White Paper

Cisco's PIX Firewall Series and Stateful Firewall Security

Overview

- Packet filter—A method or device for limiting inbound information from the Internet. A packet filter uses access control lists (ACLs) that allow it to accept or deny access based on packet types and other variables.
- Proxy server—A more recent firewall device that examines higher layers of the Open System Interconnection (OSI) model. These devices hide valuable data by requiring users to communicate with secure systems by means of a proxy. A key drawback of this device is performance.
- Stateful filtering—A secure method of analyzing data packets that places extensive information about a data packet into a table. In order for a session to be established, information about the connection must match information stored in the table.

With the spectacular growth of the Internet and online access, companies that do business on the Internet face greater security threats. How can a company prevent users who access their public Web site from accessing other highly sensitive private network resources? And what about internal employees who wish to transmit highly sensitive data from the corporate intranet to the outside world? These are only a few examples of ways in which a company's corporate security can be threatened.

For the past several years, the only protection standing between an organization's intellectual assets and the Internet was a router. Routers use packet-filtering technology and access control lists (ACLs) to restrict access to particular computers and networks. For instance, with an ACL filter, a company can restrict all File Transfer Protocol (FTP) traffic from leaving a specific network segment. This option is cost effective, because most companies already have installed routers. It also offers high performance.

For other companies, however, this security may be insufficient, because packet filters typically cannot maintain *session state*. Instead, packet filters must analyze the "acknowledgment" field in a packet to ensure session establishment, which is not foolproof. For greater security, companies must consider additional options and should augment router security with a standalone firewall.

The concept behind firewalling has been around for at least ten years. Earlier generations of firewalls use a dual-homed UNIX host and are called proxy servers. A proxy server is an application gateway or circuit-level gateway that runs on top of a general-purpose operating system such as UNIX or Windows NT. These gateways operate at the application layer of the Open System Interconnection (OSI) model, which allows them to maintain session state and support user authentication for good security. They connect a company's local network to an external network via workstations running specialized firewalling applications.

Cisco Systems

With a proxy server, users gain access to a network by going through a process that establishes session state, user authentication, and authorization policy. The proxy server offers strong security, because the session flow is retained at the application layer.

But this type of security comes at a cost in performance. First, proxy servers work at the application layer of the OSI model. Operating at this layer is process intensive and, therefore, proxy servers consume many CPU cycles. Each TCP session initiates a process on a proxy server. Therefore, 300 users will generate 300 processes, resulting in poor performance through a proxy-server firewall. Because this architecture does not scale well, companies will be unable to fully utilize high-speed Internet connectivity options.

In addition, maintaining proxy servers is expensive because of the size and "openness" of the UNIX operating system. While openness makes UNIX an ideal development platform, it makes UNIX a vulnerable foundation for a firewall. Many of the Computer Emergency Response Team (CERT) advisories pertain to UNIX. Therefore, at a minimum, the openness of UNIX requires that companies devote considerable resources and time to patch and maintain the base foundation of their UNIX-based firewalls.

Cisco's PIX Firewall Series: Strong Security, Highest Performance, and Lowest Cost of Ownership

Cisco Systems' PIX Firewall series addresses many of the security needs of companies—without the overhead and performance limitations of proxy servers. Its high performance and low cost of ownership make it a compelling solution for corporate network protection.

Strong Security: "Stateful" Information Protects Network

Cisco's PIX Firewall series ensures high security through its adaptive security algorithm (ASA) and the use of stateful information. Each time a TCP connection is established for inbound or outbound connections through the PIX Firewall, the information about the connection is logged in a stateful session flow table. The table contains the source and destination addresses, port numbers, TCP sequencing information, and additional flags for each TCP connection associated with that particular connection. This information creates a connection object in the PIX Firewall series. Thereafter, inbound and outbound packets are compared against session flows in the connection table and are permitted through the Cisco PIX Firewall only if an appropriate connection exists to validate their passage. This connection object is temporarily set up until the connection is terminated.

For security, the ASA takes the source and destination addresses and ports, TCP sequence numbers, and additional TCP flags and hashes the IP header information. The hashing acts like a fingerprint—it creates a code that uniquely identifies the client initiating the inbound or outbound connection. In order for hackers to penetrate the firewall to an end client, they would have to obtain not only the IP address, but also the port number and the TCP sequence numbers and additional IP flags. This scenario is very unlikely because Cisco's PIX Firewall series randomizes the TCP sequencing numbers for each session. Lastly, the connection object is terminated when the session is over.

