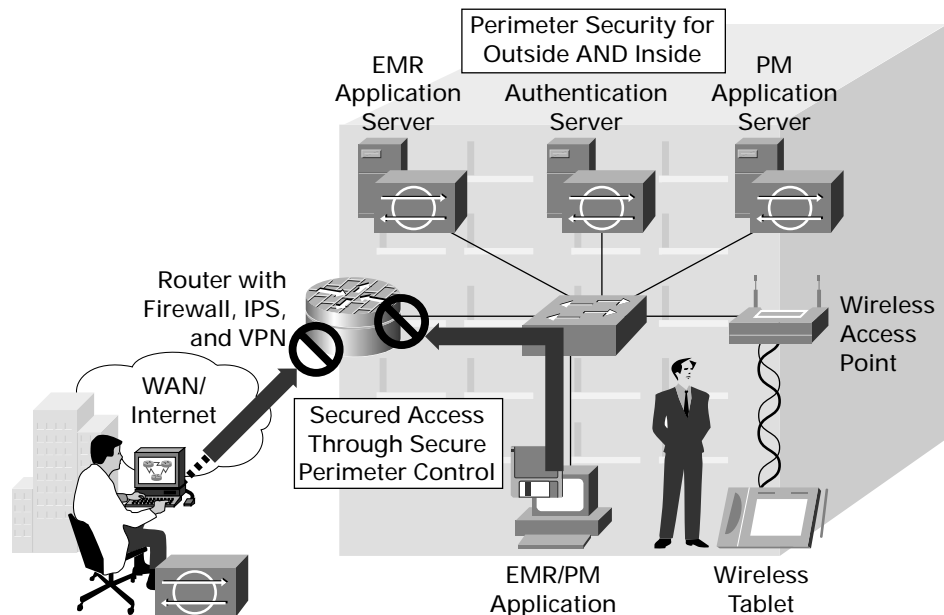
- *Does the firewall support our network security policy, or does it impose the vendor's policy?*

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 size and needs of the practice, the firewall should be able to handle a large number of user connections and to move traffic quickly enough with security rules in place.

Figure 1
Firewall Security



Intrusion Protection Systems

Intrusion protection system (IPS) solutions can also protect the network perimeter against hackers and unauthorized users. IPSs identify attacks that firewalls cannot detect (for example, distributed DoS [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 thwart further attacks. IPS solutions can be network-based systems (appliance-based sensors or a feature set in access router software) or host-based software agents.

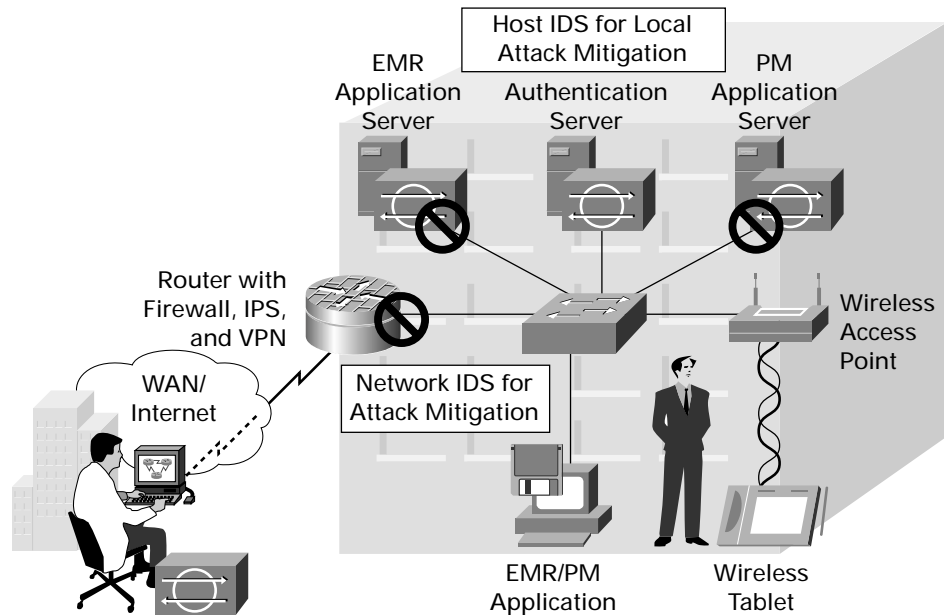
Host-based IPSs

Host-based IPSs (HIPSs) are typically loaded onto 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 remotely managed through a central management tool.

