Technical Paper

Healthcare Information Security

How a Secure Data Network Can Help Healthcare Organizations Meet the Challenge of Healthcare Security Regulations

Healthcare Information Security

How a Secure Data Network Can Help Healthcare Organizations Meet the Challenge of Healthcare Security Regulations

Contents

For more information visit us at: www.3com.com/securitynet

Acronyms and Abbreviations

3DES
Triple Data Encryption Standard

AAA
Authentication, Authorization, and Accounting

BITS
bump in the stack

BITW
bump in the wire

CA
certificate authority

CERT/CC
Computer Emergency Response Team/Coordination Center

CICS
Customer Information Control System

CPRI
Computer-based Patient Record Institute

CPU
central processing unit

DHHS
Department of Health and Human Services

DMZ
demilitarized zone

EAPOE
Extensible Authentication Protocol over Ethernet

FTP
File Transfer Protocol

HIMSS
Healthcare Information and Management Systems Society

Healthcare Information Security

How a Secure Data Network Can Help Healthcare Organizations Meet the Challenge of Healthcare Security Regulations

A 1996 United States federal law called the Health Insurance Portability and Accountability Act (HIPAA), also known as the Kennedy-Kassebaum Act, establishes regulations designed to protect health insurance benefits as well as sensitive information about the insured. HIPAA offers workers who change employment better access to health insurance coverage by limiting exclusions for preexisting conditions and restraining health plans from denying people health insurance based on their health status. But HIPAA also calls for the development and implementation of uniform national standards for the secure electronic transmission of health information.

This 3Com white paper focuses on the stringent information security policies and rules established by HIPAA. In the Internet era, comprehensive security protections in the enterprise data network must be a central part of any organization's HIPAA compliance planning. This white paper discusses network security technologies and introduces tools and solutions to help healthcare organizations implement secure, reliable, and manageable data networks that enable compliance with HIPAA requirements.

HIPAA: Protecting the Security of Confidential Data

HIPAA imposes regulations on the Department of Health and Human Services (DHHS), other federal agencies, state Medicaid agencies, private health plans, healthcare providers, and healthcare clearinghouses to assure their customers (i.e., patients, the insured, providers, and healthcare plans) of the confidentiality and privacy of healthcare information that is electronically collected, maintained, used, or transmitted.

Confidentiality of information is generally threatened by the risk of unauthorized access to stored information as well as the risk of interception while such data is in transit. The threats to confidential data kept in electronic format are no less serious than those to paper-based records. In fact, the ever-growing usage of the Internet introduces new challenges and security exposures for electronic data.

Methods are available today to ensure the protection of health information stored and transmitted in electronic format. But electronic storage and transmission of data requires organizations to adjust their information security policies—and in some cases to establish such policies for the first time. Ensuring an appropriate and consistent level of information security for computer-based patient records, both within individual healthcare organizations and throughout the entire healthcare delivery system, also requires consistent and compatible security policies among different organizations.

Since an organization's communications network becomes the principal medium for electronic delivery of healthcare information, optimal network design for secure delivery of information becomes a crucial task for healthcare providers. This paper focuses on network design and network security issues to help healthcare organizations meet HIPAA standards.

Threats to Enterprise Security

A computer networking system can be attacked in a number of ways, resulting in differing degrees of damage. These attacks can take several forms:

- Denial of service. The attacker disrupts the smooth flow of information by crashing or overloading a critical device such as a server, router, or firewall. This is an attack on the availability of information.
- Theft of information. The attacker acquires information that is proprietary to the organization. This can be achieved by eavesdropping, by masquerading as an authorized entity, or simply by a brute-force attack such as the use of a computer program that guesses passwords. This is an attack on the ownership of information and intellectual property.
- Corruption of data. The attacker either destroys or corrupts data stored on disk or

The *CPRI Toolkit*: Guidelines for Healthcare Information Security

Recognizing the importance of information security in managing computer-based patient records, the Computer-based Patient Record Institute (CPRI) chartered the Work Group on Confidentiality, Privacy, and Security in 1993. The Work Group has developed and published a series of topical guidelines on improving information security. These guidelines are now available as the *CPRI Toolkit*.

The *CPRI Toolkit* addresses individual issues in information security and promotes a comprehensive organizational process. It outlines general principles and provides "best practice" examples of how healthcare providers should manage the security of their paper and electronic records.

The sections of the *CPRI Toolkit* identify key activities that healthcare providers should initiate as part of managing information security, including:

- Monitoring and adjusting to changing laws, regulations, and standards
- Developing, implementing, and continuously updating data security policies, procedures, and practices
- Enhancing patient understanding of the organization's information security efforts
- Institutionalizing responsibility for information security

Each section of the *CPRI Toolkit* includes a copy of the latest edition of the pertinent CPRI guideline, several case studies with sample policies, procedures, and forms, and extensive references to sources of additional information. The *CPRI Toolkit* also contains summaries of the proposed DHHS rules, the DHHS model for medical privacy provisions, a summary of federal legislation on medical privacy, information about tracking state laws on medical privacy, and a thorough explanation of the standards-setting process in medical informatics. This document can help healthcare providers plan, implement, and evaluate a security surveillance process scaled to their organizational needs.

As part of its ongoing commitment to meeting the network infrastructure needs of the healthcare industry, 3Com Corporation (http://www.3com.com) is partnering with CPRI to publish and distribute the *CPRI Toolkit* in electronic format. Today, by partnering with 3Com, customers can use the wealth of information in the *CPRI Toolkit* to help ensure HIPAA compliance of their systems.

corrupts data as it is transmitted across the network. This is an attack on the integrity of information.

Threats to the availability, ownership, and integrity of information assets can arise at any of the following locations (Figure 1 on page 4):

- The people who use the system (divulging passwords, losing token cards, etc.)
- Internal network connections such as routers and switches
- Interconnection points such as gateways between corporate intranets and the Internet
- Third-party network carriers such as long-distance carriers and Internet service providers (ISPs)
- Application-level imposters, eavesdroppers, and attackers

In a 1999 survey by the Healthcare Information and Management Systems Society (HIMSS) (http://www.himss.org/survey/), senior executives and managers from healthcare organizations were asked about their top security concerns (Table 1 on page 4). As the table shows, 31 percent of the HIMSS survey respondents said that the threat from within is their number-one security concern. In fact, the FBI Computer Crime Unit reports that more than 80 percent of all network security breaches are inside jobs by disgruntled or dishonest employees.