In fact, only two accesses can be made through Cisco's PIX Firewall series:

- Cut-through proxy authentication
- Specific servers designated as static conduits through the PIX Firewall, allowing access to a specific server on the inside private network—and that server alone

Cisco's PIX Firewall series logs all these connections, as well as other authorized and unauthorized attempts. It also provides detailed audit trails using the standard Berkeley UNIX logging mechanism (syslog).

Cisco's PIX Firewall series also supports Simple Network Management Protocol (SNMP) traps. Users can also generate reports using the PIX Firewall series' Web-browser reporting tools including real-time alerts through e-mail and pager.

Cisco's PIX Firewall series also allows users to filter out Java applets, which could threaten corporate resources.

Lowest Cost of Ownership

Cisco's PIX Firewall series offers the lowest cost of ownership, because it can be configured quickly using an enhanced, Web-based graphical-user interface (GUI). In one portion of a window, the user sees a graphic illustration that highlights all of the Cisco Firewalls in the network. Another portion of the window lists the available configuration commands. After selecting a Cisco PIX Firewall series, the user selects the appropriate configuration function and begins configuring the PIX Firewall series.

There is no need for costly, day-to-day management because the PIX Firewall series is not based on UNIX. And because Cisco's PIX Firewall series runs on Flash memory, no hard drive is required, which greatly improves the mean time between failures (MTBF). For even higher reliability, Cisco devised a failover/hot standby upgrade option, which eliminates a single point of failure. With two PIX Firewall series running in parallel, if one malfunctions, the second PIX Firewall series transparently maintains the security operations. All these features allow maximum network uptime.

Additional cost savings accrue with the PIX Firewall series' cut-through proxy feature. Cut-through proxy reuses a company's dialin communication server's database, based on TACACS+ or Remote Authentication Dial-In User Service (RADIUS). Cisco Systems offers an enterprise authentication database/server called CiscoSecure™ access control server. This is a significant savings over proxy-based firewalls that may require companies to maintain separate databases, thereby requiring additional installation and maintenance costs.

Finally, the PIX Firewall series' transparent handling of multimedia applications (see *Security and Internet Multimedia Applications* section in this document). In order to use multimedia applications, competing firewall products require two time-consuming tasks: special configuration of the firewall, and configuration of the Web browser at each PC or workstation. For companies with hundreds or thousands of PCs, this is costly. Cisco's PIX Firewall series does not require this type of custom configuration.

Cut-Through Proxy Delivers Dramatic Performance Gains

Cisco's PIX Firewall series delivers dramatic performance advantages through an enhanced feature called cut-through proxy. Whereas UNIX-based proxy servers are able to provide user authentication and maintain "state" (information about a packet's origin and destination) to offer good security, their performance suffers because they process all packets inefficiently at the application layer of the OSI model. The PIX Firewall's cut-through proxy, on the other hand, challenges a user initially at the application layer, like a proxy server. But once the user is authenticated against an industry-standard database based on the TACACS+ or RADIUS and policy is checked, the PIX Firewall series shifts the session flow, and all traffic thereafter flows directly and quickly between the two parties while maintaining session state. This cut-through capability allows the PIX Firewall series to perform dramatically faster than proxy servers. The PIX Firewall series can be configured to authenticate both inbound and outbound connections through the firewall.

Cisco's PIX Firewall series offers the highest performance, supporting over 16,000 simultaneous TCP sessions that can support hundreds of thousands of users without impacting end-user performance. Fully loaded, the PIX Firewall series (model PIX 10000) operates at greater than 90 Mbps, supporting two T3 lines.