Network-based IPSs

Network-based IPSs (NIPSs) monitor activity on a specific network segment. NIPSs can be a dedicated platform or software in an access router. An 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 2
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, the Cisco 2600 Series Multiservice Access Router, 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 physician practices may require support for more simultaneous connections, higher bandwidth, and higher performance than a smaller organization. For these practices, a dedicated Cisco PIX[®] 500 Series Security Appliance offers enterprise-class firewalling and numerous customizable security services.

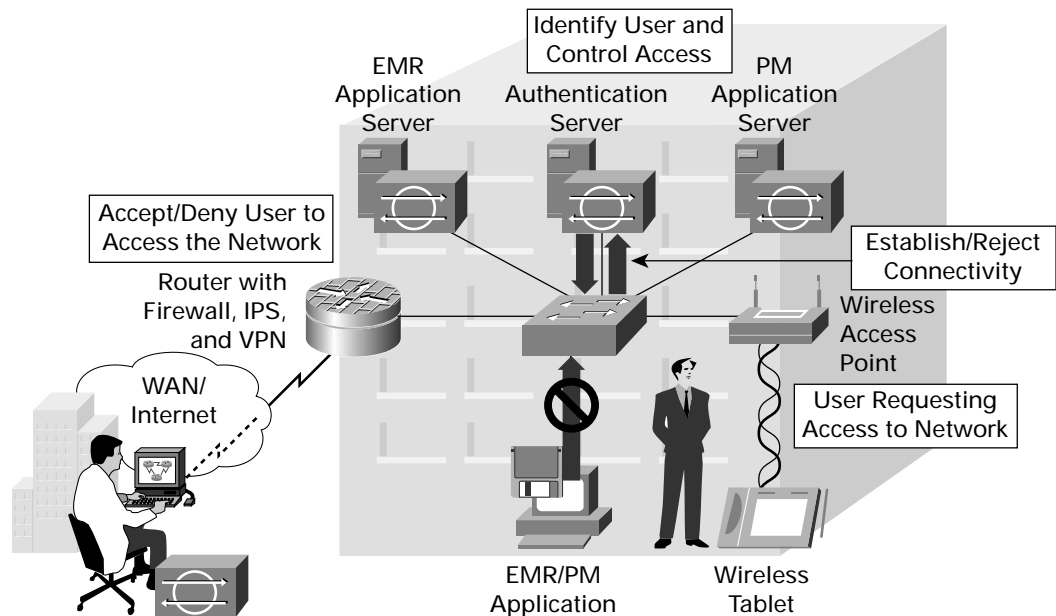
These Cisco routers and firewalls feature easy-to-use, Web-based configuration tools designed to meet the needs of smaller organizations. Even a practice with limited IT resources can deploy and manage perimeter security with confidence.

The Office LAN and Desktops

For most practices, the office LAN contains desktop PCs, file servers, and daily file backup systems and software. In a small practice, most of the office's resources may be contained on a single file server, so it is critical for these resources to 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 3
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 practices to centrally control switches and restrict unauthorized users from altering switch configurations. For larger practices, 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 CiscoWorks VPN/Security Management Solution (VMS).

WLANs

Perhaps no industry has benefited more from wireless networking than healthcare. Physicians and nurses can now use wireless-enabled tablet computers and PDAs 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, practices need to ensure that WLANs provide the same level of access control and privacy as wired LANs. In contrast to a wired LAN, where access is controlled by physical access to an Ethernet port, WLANs broadcast data through the air. Any wireless-enabled device in the area—including a patient’s laptop in a waiting room or a wireless device in a neighboring office—presents a potential security threat.