Based on the HIMSS survey, 18 percent of U.S. healthcare organizations have already implemented security policies and procedures to address HIPAA security requirement

Acronyms and Abbreviations

HIPAA
Health Insurance Portability and Accountability Act

HTML
Hypertext Markup Language

HTTP
Hypertext Transfer Protocol

IETF
Internet Engineering Task Force

IPSec
Internet Protocol Security

ISP
Internet service provider

LAN
local area network

NAT
Network Address Translation

NCSA
National Computer Security Association

NDS
Novell Directory Services

NIC
network interface card

NSP
network service provider

PKI
public key infrastructure

POP
Post Office Protocol

PPP
Point-to-Point Protocol

S/MIME
Secure/Multipurpose Internet Mail Extensions

Acronyms and Abbreviations

SA
security association

SLIP
Serial Line Internet Protocol

SNA
Systems Network Architecture

SPD
security policy database

TCP/IP
Transmission Control Protocol/Internet Protocol

TI
tunnel initiator

TS
tunnel switch

TT
tunnel terminator

VLAN
virtual local area network

VPN
virtual private network

VTAM
Virtual Telecommunication Access Method

WAN
wide area network

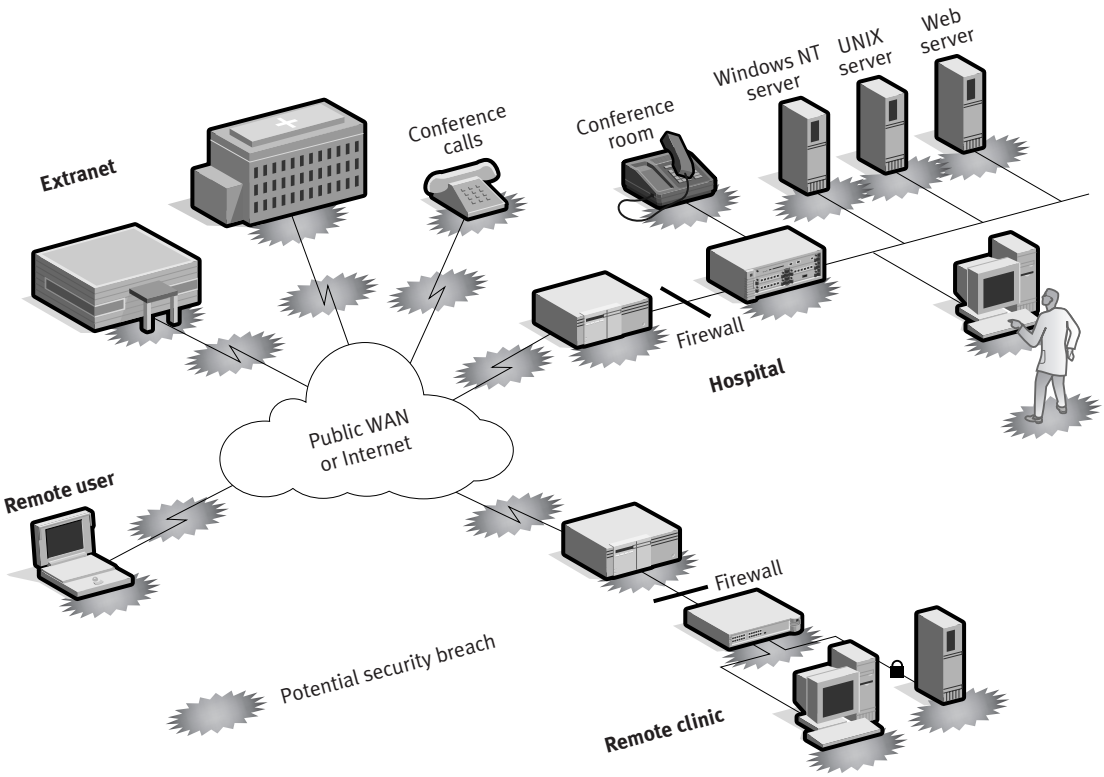


Figure 1. *Potential Security Breaches*

compliance. Table 2 shows the reported progress toward compliance. Clearly, there is still a long way to go to bring the majority of healthcare organizations into compliance with the new regulations.

Elements of a Comprehensive Security Solution

A complete security solution that maximizes the benefits of networked data communications must contain these elements:

- Physical protection: Where are you?
- User authentication: Who are you?
- Access control: What assets are you allowed to use?
- Encryption: What information should be hidden and how?
- Management: What is happening within the network?

Establishing adequate or even impenetrable security in one of these areas without addressing each of the others exposes the organization to unacceptable risks. The following sections look more closely at each element in a total security solution.

Table 1. *Security Concerns of Senior Healthcare Managers*

Security Concern	Percent of Respondents
Internal breach of security	31
The limits of existing security technology	21
External breaches of security	14
Unauthorized use of data by third parties	13
Patients' lack of confidence in the security of information	11
I am not concerned about information security	7
Don't know	3

Table 2. *Reported Progress Toward Compliance with HIPAA Security Requirements*

Progress Statement	Percent of Respondents
We haven't begun yet	13
Assessed organization compliance	24
Documented security policies and procedures	22
Implemented security policies and procedures	18
Hired a security officer	13
Don't know	10

Physical Security

Physical risks most often involve access to machines or people. A number of strategies can be used to enhance physical security:

- Place computers in a secure environment. The degree to which the console, keyboard, and monitor of a computer can be physically accessed determines to a large extent the level of system security. This is a common "back-door" opening to an intruder. To implement physical security, organizations often use receptionists, security guards, physical keys, combination or electronic door locks, and other access controls. With PCs in areas where patients often spend many minutes alone or at nursing stations where multiple users share a single workstation, this threat is even more severe.
- Destroy sensitive documents, including those stored electronically, when they are no longer used. Sophisticated tools can reconstruct files supposedly erased from a disk. Only destroying the disk itself guarantees the destruction of the data it once contained.
- Store digital keys on smart cards or fobs, not on disks. Disks can be duplicated; smart cards or fobs are more difficult to copy.
- Keep passwords secure. Avoid writing passwords down, then sending them through electronic mail or placing them in messages that are archived or incorporated in group discussion systems.
- Do not write PINs on ID cards. Writing a PIN number on an ID card is similar to hiding the front door key under the welcome mat. Security training can help make employees aware of their part in maintaining network security.
- Lock down portable equipment. The laptop computer represents one of the greatest physical threats to a security system, because it contains a great deal of information and can easily be carried off. The same is true of other devices such as external disk drives and tape backup systems. These devices must be locked away or bolted to the desk to guard against theft.

User Authentication

Proof of identity is an essential component of any security system. It is the only way to differentiate authorized users from intruders. User authentication to the network is a necessity for any enterprise that is serious about protecting information assets and knowing who is attempting to gain access to the network. Authentication becomes particularly important when some of the more sophisticated communication methods are used.