Greatest Network Security: A Two-Tiered Approach

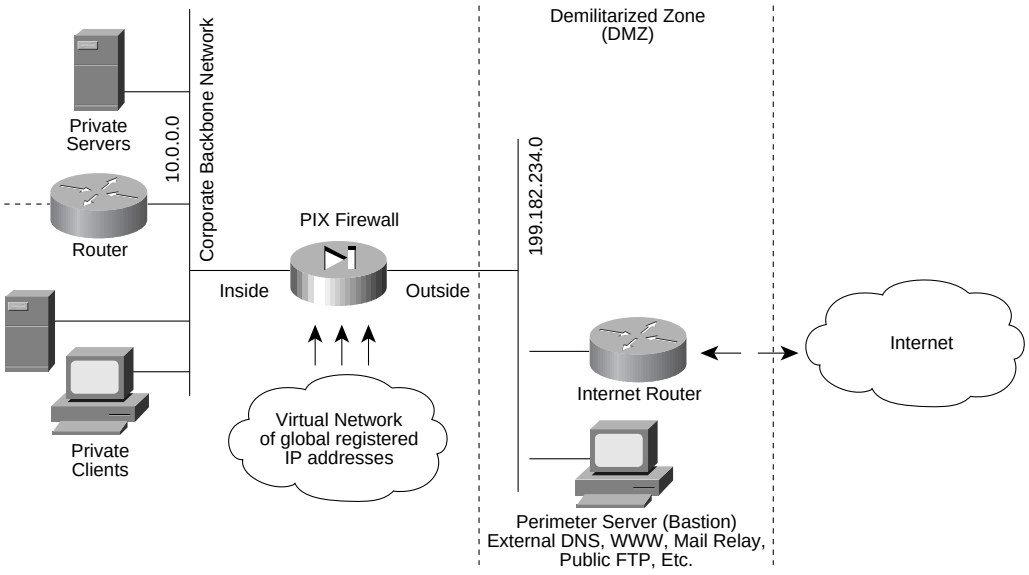
For foolproof network security, Cisco recommends a two-tiered approach (see Figure 1). Companies should locate their external servers—WWW servers, mail, public FTP, and others—behind the first tier of the diagram, which is known as the demilitarized zone (DMZ). To access this tier, users come through a router that provides initial security. Beyond this first tier is Cisco's PIX Firewall series, which represents the second-tier security perimeter. In case there is a breach of security in the DMZ, Cisco's PIX Firewall series acts as a strong security barrier to prevent outside users from gaining access to the corporate private network, where private servers, mail hubs, and private clients are located. Coupling Cisco's PIX Firewall series with Cisco routers running Cisco Internetwork Operating System (Cisco IOS™) software provides organizations with a powerful security solution. It forces hackers to penetrate multiple lines of defense.

Security and Internet Multimedia Applications

Internet multimedia applications are gaining in popularity as companies and users experience the extraordinary impact of using these applications. But handling multimedia applications represents a considerable security threat because of their extra throughput demands, which require making more ports available. To accommodate the incoming data streams, a standard packet-filtering firewall must open one or more ports. These open ports are a security concern, because they can allow outside hackers to determine the address of the internal client.

The increased data rate and data volume that characterize multimedia applications demand higher network performance, and they can strain administrative resources. Network managers need a powerful and easily managed way to deliver multimedia to users without high administration costs. Network managers must also be able to control multimedia—to shut it down when it becomes an excessive strain on network resources, and to prevent unauthorized network access via the enormous data stream of a multimedia connection.

Figure 1 Cisco PIX Firewall's Two-tiered Configuration



The PIX Firewall series offers a number of features that provide the control and security needed in an easily managed, scalable, and secure manner.

Common Multimedia Applications

Applications that are enhanced by multimedia such as audio and video, for example, include distance learning, marketing, and training applications. The impact includes:

- Catching the viewer's attention with lively and exciting material
- Retaining that attention with an easy-to-use delivery mechanism
- Improving viewer retention of concepts and ideas

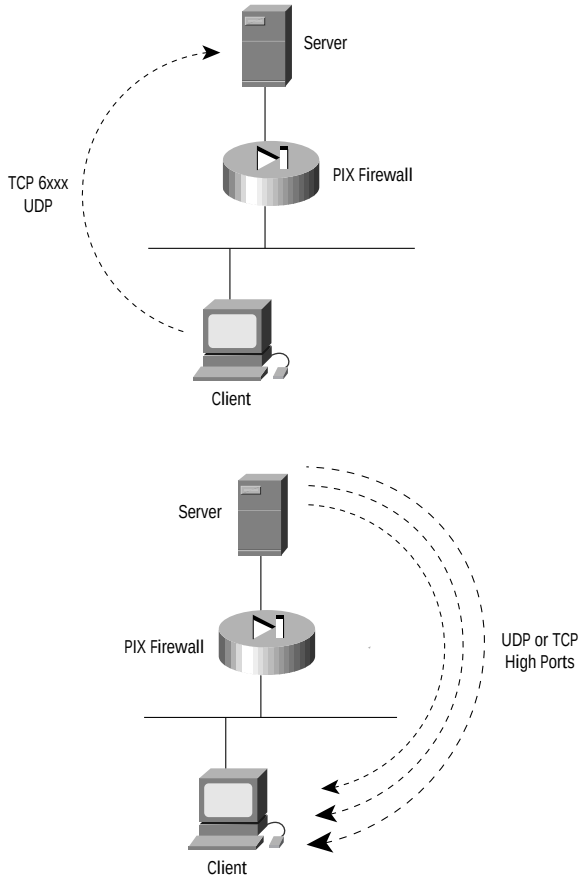
Internet multimedia comprises a broad class of applications. A representative sample follows:

- VDOnet's VDOLive allows Internet video broadcasting for such services as vacation tours, music videos, movie premiers, and corporate communications. VDOPhone allows telephony over the Internet with simultaneous two-way video and audio.
- Vocal Tec's Internet Phone enables unlimited long-distance phone conversations for the cost of an Internet connection.
- Xing Technologies' StreamWorks server acts as a live broadcast center, delivering live video and audio simultaneously to a large audience. StreamWorks server can deliver digital audio and video—live or on-demand—to intranets and the Internet.
- Progressive Networks' RealAudio is a streaming audio solution. RealAudio's IP multistream broadcast support allows transmission of an audio stream of live or on-demand audio content to many listeners simultaneously. IP multistream broadcast allows a large number of listeners to share a single stream for a large broadcast.
- White Pines Software's CU-SeeMe is desktop videoconferencing software for real-time person-to-person or group conferencing. CU-SeeMe allows live Internet conferences, broadcasts, or chats.
- Microsoft's NetShow provides live multicasting of audio and on-demand streaming of stored audio, illustrated audio (audio synchronized with images), and video.
- Cisco's PIX Firewall is fully compliant with the H.323 videoconferencing standard and allows users to conduct audio/video conferences from their desktop PC with any other H.323-compliant products such as Intel's Internet Phone or Microsoft's NetMeeting V.2.0.

Internet Connection Strategies for Multimedia

Multimedia applications communicate using the following general principles. The requester client on the inside connects (through the firewall) to the outside server using a straight TCP or User Datagram Protocol (UDP) connection. The server replies to the connection in the normal manner. So far, this follows the pattern of normal TCP or UDP communications, and the firewall handles this connection normally. This connection acts as the security connection. As long as this connection is maintained with that particular outside server, the firewall allows the multimedia session to proceed. Multimedia applications then, for throughput efficiency, send data to the original host using one or more *different* TCP or UDP streams (the "data" connection). This data stream presents a challenge to packet-filtering firewalls.

Figure 2 An Example of Multimedia Connections



Security Challenges for Multimedia

In order to accommodate the incoming TCP or UDP streams, a standard packet filtering firewall must open one or more "high" ports (TCP or UDP ports higher than 1023) for the incoming connections. This is a security issue because a high port might be open for internal network use (for example, by a database server or other service). In this situation, outside hackers can probe the network to find the address of the internal host that has the service open on the high port.

Many multimedia vendors favor UDP over TCP because of its lower overhead, thus higher throughput. However, since the server does not send the UDP data packets back on the same requested port from the client, the packet filtering routers have difficulty controlling the data stream flow. The only way a packet filter can control/allow the data stream back to the client is by opening many high UDP ports on the router, which opens a security vulnerability.

Cisco Solution: Enhanced Multimedia Adaptive Security

With the PIX Firewall series, no special client configurations are required. The PIX Firewall series' conditional, stateful, connection-oriented adaptive security strategy includes the following features:

- No special port or protocol setup/configuration is required at user PCs; dramatically saves on installation and maintenance costs
- No proxy settings are required at the PIX Firewall; no retransmission overhead
- No limit to data stream port count; highest throughput, no bottleneck at firewall
- Both TCP and UDP connections are allowed; higher throughput and ease of use