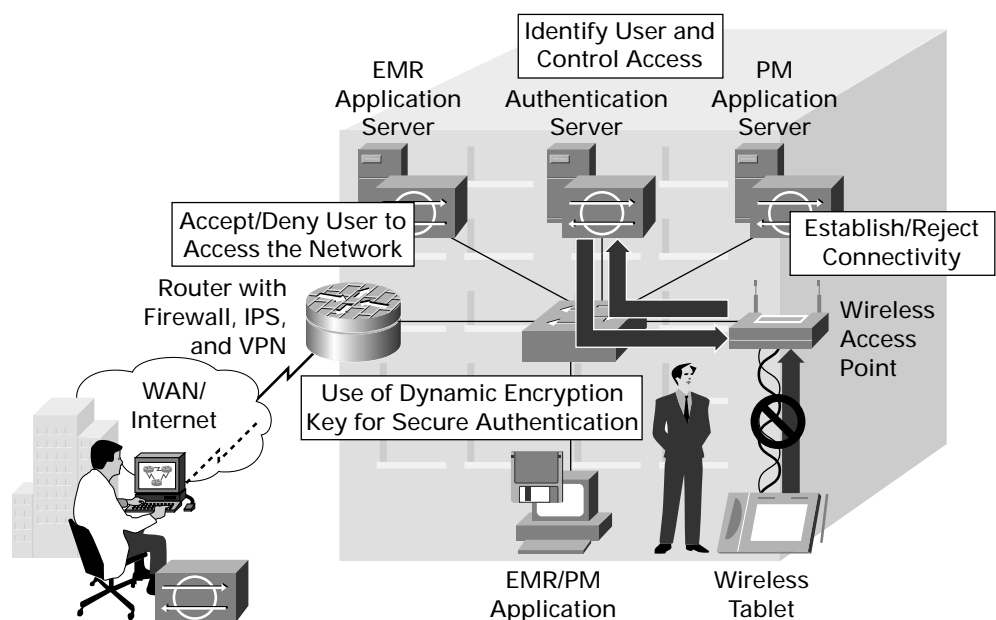
Deploying WLAN Security

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

Traditional WLAN security includes the use of service set identifiers (SSIDs), open- or shared-key authentication, static Wired Equivalent Privacy (WEP) keys, and Media Access Control (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 at a physician practice.

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 without encryption over the wireless medium.

Figure 4
WLAN Security



The Cisco Solution

Cisco Aironet® 1100 and 1200 series wireless access points deliver 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 parallel 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 (LEAP), which enables local authentication within individual access points. While LEAP offers an ideal solution for smaller practices with a limited number of access points, larger practices may prefer to manage wireless authentication centrally. For these organizations, the Cisco Access Control Server (ACS) platform delivers the full range of wireless and wired authentication services.

Teleworking and Remote Access

Many practices have adopted remote connectivity solutions that enable physicians to access practice applications remotely. Using VPNs, physicians can now securely access patient and clinical information from an off-site conference, a satellite facility, and even from home. As remote connectivity becomes a standard healthcare tool, practices need to ensure that remote connectivity solutions are as secure and reliable as the wired and wireless office network.

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

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

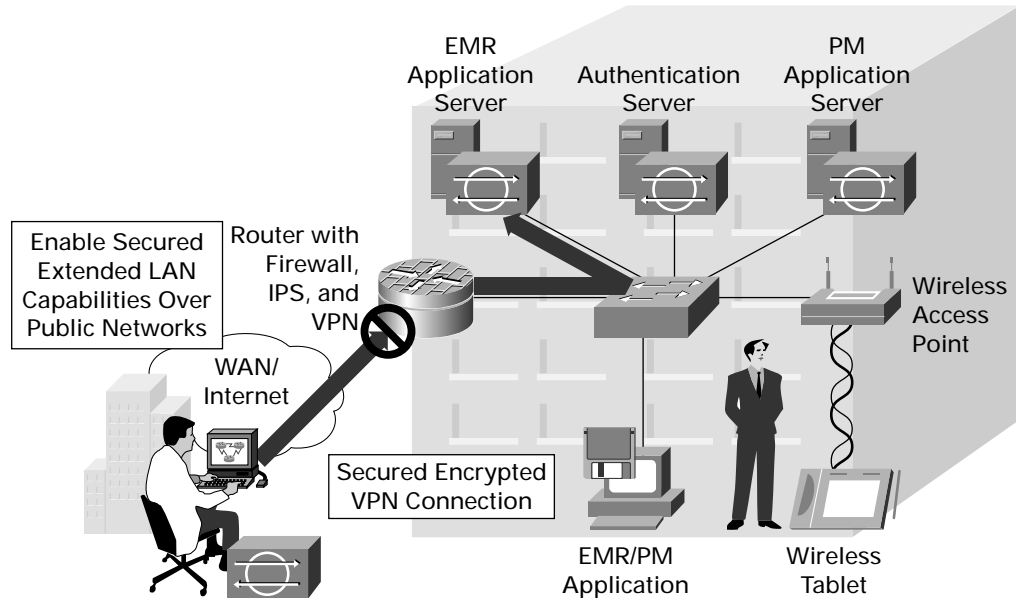
A healthcare VPN solution must include all of the security features needed to keep VPN traffic private and secure. VPNs use a "tunneled" connection to carry encrypted data between the remote user and the practice network. Practices should make sure that their VPN solutions support primary tunneling protocols, including IP Security (IPSec), Layer 2 Tunneling Protocol (L2TP), and generic routing encapsulation (GRE).