In addition to proving identity, authentication systems are used to determine what information the requestor can access—for example, a human resources database or corporate financial database. True authentication generally incorporates two or all three of the following elements:

- What the user has or possesses (smart card, certificate)
- What the user knows (password)
- A physical attribute (fingerprint or other biometric information)

Additional information on HIPAA requirements for physical security can be found in P.3–P.6, Chapter 4.1, Sections D and E of the CPRI Toolkit *(http://www.3com.com/securitynet).*

The Evolution of Enterprise Networks

Historically, enterprise networks consisted of terminals directly attached via terminal or cluster controllers to IBM Systems Network Architecture (SNA)–based host mainframes running mission-critical applications. These physical connections were invariably made over coax or twinax cabling. In the early 1980s, PCs began appearing on the floors of corporate businesses, connected together in local area networks (LANs) over Token Ring or Ethernet media. Although network vendors developed terminal and printer emulation software for PCs to share the host resources with the LAN-based clients, true integration was limited.

Mainframe-centric SNA- and LAN-based enterprise networks evolved separately through upgrade, acquisition, and corporate mergers. The result? Different client platforms running different applications over a mix of SNA and non-SNA LAN protocols. In some networks, SNA could be supported down to the client machines in the network. In other cases, it was often not desirable or possible to deploy SNA support software on LAN-based clients. And because LAN and SNA networks were designed, developed, and maintained separately, when departmental LANs requested access to the host data at the centrally managed data center, the interface was frequently awkward and actual data extraction extremely cumbersome.

In most cases, SNA and LAN networks still exist side by side (Figure 2). Such a network strategy may be safe, but it is costly. Maintaining parallel networks for different protocols can, at the extreme, cost twice as much as a single network for several reasons:

- **Increased administrative burden.** Connecting PCs to host systems incurs a significant administration burden. Each PC must have a corresponding VTAMLST definition on VTAM hosts, so a host change can affect hundreds of client configurations.
- **Increased network downtime.** Host configuration changes translate to increased downtime.
- **Decreased performance.** Directly connecting PCs degrades overall system performance because of the increased processing

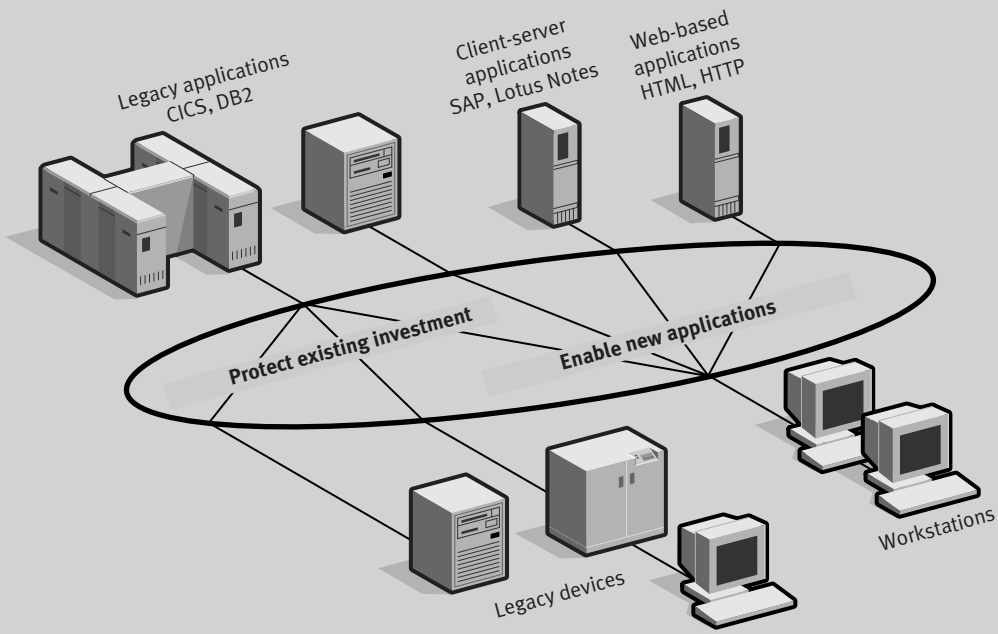


Figure 2. *Legacy and Multiprotocol Networks Coexist in Today's Enterprises*

overhead on the host CPU as well as increased traffic on the SNA backbone.

Because of the ever-growing variety of PC-based applications and productivity tools in the enterprise network, there is an expanding need to integrate not only PC- and host-based applications, but also the data residing on these platforms. New business applications are requiring advanced functionality such as integration of multimedia data from multiple hosts, servers, and workstations into a single screen view; or integration of server- and workstation-based files, databases, security systems, and transactions. In addition, Transmission Control Protocol/Internet Protocol (TCP/IP) Web applications have spurred the development of Web browser–based presentation techniques. This new phenomenon radically changes the way information is accessed and presented in traditional mainframe-based environments.

Sound security policies and functionality have been characteristic of the centralized, SNA mainframe-based enterprise networks. However, LAN-based networks have traditionally been less concerned with security. As a result, the emerging networking paradigm, which combines mainframe and LAN-based intranets and connects them to the Internet and extranet, usually requires a major overhaul of security strategies and processes.

The key to successful multiprotocol integration lies in evaluating and selecting among the implementation alternatives to find a mix that best suits an organization's business needs. Selection of a credible and trustworthy network consulting partner can substantially expedite, simplify, and improve the process of network design and implementation.

Authentication is most often achieved through challenge and response, digital certificates, or message digests and digital signatures.

Challenge and Response. In this authentication method, a software agent within a database system or a workgroup server presents the person requesting access to a resource with a challenge, most often requesting a username and password. This is the most common form of security and one that is easily broken when passwords are not carefully chosen and maintained.

Digital Certificates. One of the earliest uses of digital certificate technology was Privacy Enhanced Mail, the predecessor to Secure/Multipurpose Internet Mail Extensions (S/MIME), a widely used specification that brought a higher level of security to e-mail through encryption and digital signature-based authentication. Since their introduction, the use of digital certificates has continued to grow steadily.

Digital certificates are essential components of a public key infrastructure (PKI), which can be generally defined as a security system that consists of protocols, services, and standards that support applications of public key cryptography. Public key cryptography is used to validate messages that have been digitally signed and to decrypt messages encrypted with a private key. Such messages can be simple e-mail or part of a protocol for establishing a secure communications session.

To be authenticated, the sender of the message digitally signs the message using a private key. The signature can be validated using the sender's corresponding public key, which is contained in the sender's certificate and can either be sent along with the message or retrieved from a certificate repository.