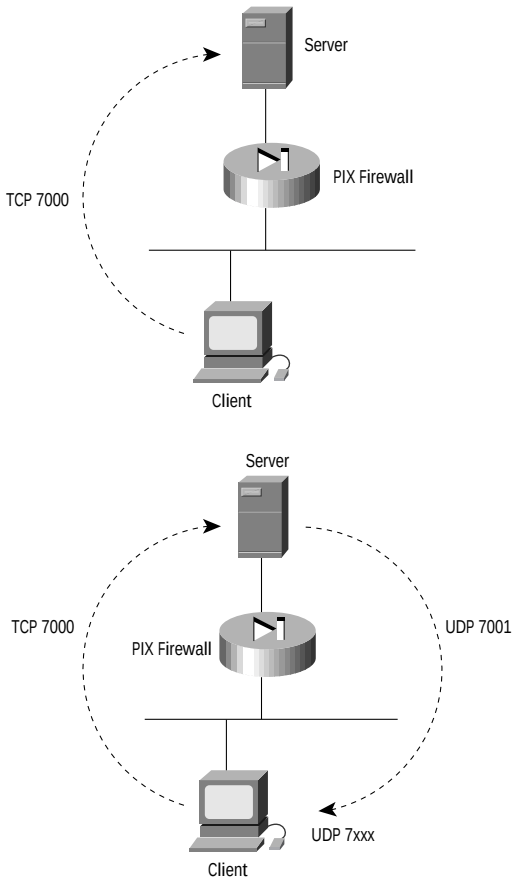
Example Security Scenarios for Multimedia Applications

This section outlines the behavior of several multimedia applications to compare firewall effectiveness.

VDONet VideoLive

VideoLive sends the client's originating request to the server's TCP port 7000. The server sends the response data from source port UDP 7001 to a solicited destination port on the client. See Figure 3.

Figure 3 VideoLive Connection Sequence



Proxy Firewalls

Proxy firewalls require either the network manager or the client/user to specially configure the preferences/ configuration window on the multimedia player to allow the video/audio stream to the client workstation. This process presents laborious and costly installation and maintenance issues for proxy servers.

Stateful Filtering Firewalls

For this approach, the system administrator must configure the firewall to expect port 7001 for VideoLive to any destination port.

The PIX Firewall series differs from other stateful and proxy firewalls by transparently supporting VideoLive. When a client requests a connection to TCP port 7000, the PIX Firewall series expects an incoming connection from UDP 7001 to a solicited port specified in the control connection stream. The PIX Firewall series allows only that host to send on UDP 7001 to only the solicited destination port during the time that the security connection is maintained on TCP port 7000. If either end disconnects, the PIX Firewall series closes both UDP port 7001 and TCP port 7000.

CU-SeeMe

A CU-SeeMe client sends the originating request from TCP port 7649 to TCP port 7648 at the video server (the "reflector"). The CU-SeeMe datagram is unique in that it includes the legitimate IP address provided by the firewall in the header as well as a binary copy of the internal IP source address in the data portion of the datagram. See Figures 4 and 5. In normal TCP mode, the firewall hides the address of the internal client from the outside by replacing it with a legitimate IP address (randomly chosen from a pool) in the header. The CU-SeeMe reflector compares the IP address in the header with the IP address in the data section of the datagram. If the addresses match, the reflector opens UDP port 7648 for data streaming. However, with standard firewalls, the reflector notes the discrepancy between the address in the header and the address in the data section and does not open UDP port 7648. Thus, typical stateful filtering requires a legitimate IP address on the inside—a private address does not work. This represents a security breach.

Packet Filters

This approach requires opening TCP ports 7648 and 7649 and UDP ports 7648 and 7649 at all times. This represents a security breach.

Stateful Filtering Firewalls

This approach requires a legitimate, registered (Internet-routable) IP address on the inside. This represent a security breach.

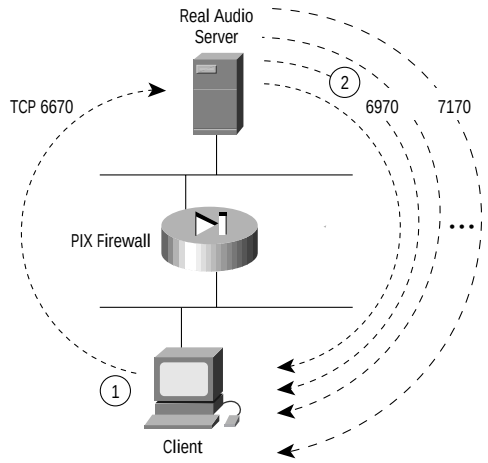
The PIX Firewall series provides transparent support for CU-SeeMe.

The PIX Firewall series changes the IP address in the data section of the CU-SeeMe datagram to match the legitimate IP address that it assigned to this connection. The reflector compares the addresses, finds that they match, and opens the UDP data connection to allow data to stream. Security is maintained by the security connection on UDP ports 1234 and 1558. This allows CU-SeeMe to be used with both registered and nonregistered IP addresses.