VPN Hardware and Software Client

Remote physicians can use software or hardware VPN clients to connect with the practice, or they can take advantage of Secure Sockets Layer (SSL) VPNs or "clientless" VPNs that require only a Web browser. For physicians who will use the solution while traveling or working from a remote conference or satellite location, the software client or SSL VPN makes the most sense. However, when using a software client, information on the physician's PC is only protected while connected to the VPN (information on the laptop is not inherently protected while a physician is surfing the Internet, for example).

For a physician'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 office with more than one user, the office router or firewall can also act as a VPN client, providing 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 5
IP VPN Security



The Cisco Solution

Cisco offers VPN connectivity solutions for physician practices of all sizes. Cisco 1700 Series modular access routers, Cisco 2600 Series multiservice access routers, Cisco 3700 Series multiservice access routers, and Cisco PIX 500 Series security appliances provide native VPN support, enabling smaller practices to terminate and manage remote VPN sessions without deploying a separate appliance. Larger practices that require support for more than 50 simultaneous VPN tunnels can deploy a more scalable Cisco VPN 3000 Series Concentrator behind the router or firewall.

For remote small and home offices, Cisco 800 Series secure routers, Cisco uBR900 Series cable access routers, and Cisco VPN 3002 hardware clients provide a secure, high-performance teleworker solution. Traveling physicians can use Cisco VPN Client software, a secure, intelligent software client included with all Cisco VPN solutions, or the SSL VPN currently available with the Cisco VPN 3000 Series Concentrator.

Satellite Offices

Satellite offices of a physician practice function as independent, autonomous networks with their own local servers and user workstations. The satellite office should be configured in the same way as a small practice's main office, and should include the same components, design principles, and considerations discussed above. However, practices still need to consider WAN connectivity to the main office.

Practices have two options for connecting the satellite office—private WAN links and IPSec VPNs. Private WANs, such as Frame Relay, 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, since traffic is not encrypted, private WANs do not provide inherent security. Alternatively, IPSec VPNs use encrypted VPN connections over a service provider network or the Internet to support WAN connectivity. Bandwidth costs for VPN connections are generally much less than private WAN links. HIPAA should be taken into account when making WAN choices; encrypted IPSec VPNs offer considerably more privacy protection to the traffic traveling over them.

The Cisco Solution

Cisco 1700 Series modular access routers, Cisco 2600 Series multiservice access routers, 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 secure, cost-effective WAN connectivity in a single, highly manageable form factor.

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 life cycle, including Web-based configuration management and troubleshooting tools for Cisco devices and most third-party assets. For larger practices, CiscoWorks VMS offers enterprise-class security features and services for managing larger networks.