The association between the sender's identity and the sender's public key can be authenticated through a digital certificate issued by a trusted certificate authority (CA). The CA certificate is issued in advance to all parties, and its public key can be used to authenticate the public key in the sender's certificate. When the sender's public key has been validated, it can be used to authenticate the digital signature of the message itself. Since

Additional information on HIPAA requirements for user authentication can be found in S5.1–S5.7, Chapter 4.1, Sections D and E of the CPRI Toolkit *(http://www.3com.com/securitynet).*

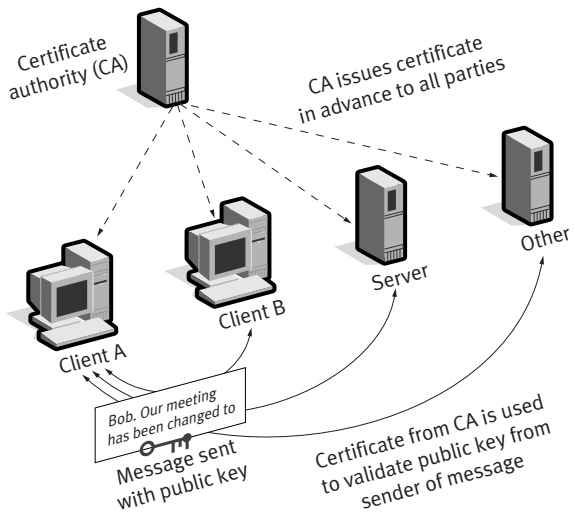


Figure 3. *Deploying Digital Certificates*

the CA certificate is already available to both the sender and receiver, this method can be used to authenticate messages in either direction without contacting a third party.

To implement a secure certificate or signature system (Figure 3), the following conditions must be met:

- A certificate authority service provider or software package must issue a certificate to all potential senders and receivers.
- The receiver must be able to use the CA certificate to verify the sender's public key.
- The sender's authenticated public key must then be used to verify the digital signature of the message itself.

Although a digital certificate system can affect the performance of heavily used servers, this is usually not the case. Typically, the client provides the certificate, in which case the authenticator does not need to perform any server access. Moreover, the value of preventing a security breach often far outweighs the inconvenience of slightly delayed access.

Message Digests and Digital Signatures. Applying a one-way hash function such as MD5 or SHA-1 to a message creates message digests. "One-way" means that the original message cannot be recreated from the digest. A digital signature uses the private key of an individual to encrypt the message digest (Figure 4). At the receiving end, the digest is recreated from the message text, the public key is used to decrypt the digest from the digital signature, and the two message digests are compared. If they match, the messages are in all probability the same. Comparison of the message digests provides both a means of authenticating the signature and a check of message integrity.

Additional information on HIPAA requirements for access control can be found in Chapter 4.1, Sections D and E of the CPRI Toolkit *(http://www.3com.com/securitynet).*

Access Control

Access control governs a user's ability to make a connection to a particular network, computer, or application, or to a specific kind of data traffic. The increasing use of the Internet is heightening the concerns of network administrators about the security of their network infrastructure and their organization's private data. And in light of HIPAA security regulations, these concerns are becoming even more critical for healthcare providers.

The first step in establishing secure network access is to define a security policy. The National Computer Security Association (NCSA), for example, recommends starting with the most secure policy: denying all services to anyone, except for what is explicitly permitted. Many policies can be enforced through the use of technology.

Access from external systems is generally implemented using network firewalls. A fire-

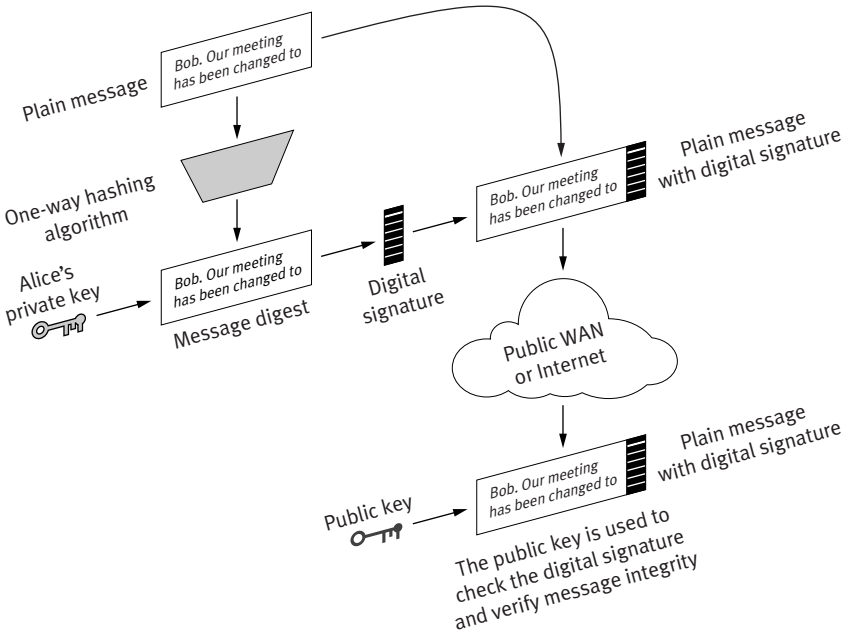


Figure 4. *Authentication with Digital Signature*

wall is a group of systems or a mechanism that enforces a security policy to protect an internal (trusted) network from an external (untrusted) one. The firewall determines which inside services can be accessed from the outside, which outsiders are permitted access to the permitted inside services, and which outside services can be accessed by insiders.

For a firewall to be effective, all traffic to and from the Internet must pass through the firewall, where it can be inspected (Figure 5). The firewall must permit only authorized traffic to pass, and the firewall itself must be immune to penetration. A firewall system cannot offer any protection once an attacker has gotten through or around the firewall.

A firewall consists of several components, including filters or screens that block transmission of certain classes of traffic. Some of the well-known methods of attack that can be prevented by firewalls include IP address "spoofing," IP source-routed attack, "tiny fragment" attacks, IP tunnel attacks, and certain types of denial-of-service attacks. For detailed information about firewall design, refer to the 3Com white paper "Internet Firewalls and Security: A Technology Overview"

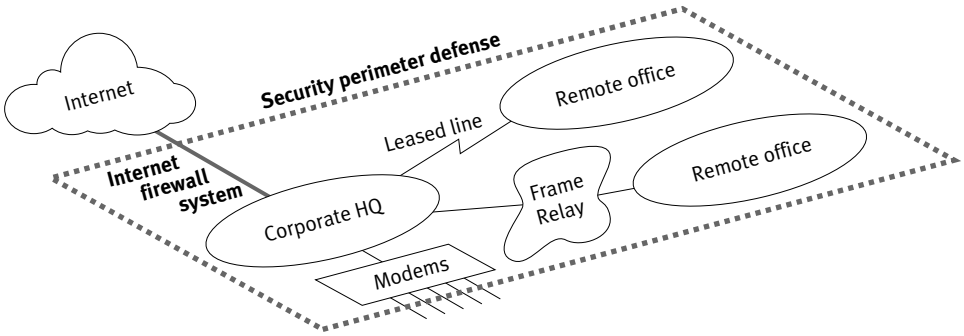


Figure 5. *Security Policy Creates a Perimeter Defense*

Security in the Internet Age

What is so special about Internet security? And why are Internet security concerns so much greater than those for public circuit switched, packet switched, or Frame Relay networks?