Progressive Network's Real Audio

Real Audio sends the originating request to TCP port 7070. The Real Audio server replies with multiple UDP streams anywhere from UDP 6970 through UDP 7170 to solicited destination ports on the client. See Figure 6.

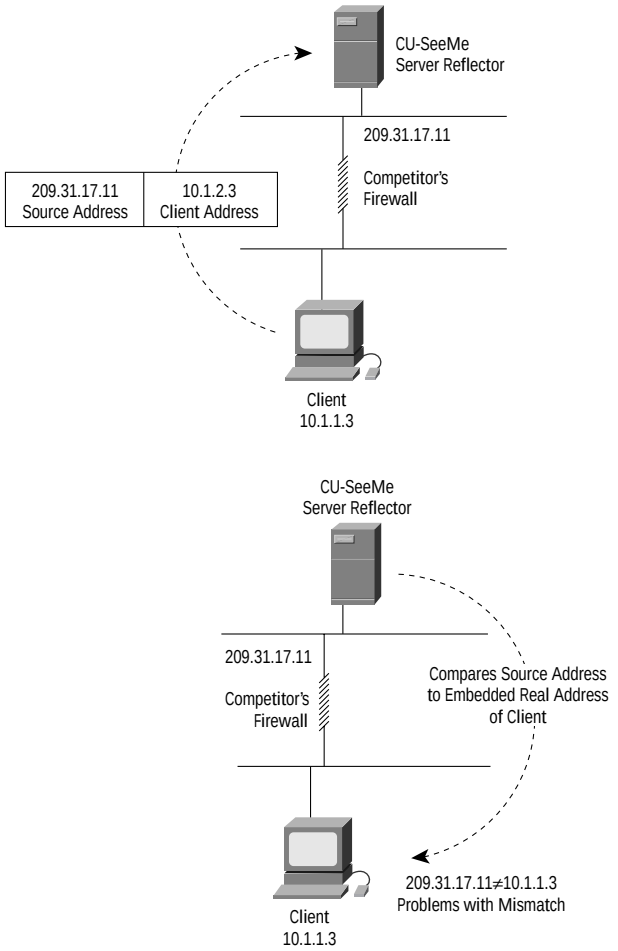
Figure 4 Real Audio Connection Sequence



Proxy Firewalls

The client must be installed with a proxy configuration. The proxy server is easily overloaded because it must manage many connections per client. Sound quality decreases due to the low UDP ports supported.

Figure 5 CU-SeeMe Connection Sequence, Competitors' Firewalls



Stateful Filtering Firewalls

Proxies require the user to throttle down to TCP, decreasing sound quality.

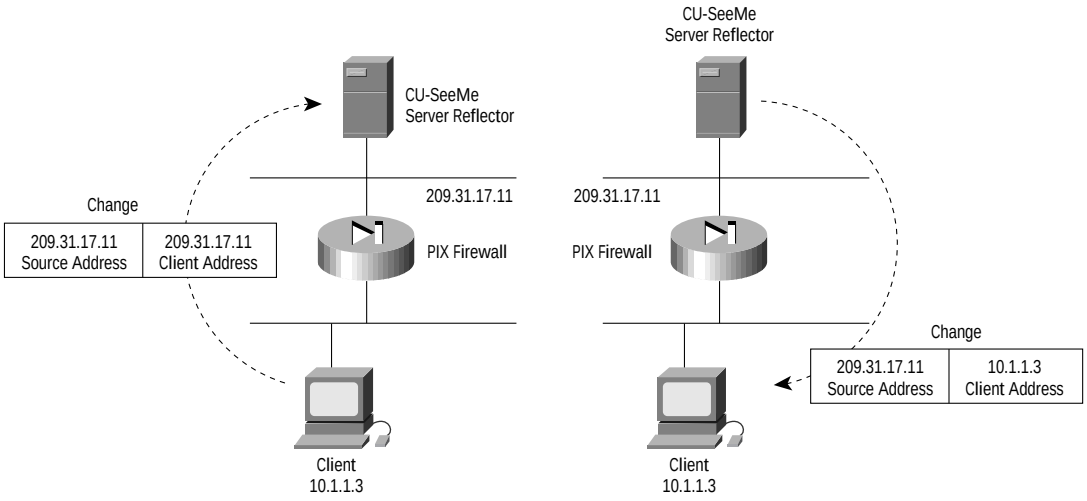
The PIX Firewall series monitors the TCP control connection to destination port 7070 and allows only the destination host to communicate to the global pool via UDP ports 6970 through 7070 while the TCP control connection is active. Because multiple UDP ports are available to handle high data rates, the PIX Firewall series connection maintains higher sound quality than the other firewall approaches.