DEPLOYMENT BLUEPRINTS FOR PHYSICIAN PRACTICES

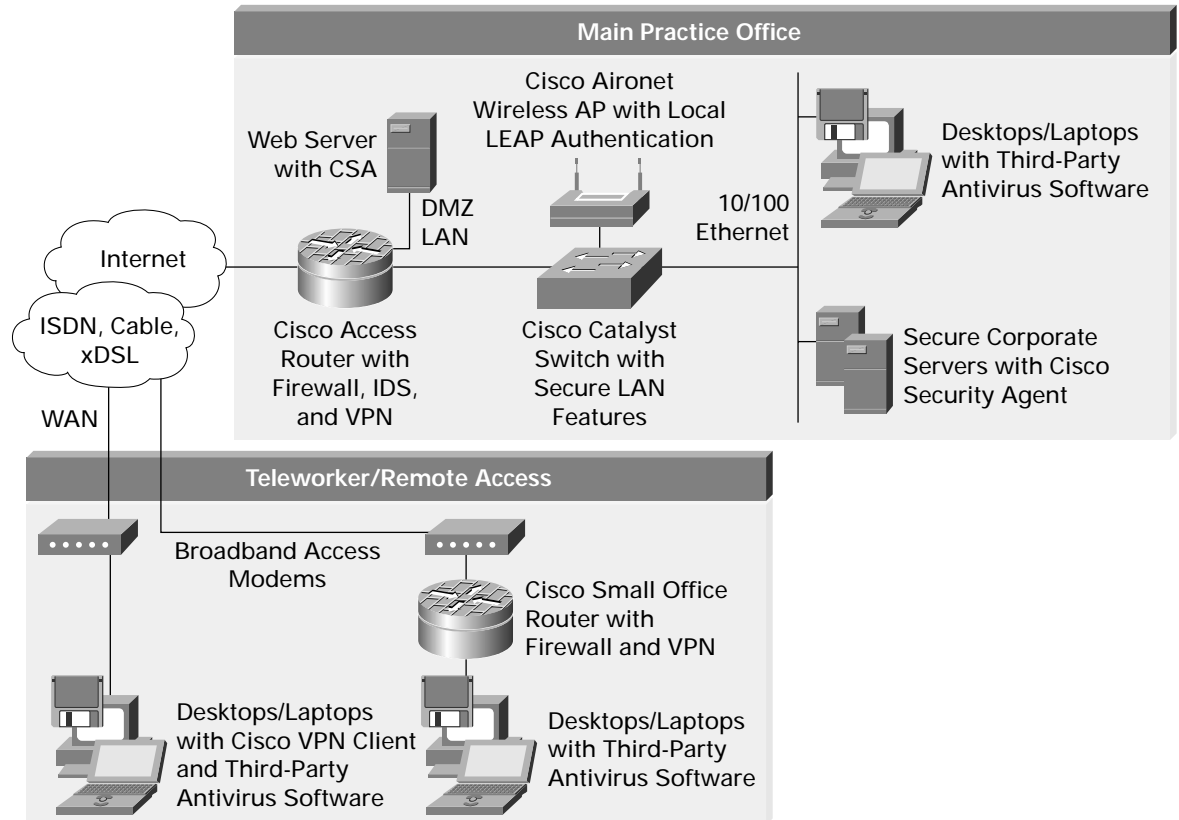
The following blueprints illustrate sample network architectures for small, midsize, and large practices.

Small Practice

This deployment blueprint supports a practice with 1 to 5 physicians and up to 25 total employees (Figure 6). A Cisco 1700 Series Modular Access Router provides all of the connectivity services required for the practice's main office, as well as supporting 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 LEAP authentication of wireless users.