One of the key differences is that no single body is responsible for the Internet. If, for example, a company were using a certain carrier for public Frame Relay service, this carrier would have contractual obligations to deliver reliable and secure services. With the Internet, such an approach would not be applicable. Although virtual private network (VPN) offerings are an interesting recent development in this area, there is still a long way to go.

Another major issue is the ever-growing number of sophisticated users who are "surfing" the net, sometimes with a clear intention to break into someone's network, either as a "hobby" or for industrial espionage.

For up-to-date information concerning attacks on Internet sites, contact the Computer Emergency Response Team/Coordination Center (CERT/CC) (http://www.cert.org). CERT publishes warnings and summaries to draw attention to the various types of attacks that have been reported to their incident response staff. These reports also contain information and solutions for defeating each type of attack. New or updated files are available for anonymous FTP downloads from ftp://info.cert.org, and past summaries are available from ftp://info.cert.org/pub/cert_summaries.

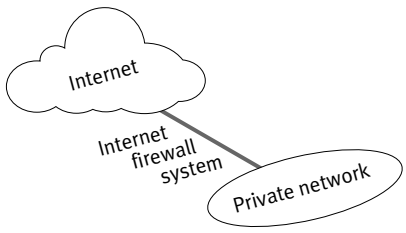
For more information concerning the techniques employed by hackers, see http://www.attrition/org and track the following USENET newsgroups:

comp.security.announce
comp.security.mis
comp.security.uni
alt.2600
alt.wired
alt.hackers
alt.security

(http://www.3com.com/technology/tech_net/white_papers/500619s.html).

An Internet firewall offers a number of security benefits to the organization (Figure 6). It provides a centralized "choke point" to help keep unauthorized users out of the protected network. It generates security alarms and provides a centralized location for monitoring and logging Internet usage. An Internet firewall is a logical place to deploy Network Address Translation (NAT), which can help alleviate the Internet address space shortage and eliminate the need to modify IP addressing when an organization changes Internet service providers. The Internet firewall is also the ideal location for deploying World Wide Web and FTP servers for information delivery to those outside the organization.

An Internet firewall cannot protect against attacks that do not go through the firewall. For example, if unrestricted dial-out is permitted from inside the protected network,



- Concentrates network security
- Serves as centralized access "choke point"
- Generates security alarms
- Monitors and logs Internet usage
- Good location for Network Address Translation (NAT)
- Good location for WWW and FTP servers

Figure 6. *Benefits of an Internet Firewall*

internal users can make a direct Serial Line Internet Protocol (SLIP) or Point-to-Point Protocol (PPP) connection to the Internet. These types of connections bypass the firewall and create a significant potential for back-door attacks. Firewalls also do not protect against attacks where a hacker, pretending to be a supervisor or a befuddled new employee, persuades a less sophisticated user to reveal a password or grant them "temporary" network access. Internet firewalls cannot protect against the transfer of virus-infected software or files. Organizations should deploy anti-viral software at each desktop to protect against such infection.

Finally, Internet firewalls cannot protect against data-driven attacks. A data-driven attack occurs when seemingly harmless data is mailed or copied to an internal host and is executed to launch an attack. For example, a data-driven attack could cause a host to modify security-related files, making it easier for an intruder to gain access to the system. For improved protection, network security should involve application gateways on specially created subnets with secure "bastion" hosts for proxy sessions with outside networks. Proxy sessions let the gateway server pass all requests to the WAN, while keeping the internal networks isolated.

It is important to note that an Internet firewall must be part of an overall security policy that creates a perimeter defense designed to protect the information resources of the organization. This security policy must include: (1) published security guidelines to inform users of their responsibilities; (2) corporate policies defining network access, service access, local and remote user authentication, dial-in and dial-out, disk and data encryption, and virus protection measures; and (3) employee training. All potential points of network attack must be protected with the same level of network security. Setting up an Internet firewall without a comprehensive security policy in place is like placing a steel door on a tent.

Encryption

Even if both authentication and access control security systems are completely effective, the enterprise can still be at risk when data communications travel over a third-party network such as the Internet. Indeed, the low cost and ease of connecting to the Internet have made it an extremely attractive medium for communication within and between enterprises.

Encryption is used to protect against eavesdropping. It renders information private by making it unreadable to all except those who have the key needed to decrypt the data. It does not matter whether a third party intercepts packets sent over the Internet; the data still cannot be read. This approach can be used throughout the enterprise network, including within the enterprise (intranet), between enterprises (extranet), or over the public Internet to carry private data in a VPN.

The degree of protection afforded by encryption depends upon the strength of the encryption algorithm. Against brute-force attacks, that strength is determined by the number of possible keys, which in turn is defined by the key size, as shown in Table 3.

A recent brute-force attack was able to try 245 billion keys per second. With this type of computing power, an intruder could try all possible 56-bit keys in 81 hours, finding the key in an average of 40 hours. However, with 112-bit keys and the ability to try 245 billion keys per second, it would take an average of 336 trillion years to discover the key. A Triple Data Encryption Standard (3DES) system uses either 112-bit or 168-bit keys.

Table 3. *Number of Possible Encryption Keys Is a Function of Key Size*

Key Size	Number of Keys
32 bits = 2^{32}	$4.3 \cdot 10^{9}$
56 bits = 2^{56}	$7.2 \cdot 10^{16}$
112 bits = 2^{112}	$5.2 \cdot 10^{33}$
128 bits = 2^{128}	$3.4 \cdot 10^{38}$
168 bits = 2^{168}	$3.7 \cdot 10^{50}$

HIPAA encryption-related requirements can be found in S1.2 Chapter 3.5 and 4.1 of the CPRI Toolkit *(http://www.3com.com/securitynet).*

Encryption systems in common use today include the following:

- Shared key encryption. Both or all parties possess a previously distributed key that locks and unlocks the data. The sender provides the key to a shared symmetrical encryption algorithm to encode the data before placing it in a packet bound for the remote site; the remote site then provides the key to the same encryption algorithm to decode the data.
- Public key encryption. One party possesses a private unlocking key and makes a public locking key. Any sender can use the public key to encrypt the communication; the receiver then uses its corresponding private key to decrypt the data.
- Secure key exchange. Both parties first authenticate themselves (often using digital certificates) during a session-specific encryption key distribution process. The session key is created based on data generated by both parties at the time of communication. This key can then be used to encrypt and decrypt all other communications.