Internet Address Depletion

The combination of explosive growth in TCP/IP networking and the long-standing practice of assigning globally unique IP addresses to all hosts on TCP/IP networks has resulted in rapid depletion of the available IP address space. The Cisco PIX Firewall series offers a method for resolving IP address depletion, enabling companies to save days or weeks by avoiding manually renumbering networks.

Telecom Solutions, for example, a United States-based telecommunications equipment manufacturer, estimated that it would have required five staff members at least one week to create an entirely new subnet infrastructure for its 400 end users across three sites when it considered upgrading its existing Internet access technologies. By choosing Cisco's PIX Firewall, this company saved many hundreds of thousands of dollars in implementation, maintenance, and support costs.

Figure 6 CU-SeeMe Connection Sequence, PIX Firewall



What's the Problem?

Each host that is connected to the global Internet requires a unique address, and this presents a serious problem for new enterprise connections because there are a limited number of these addresses. How does a company with hundreds or thousands of machines connect to the Internet if it cannot procure additional addresses?

One option on the horizon is called the IP: next generation (IPng), which is an area of the Internet Engineering Task Force (IETF) that is currently considering proposals for a long-term solution. As stated in RFC 1669, "Given the potential proliferation of network address translation devices, it is not clear that IPng will secure sufficient following to attain market viability." In the meantime, three primary strategies have emerged for maximizing the longevity of the current IP standard.

Address Allocation Guidelines and Private Internets

The traditional method of Internet address allocation splits the address space into three classes of networks based on the number of hosts within them. For convenience, address classes are divided on eight-bit boundaries, allowing approximately 250 hosts on a Class C network, 64,000 on a Class B network, and 16 million on a Class A network. Unfortunately, this lack of granularity does not reflect the realities of enterprise networking. Many organizations have networks that fall somewhere between the Class C and Class B magnitudes. A network manager with 4000 hosts, for example, faces the dilemma of using 16 Class C registrations, or 1/16 of a Class B registration.

Because of the underutilization of address space within assigned Class B addresses, Class B addresses are now nearly impossible to get. The Internet Registry (IR) assigns blocks of multiple Class C addresses to applicants who do not meet the IR requirements for a Class B allocation, which include a minimum of 4096 hosts and the submission of a detailed network plan.

According to RFC 1466, "The restrictions in allocation of Class B network numbers may cause some organizations to expend additional resources to utilize multiple Class C numbers. This is unfortunate, but inevitable if we implement strategies to control the assignment of Class B addresses. The intent of these guidelines is to balance these costs for the greater good of the Internet."

Organizations have historically been assigned globally unique IP network addresses regardless of their intent to connect their private network to the Internet. Even those that do join the Internet usually allow Internet access to only a small percentage of the hosts on their leaf domain. According to RFC 1687, the ratio of hosts with direct Internet access to hosts without such connectivity is typically between 1:1000 and 1:10,000 in large corporate networks. The use of registered, globally unique IP addresses for such large numbers of hosts that don't need them has further exacerbated the address depletion problem.

Recently, the Internet Assigned Numbers Authority reserved three blocks of the address space for use by private networks: one Class A, 16 Class B, and 255 Class C network numbers. These addresses may be used on the enterprise LAN for hosts that will never have direct IP connectivity with external hosts. But in real-world enterprise networks, hosts fall naturally into three categories, not the "always/never connected to the Internet" dichotomy implied by RFC 1597.

Table 1 Three Categories of "Real-World" Hosts

Levels of Connectivity	Example
Always	E-mail, FTP, WWW servers
Sometimes	User's workstation or PC
Never	Secure hosts, corporate database servers

The private network addressing scenario laid out in RFC 1597 relegates the connectivity needs of this middle category of hosts to "application layer relays," otherwise known as proxy servers. Demand from end users for the direct Internet connectivity they need to run World Wide Web browsers on their desktops is growing daily, but the deployment of proxy servers to meet this need will add yet another layer of complexity (along with potential maintenance and administrative headaches) to the network.