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

Figure 6
Practice with One to Five Physicians



Midsize Practice

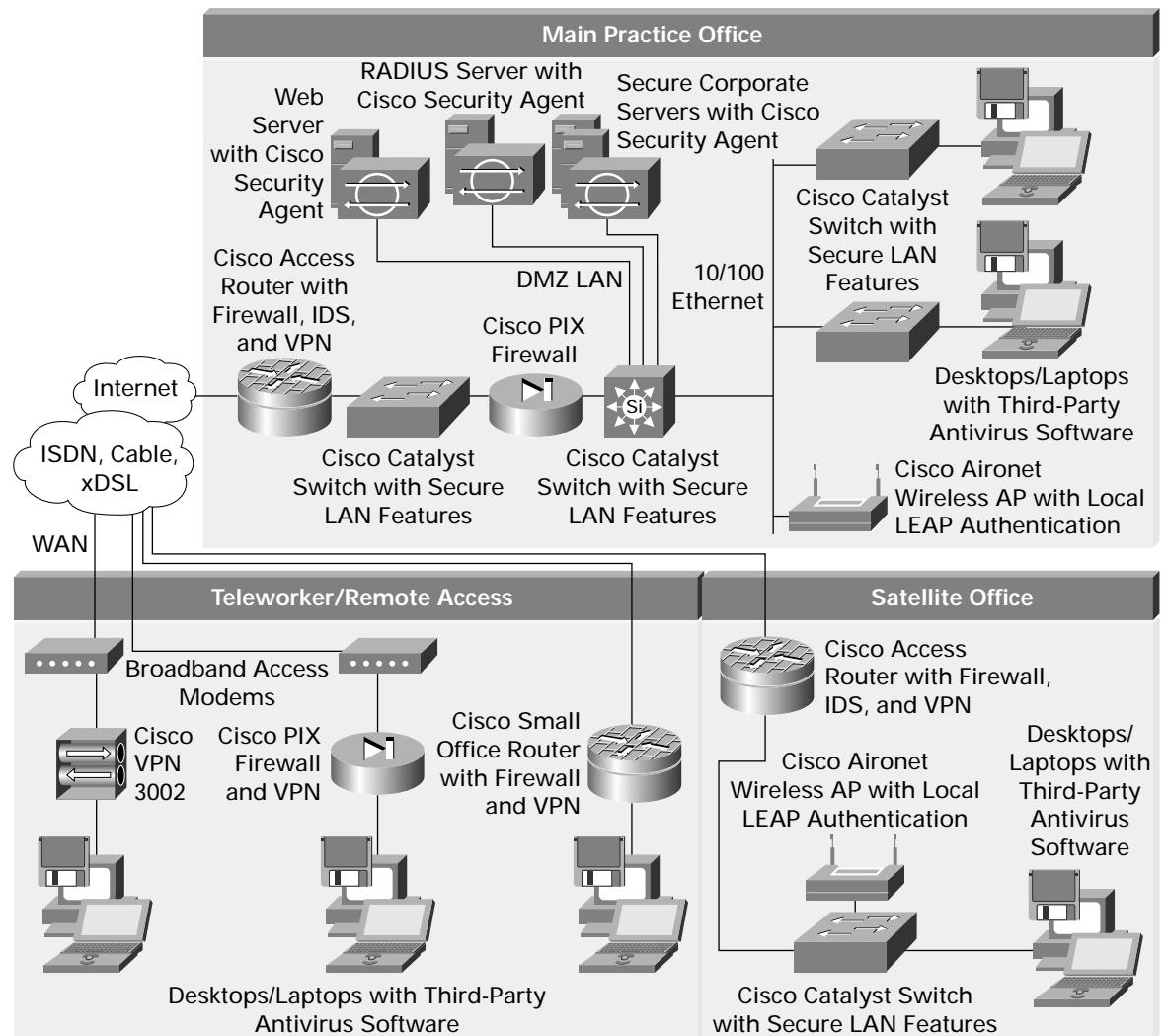
This deployment blueprint supports a practice with 6 to 49 physicians, and up to 250 total employees (Figure 7). In this blueprint, a Cisco 1700 Series Modular Access Router at the main practice office provides connectivity, firewall, IDS, and VPN services at the network perimeter. A Cisco PIX 500 Series 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 servers with the 10/100 Ethernet LAN, and Cisco Catalyst 2950 Series switches connect local users.

Midsize practices can use Cisco Aironet 1100 Series access points for local wireless access. Or, if the practice needs to support both the 802.11a and 802.11b standard in a single access point, Cisco Aironet 1200 Series access points can be deployed. Practices of this size still use LEAP authentication within the access points to control access to the wireless network.

Teleworkers at a midsize practice can use Cisco VPN Client software, a Cisco 800 Series Secure Router with firewall features, or a dedicated VPN hardware client such as the Cisco VPN 3002 Hardware Client or a Cisco PIX 500 Series Firewall with VPN features.

In this deployment, the main practice office also connects with a satellite office. The satellite deployment is identical to the architecture used for a small physician practice. WAN connectivity is delivered through an IPSec VPN tunnel between the main practice office and the satellite clinic, managed with the IPSec VPN features of the Cisco routers.