All encryption systems place an additional load on the network because one or more round trips are needed to authenticate the parties. The machines involved in the communication must also perform large mathematical operations to encrypt and decrypt data, and this can amount to a noticeable increase of CPU cycles on systems that pass many packets. To free the CPU from this task, the conventional burden of encryption systems can be moved to firmware or hardware, such as a coprocessor on the network interface card (NIC) or elsewhere in an embedded system.

Additional information on HIPAA requirements for security management can be found in A10.1–10.4, Chapter 4.1, Sections C, D, and E of the CPRI Toolkit *(http://www.3com.com/securitynet).*

Security Management

A security system should allow for oversight and control by a human authority. Any system that uses authentication requires some central authority to verify those identities, whether it be the /etc/password file on a UNIX host, a Windows NT domain controller, or a Novell Directory Services (NDS) server. The ability to see histories, such as repeated failed attempts to breach a firewall, can provide invaluable information to those charged with protecting information assets.

Some of the more recent security specifications, such as Internet Protocol Security (IPSec), require the presence of a database containing policy rules. All these elements must be managed for the system to work correctly. However, management consoles or functions themselves represent another potential point of failure of a security system. It is therefore important to ensure that these systems are physically secured and that authentication is in place for any logon to a management console.

New policy-powered networking or directory-enabled networking technologies are simplifying security management methodologies and enabling automation for access control, authorization, scope of control, span of commands, and privacy of content. Security information can be strategically placed into the policy-powered networking directories, giving network and security managers powerful new tools to monitor and enforce network security and information privacy.

Internet Protocol Security. To promote security for business communications, the Internet Engineering Task Force (IETF) developed IPSec. IPSec offers a complete and integrated system for securing data networks. IPSec can be used within the organization or on the Internet because it is based on a set of open specifications, including the entire TCP/IP protocol suite. Also, like TCP/IP (and unlike proprietary schemes), IPSec is designed for interoperability between enterprise systems.

In an IPSec communication, the two communicating entities (which can be individual hosts or intervening devices such as routers or firewalls) first establish a security association (SA). During negotiation of the SA, the two entities agree on what kind of security will be employed.

A security policy database (SPD) keeps track of the kinds of security, encryption, and authentication that a particular enterprise can implement, and also keeps track of the active security associations. This makes it possible to monitor IPSec activity across the network, and

to manage the security systems employed at any given site.

Network system designers can integrate IPSec into an existing system in three ways:

- By integrating IPSec processing into the TCP/IP network stack of the host or other device. This requires the host CPU to do security processing.
- By performing IPSec processing in software before the data packets are processed by the existing TCP/IP networking stack (known as a bump in the stack, or BITS). This approach also requires the host CPU to do security processing.
- By performing IPSec processing before the data packets are processed by the host computer (known as bump in the wire, or BITW). This system offloads security processing to a processor on a network component, such as a NIC with an on-board encryption chip, and leaves the CPU free.

The use of an additional processor (or BITW) to handle IPSec security tasks promises the greatest throughput while still delivering the full benefit of a comprehensive security system.

Securing End-to-End Data Access

It is hard to overstate the importance of the end-to-end aspect of network security. Security starts with well-defined and -enforced security policies implemented by efficient and robust encryption on NICs, authentication and authorization in the LAN switches, and robust and flexible firewall and security management instrumentation.

3Com can offer best-of-breed security technologies for each component in the end-to-end networking paradigm. And since it is both important and rational to control security at the edges of the network, the IEEE P802.1x/D1 working group is currently developing an important technology for policing LAN security on devices at the network edge, called Extensible Authentication Protocol over Ethernet (EAPOE). EAPOE technology is based on the *Network Login* technology pioneered by 3Com.

VPNs and Tunnel Switching

A VPN is a secure connection that offers the privacy and management controls of a dedicated, point-to-point link but actually occurs over a shared, routed network such as the Internet. VPNs are created using encryption, authentication, and tunneling—a method by which data packets in one protocol are encapsulated within another protocol. Tunneling enables traffic from multiple enterprises to travel across the same network unaware of each other, as if enclosed in their own private pipes (Figure 7).

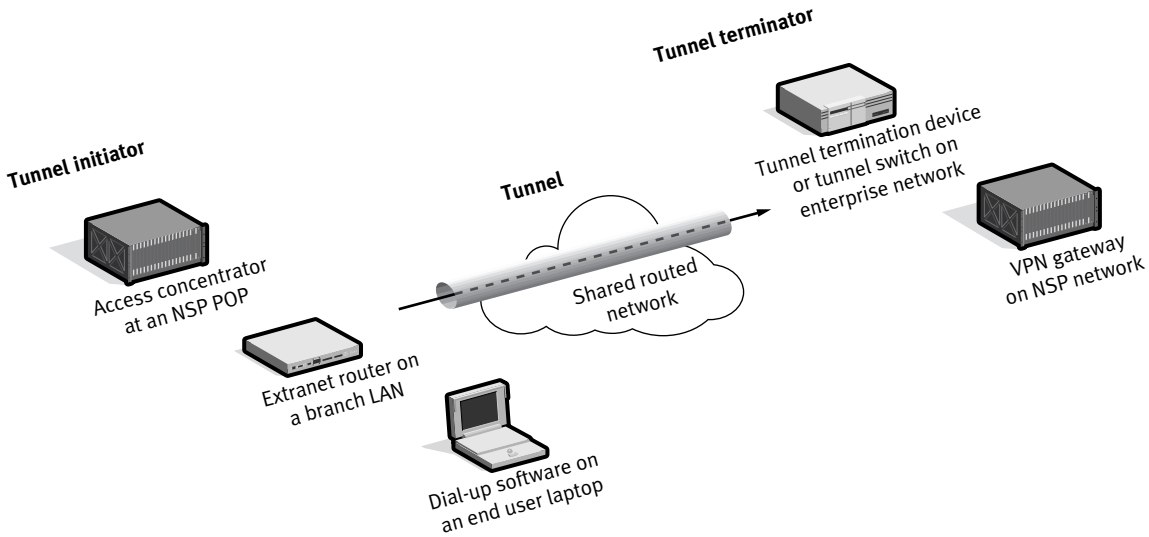


Figure 7. *Typical VPN Tunneling Without Tunnel Switching*

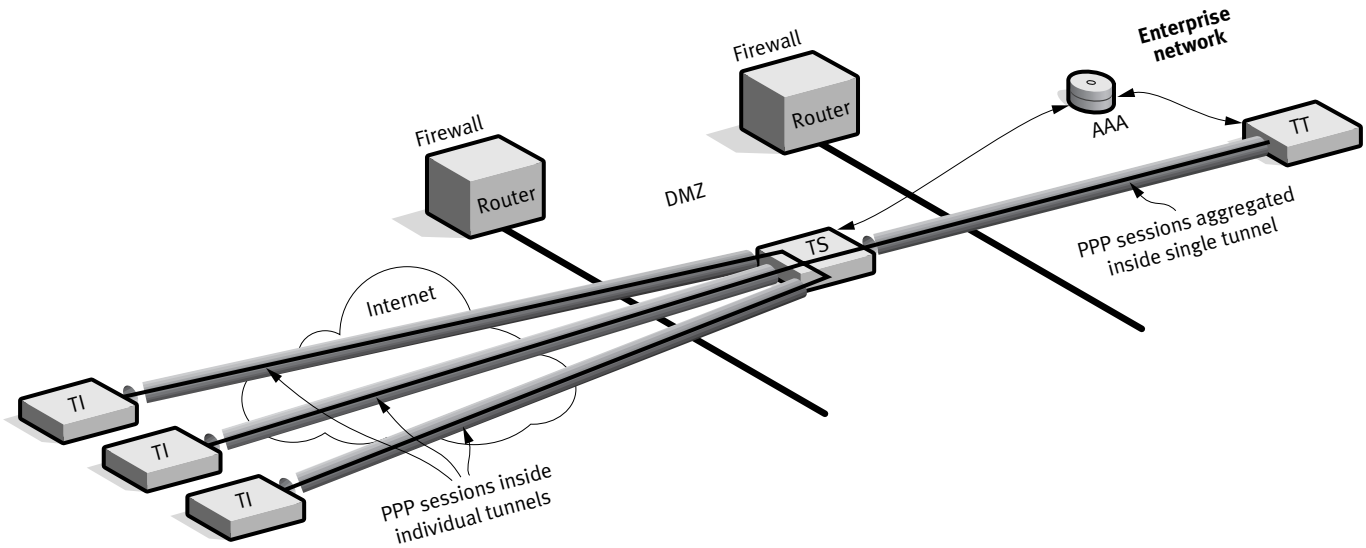


Figure 8. *Tunnel Switching Extends the Original Tunnel to a New Destination*

Tunnel switching is a 3Com technology that increases the security, manageability, performance, and scalability of VPNs. It allows organizations to bring multiple VPNs into the network through a single edge device, efficiently aggregate them for internal delivery, and flexibly locate their end points anywhere in the enterprise.

While VPN tunnels are generally terminated at the enterprise network edge, tunnel switching allows them to be extended safely across firewalls to specific tunnel termination points within LAN administrative domains (Figure 8). In this way, all tunneled traffic can be addressed to the tunnel switch, with its single, publicly known address, while actually being terminated at any number of internal destinations, whose addresses and security measures are hidden from the Internet.

Tunnel switching increases security by moving primary security controls inside the network and adding a second layer of security at the edge. Instead of terminating the tunnel outside the firewall or in a "demilitarized zone" (DMZ) between two firewalls, then transmitting packets over an unsecured link to an internal server, enterprises can maintain packets in their secure tunnels through the firewall to the other side. This approach allows multiple protocols and applications to be supported while opening only a "pinhole" in the firewall for the tunneling protocol.

In addition, while the tunnel switch performs preliminary authentication on incoming tunnels, it need not be aware of encryption keys, digital signatures, and other security measures employed by tunnel terminators. As a result, the amount of security information stored at the network edge, requiring protection against potential threats from the Internet, is minimized. Nor does the tunnel switch participate in the Point-to-Point Protocol sessions between the source and ultimate destination host; in the event that the tunnel switch is compromised, the PPP session is not.

Organizations can determine the level of security that will be applied to various types of tunneled traffic. Tunnel switches can direct employee traffic, for example, to one tunnel terminator, while traffic from consultants and suppliers is directed to another terminator that enforces stricter security. Government organizations and universities often use tunnel switching to allow internal agencies or departments to implement their own security policies, while still providing a single address for tunnels coming in from the outside world.

Other advantages of tunnel switching include improved VPN manageability. Enterprises can change the location of tunnel termi-

nators, addressing schemes, or indeed the entire network topology behind the firewall without having to notify all tunnel initiators (which could comprise tens of thousands of remote users). Tunnel switching also facilitates VPN access to legacy applications and allows VPN users to be members of virtual local area networks (VLANs), simplifying user moves and changes.

For more information about tunnel switching technology, refer to the 3Com white paper "Tunnel Switching: 3Com Technology Boosts VPN Security and Reliability," (http://www.3com.com/technology/tech_net/white_papers/503049.html).

Conclusion

The HIPAA legislation confronts many healthcare providers with the need to review and upgrade security policies and procedures. Although this is not an easy task, 3Com offers product solutions and consulting services to help ensure that an organization's data network infrastructure provides the security, reliability, and manageability to support compliance with the regulations.

The *CPRI Toolkit* provides models and methods for assisting healthcare providers in managing patient records as a broad institutional process, including the technical protection of the information system. In addition to

For More Information About Internet Security

Reference information on security technology and specific offerings can be obtained at:

- **Enhancing Enterprise Security** http://www.3com.com/technology/tech_net/white_papers/503023.html
- **Private Use of Public Networks for Enterprise Customers** http://www.3com.com/technology/tech_net/white_papers/500651.html
- **Private Use of Public Networks for Service Providers** http://www.3com.com/technology/tech_net/white_papers/500649.html
- **Tunnel Switching: 3Com Technology Boosts VPN Security and Flexibility** http://www.3com.com/technology/tech_net/white_papers/503049.html
- **Securing Information Access in Today's Networks** http://www.esj.com/fullarticle.asp?ID=3159944456pm
- **Security on the Net** http://pubs.comsoc.org/ci1/public/1997/mar/internet_column.html
- **Internet Firewalls and Security** http://www.3com.com/technology/tech_net/white_papers/500619s.html
- **A Security Architecture for the Internet** http://www.3com.com/technology/research/presentations/sectut4/index.html
- **Securing an Internet Connection** http://pubs.comsoc.org/ci1/public/1997/nov/internet_column.html
- **Cypherpunks Home Page** ftp://ftp.csua.berkeley.edu/pub/cypherpunks/Home.html
- **Computer Incident Advisory Capability** http://ciac.llnl.gov
- **COAST Homepage** http://www.cs.purdue.edu/coast
- ftp://info.cert.org
- http://www.cert.org

these technical methods, however, healthcare providers should institutionalize a sense of responsibility for maintaining patient confidentiality at all levels, including individual staff, program managers, and organizational administrators.

Designing and maintaining a secure, HIPAA-compliant network is not a trivial task. Fortunately, sophisticated tools and comprehensive service offerings are available and are continuously being improved. These tools and services can help with the process of designing secure, reliable networks, as well as with re-engineering existing networks to meet today's new security challenges. The products, technologies, and practices available today can provide flexible security solutions for a range of Internet, intranet, and extranet applications.