Figure 7
Practice with 6 to 49 Physicians



Large Practice

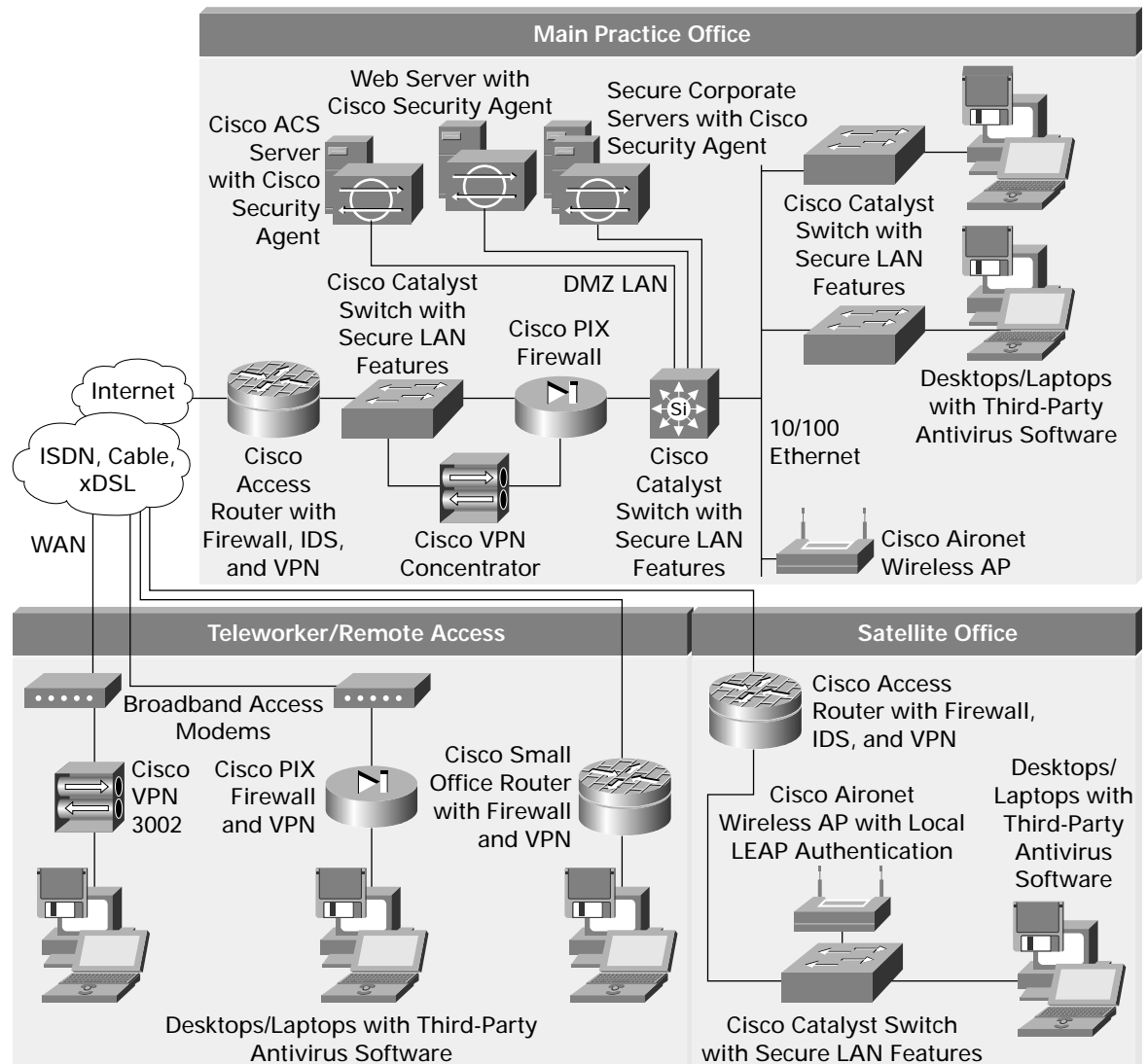
This deployment blueprints illustrates a practice with 50 to 99 physicians (up to 500 total users) or a practice with more than 100 physicians (more than 500 total users) (Figure 8). The basic network architecture is the same for both sizes; however, a practice with more than 100 physicians may require a more robust, scalable access router and switch, and more LAN switches to support additional users.

In this blueprint, the practice uses a Cisco 2600 or 3700 series multiservice platform to deliver enterprise-class connectivity, firewall, IDS, and VPN services. At the core of the practice network is a Cisco Catalyst 3550 or 4500 series switch that delivers the highest levels of performance and network traffic control. Large practices can still use Cisco Catalyst 2950 Series LAN switches to support local users.

Cisco Aironet 1200 Series access points deliver wireless services to local users; however, wireless authentication is no longer managed locally by the access points. Instead, Cisco 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 a midsize practice with one exception. Instead of terminating remote-access VPN tunnels with the Cisco router, a Cisco VPN 3000 Series Concentrator provides a more scalable, manageable solution for supporting more than 50 simultaneous VPN connections.

Figure 8
Practice with 50 to More Than 100 Physicians



CONCLUSION

As the risks and security concerns for healthcare networks grow, physician practices should take a systematic, multitiered approach to planning and deploying a secure network infrastructure. This approach should include a careful evaluation of each area of the network, identification of potential threats, and development of a practice security policy, as well as implementation of network security technologies.

Cisco Protected Healthcare Solutions for Physician Groups and Clinics offer a comprehensive, modular approach to security that can evolve as a practice'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 practices 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 best practices gained from working with healthcare organizations around the world, and can help physician practices deploy secure network services with confidence.