The best way to remain consistently informed about the integrity and reliability of your network's security is through regular security audits. To ensure a successful and reliable security implementation, it is important to partner with a competent network consulting organization for both the initial design and deployment of a secure networking infrastructure as well as for ongoing evaluation of security methodologies and HIPAA compliance. 3Com's Consulting Services are available to help customers and partners identify, design, implement, and manage cost-effective, best-of-breed networking security solutions.

Regardless of what some vendors may claim, no technology or technique can guarantee 100 percent security for the network or data resources. But a sound, up-to-date, and continuously reviewed and improved security policy can help ensure regulatory compliance and can make it very expensive, perhaps even cost-prohibitive, for anyone to compromise network security. ◘

About 3Com Corporation

With more than 300 million customers worldwide, 3Com Corporation connects more people in more ways to information than any other networking company. 3Com delivers innovative information access products and network system solutions to large, medium, and small enterprises; carriers and network service providers; PC OEMs; and consumers. 3Com. More connected.™

3Com Corporation
5400 Bayfront Plaza
P.O. Box 58145
Santa Clara, CA
95052-8145
Phone: 1 800 NET 3Com
or 1 408 326 5000
Fax: 1 408 326 5001
World Wide Web:
www.3com.com

3Com Americas International
U.S. Headquarters (serving Canada and Latin America)
Phone: 1 408 326 6328/1 408 326 6075
Fax: 1 408 326 5730/
1 408 326 8914
Miami
Phone: 1 305 461 8400
Fax: 1 305 461 8401/02

3Com Canada
Burlington
Phone: 905 336 8168
Fax: 905 336 7380
Calgary
Phone: 403 265 3266
Fax: 403 265 3268
Edmonton
Phone: 780 423 3266
Fax: 780 423 2368
Montreal
Phone: 514 683 3266
Fax: 514 683 5122
Ottawa
Phone: 613 566 7055
Fax: 613 233 9527
Toronto
Phone: 416 498 3266
Fax: 416 498 1262
Vancouver
Phone: 604 434 3266
Fax: 604 434 3264

3Com Latin America
Argentina (serving Argentina, Paraguay, and Uruguay)
Phone: 54 11 4510 3200
Fax: 54 11 4314 3329
Brazil
Phone: 55 11 5641 5001
Fax: 55 11 5641 3444
Chile (serving Bolivia, Chile, and Peru)
Phone: 562 240 6200
Fax: 562 240 6231
Colombia
Phone: 57 1 629 4110
Fax: 57 1 629 4503
Costa Rica
Phone: 506 280 8480
Fax: 506 280 5859
Mexico
Phone: 525 201 0000
Fax: 525 201 0001
Peru
Phone: 51 1 221 5399
Fax: 51 1 221 5499
Venezuela
Phone: 582 267 5550
Fax: 582 267 3373

Asia Pacific Rim
Melbourne, Australia
Phone: 61 3 9934 8888
Fax: 61 3 9934 8880
Sydney, Australia
Phone: 61 2 9937 5000
Fax: 61 2 9956 6247
Beijing, China
Phone: 8610 6588 0568
Fax: 8610 6588 0602
Shanghai, China
Phone: 86 21 6350 1581
Fax: 86 21 6350 1531
Hong Kong
Phone: 852 2501 1111
Fax: 852 2537 1149
India
Phone: 91 11 629 3177
Fax: 91 11 623 6509
Indonesia
Phone: 62 21 572 2088
Fax: 62 21 572 2089
Osaka, Japan
Phone: 81 6 6379 1767
Fax: 81 6 6379 0871
Tokyo, Japan
Phone: 0120 31 3266
(toll free from Japan)
Phone: 81 3 5977 3266
Fax: 81 3 5977 3370
Korea
Phone: 82 2 3455 6300
Fax: 82 2 319 4710
Malaysia
Phone: 60 3 715 1333
Fax: 60 3 715 2333
New Zealand
Phone: 64 9 366 9138
Fax: 64 9 366 9139
Philippines
Phone: 632 849 3979
Fax: 632 849 3970
Singapore
Phone: 65 538 9368
Fax: 65 538 9369
Taiwan
Phone: 886 2 2 377 5850
Fax: 886 2 2 377 5860
Thailand
Phone: 662 231 8151 5
Fax: 662 231 8158

3Com Austria
Phone: 43 1 580 17 0
Fax: 43 1 580 17 20

3Com Benelux B.V.
Belgium
Phone: 32 2 711 94 00
Fax: 32 2 711 94 11
Netherlands
Phone: 31 346 58 62 11
Fax: 31 346 58 62 22

3Com Eastern Europe/CIS
Bulgaria
Phone: 359 2 962 5222
Fax: 359 2 962 4322
Czech Republic
Phone: 420 2 21845 800
Fax: 420 2 21845 811
Hungary
Phone: 36 1 250 83 41
Fax: 36 1 250 83 47
Poland
Phone: 48 22 6451351
Fax: 48 22 6451352
Russia
Phone: 7 095 258 09 40
Fax: 7 095 258 09 41
Slovak Republic
Phone: 421 7 317 850
Fax: 421 7 317 849

3Com France
Phone: 33 1 69 86 68 00
Fax: 33 1 69 07 11 54

3Com GmbH
Unterfoehring, Germany
Phone: 49 89 992200
Fax: 49 89 9577 220

3Com Iberia
Portugal
Phone: 351 1 3404505
Fax: 351 1 3404575
Spain
Phone: 34 91 509 69 00
Fax: 34 91 307 66 63

3Com Italia S.p.A.
Milan, Italy
Phone: 39 02 253011
Fax: 39 02 27304244
Rome, Italy
Phone: 39 06 5279941
Fax: 39 06 52799423

3Com Middle East
Phone: 971 4 319533
Fax: 971 4 316766

3Com Nordic AB
Denmark
Phone: 45 48 10 50 00
Fax: 45 48 10 50 50
Finland
Phone: 358 9 435 420 67
Fax: 358 9 455 51 66
Norway
Phone: 47 22 58 47 00
Fax: 47 22 58 47 01
Sweden
Phone: 46 8 587 05 600
Fax: 46 8 587 05 601

3Com Southern Africa
Phone: 27 11 700 8600
Fax: 27 11 706 0441

3Com Switzerland
Phone: 41 844 833 933
Fax: 41 844 833 934

3Com UK Ltd.
Edinburgh
Phone: 44 131 240 2900
Fax: 44 131 240 2903
Ireland
Phone: 353 1 823 5000
Fax: 353 1 823 5001
Manchester
Phone: 44 161 874 1700
Fax: 44 161 874 1737
Winnersh
Phone: 44 1189 27 8200
Fax: 44 1189 695555

To learn more about 3Com products and services, visit our Web site at www.3com.com. 3Com Corporation is publicly traded on Nasdaq under the symbol COMS.

Printed in U.S.A. on recycled paper

503069-001 11/99