APPENDIX A: PRODUCT LIST

The following products, discussed in this guide, can be part of a comprehensive Cisco network infrastructure:

- *Cisco Aironet 1100 Series access points*—Secure wireless access points compliant with either the 802.11a or 802.11b standard, offering all the features of a wired LAN connection with enhanced wireless security features, including LEAP authentication.
- *Cisco Aironet 1200 Series access points*—Dual-mode wireless access points, compliant with 802.11a and 802.11b, that deliver enterprise-class security, manageability, and reliability for high-performance WLANs.
- *Cisco PIX 500 Series security appliances*—Firewall platforms that cost-effectively deliver robust, easy to deploy security services, including stateful packet inspection (SPI), firewall, IPSec VPN, and intrusion protection.
- *Cisco 800 Series secure routers*—Fixed-configuration routers tailored for small and home offices and telecommuters. These routers support ISDN, DSL, serial connections (such as Frame Relay or asynchronous dialup), or dual Ethernet.
- *Cisco uBR900 Series cable access routers*—This small office/home office access router combines a fully integrated Cisco IOS® Software router and DOCSIS 1.1 standards-based cable modem in a single device.
- *Cisco 1700 Series modular access routers*—A cost-effective platform for small and midsize organizations and enterprise small branch offices. The series supports network connectivity, firewall, IDS, VPN, and other services in a single, integrated form factor ideal for small offices.
- *Cisco 2600 Series multiservice platforms*—A modular access router that delivers enterprise-class versatility for larger organizations, as well as supporting integrated security and enhanced communications services.
- *Cisco 3700 Series multiservice platforms*—An enterprise-class access router that delivers the highest levels of application and service integration, as well as scalability and manageability.
- *Cisco Catalyst 2950 Series switches*—A line of affordable, fixed-configuration, stackable, and standalone switches that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity.
- *Cisco Catalyst 3550 Series switches*—A scalable line of stackable 10/100 and Gigabit Ethernet switches that deliver premium performance, availability, and security, as well as support for integrated voice, video, and data.

- *Cisco Catalyst 4500 Series switches*—A line of enterprise-class, high-density switches offering integrated Fast Ethernet and Gigabit Ethernet LAN connectivity, packet telephony, content networking, security, and QoS.
- *Cisco VPN 3000 Series concentrators*—Purpose-built, remote-access VPN platforms that combine high availability, high performance, and scalability with the most advanced encryption and authentication techniques available.
- *Cisco VPN 3002 hardware clients*—Ideal for remote office or home office deployments, these devices combine the ease of use and scalability of a VPN software client with the additional reliability and stability of a hardware platform.
- *CiscoWorks SNMS*—A Web-based network management solution that provides smaller organizations with a powerful set of network life cycle tools, including configuration management and troubleshooting for Cisco and third-party network devices.
- *CiscoWorks VMS*—A bundle of applications that provides centralized security monitoring and management for larger networks.
- *Cisco Security Agent*—An endpoint protection agent for both desktops and servers that provides protection against day zero attacks and known threats.

APPENDIX B: DEPLOYMENT AND SUPPORT SERVICES

Cisco and its partners offer several services to help smaller organizations manage every aspect of network planning, design, configuration, implementation, and ongoing support.

Technology and Service Specialized Partners

Technology specializations provide Cisco partners with comprehensive training for planning, deployment, and post-deployment support. Organizations working with these partners are assured that they have proven expertise with Cisco technologies.

Cisco Direct and Partner Enabling Services

Cisco Technical Support Services augment the resources of IT staff by providing them with access to information, expertise, and software updates. Cisco's industry-leading Technical Assistance Center (TAC) and Cisco SMARTnet[®] services help to ensure that Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

For more information on Cisco support services, visit:

http://www.cisco.com/en/US/products/svcs/ps3034/ps2827/serv_group_home.html

Cisco Advanced Services

Cisco Advanced Services are a comprehensive suite of professional engineering support offerings for Cisco networking solutions, delivering the highest levels of availability, QoS, and security.

For more information on Cisco Advanced Services, visit:

http://www.cisco.com/en/US/products/svcs/ps11/services_segment_category_home.html

Cisco Secure Consulting Services

Cisco Secure Consulting Services provide customers with responsive, unparalleled network security expertise. Cisco Network Security Engineers (NSEs) have professional experience in critical information protection in military and commercial environments, and are entrusted by Fortune 100 clients.

For more information on Cisco Secure Consulting Services, visit:

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns267/networking_solutions_package.html



Corporate 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: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Aironet, Catalyst, Cisco IOS, PIX, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R) N2/JB/LW5648 02/04