Classless Interdomain Routing––CIDR

Classless interdomain routing (CIDR), as described in a series of Internet RFCs (1467, 1481, 1517, 1518, 1519, and 1520), is primarily aimed at increasing the efficiency (and reducing the size) of the Internet routing tables. This goal is being accomplished by a policy of allocating IP addresses in a way that allows routing information for multiple networks to be aggregated into a single routing table entry. Internet service providers are now being assigned contiguous blocks of the Class C address space, which are in turn reallocated to their new customers. The incorporation of variable-length netmask information into the routing protocols makes it possible for these multiple Class C networks to be served by a single routing table entry on the Internet. The designation of this mechanism as classless comes from the fact that it enables routing at intermediate levels between the traditional eight-bit boundaries of IP network classes.

One unfortunate side effect of CIDR is that, in order to maximize its effectiveness, existing domains may need to be renumbered. The result is a high administrative cost for the networks involved.

Network Address Translation––NAT

The third (and most easily deployable) strategy for alleviating IP address depletion is network address translation (NAT, RFC 1631). Based on the concept of address reuse by private networks, NAT operates by mapping the reusable IP addresses of the leaf domain to the globally unique ones required for communication with hosts on other networks. It would be difficult indeed to take full advantage of reusable addresses on a private network without employing NAT functionality.

It is also unlikely that many network managers will voluntarily incur the expense of renumbering their networks, as will eventually be necessary for full deployment of CIDR. The insertion of a network address translator at the Internet connection point makes this a one-step operation, eliminating the need to visit each host on the corporate LAN to change its IP address. NAT is in synch with both reusable addressing and CIDR, simplifying or eliminating many of the obstacles associated with the deployment of these initiatives. But NAT also provides simple solutions for numerous other network management problems.

Cisco's PIX Firewall Series

Cisco Systems introduced the PIX Firewall series, the first commercially available implementation of NAT, in late 1994. The PIX Firewall series does true RFC 1631 translation, as well as port address translation (PAT), which allows multiple high ports to be mapped to a single visible IP host address. Many other firewalls only support PAT and not true RFC 1631 NAT.

The Cisco PIX Firewall series can be configured to selectively perform or not perform address translation, depending on the user's needs. Configuration is simplified with an enhanced Web browser-based GUI. A Cisco IOS-based, command-line interface is also available.

Cisco's PIX Firewall series, which incorporates strong firewall security and cut-through proxy authentication functionality along with its NAT and PAT features, comes in a standard, 19-inch, rack-mountable package and is equipped with two 10/100-Mbps Ethernet or 4/16-Mbps Token Ring ports. In a typical installation, the inside (local) port is connected to the private network and the outside (global) port connects Cisco's PIX Firewall series to the DMZ segment, where the Internet router resides. Once configured, Cisco's PIX Firewall series broadcasts a default route to the inside network and provides proxy Address Resolution Protocol (ARP) within the DMZ segment for hosts on the inside network.

Cisco also offers an innovative feature called Dual NAT for customers who need to connect two overlapping IP addresses together. This is particularly important with intranet designs, where a company must connect a partition of networks from one unregistered address to another registered address. Dual NAT resolves this conflict by tracking which addresses are from which network, allowing delivery of data to the proper network.

Cisco also offers the PIX Private Link encryption card that uses the Data Encryption Standard (DES) algorithm to encrypt data packets. This capability allows companies to create a virtual private network (VPN) across the Internet or any other packet network. The PIX Private Link card also supports standards-based technology by incorporating the IETF's Authentication Header/Encapsulating Security Payload (AH /ESP) protocols (RFCs 1826 and 1827, respectively).

Dynamic and Static Address Allocation

Mapping between local and global addresses is done dynamically or selectively. An Internet-bound packet sent by a host on the inside network follows default routes to the inside interface of Cisco's PIX Firewall series. Upon receipt of the outbound packet, the source address is extracted and compared to an internal table of existing translations. If the inside host's address does not appear in the translation table, a new entry is created for that host, assigning a globally unique IP number from the pool of available addresses. The actual translation is accomplished by changing the source address of the packet to this "legal" address. Since the differences between the original and translated versions of the packet are known, the checksums are efficiently updated with a simple adjustment rather than a complete recalculation. After a user-configurable timeout period, during which there have been no translated packets for a particular address mapping, the entry is removed and the global address is freed for use by another inside host.

As mentioned previously, the number of hosts needing Internet connectivity from inside the corporate firewall is generally a very small percentage of the domain, but even fewer of them will require access simultaneously. Dynamic and static address allocation as implemented in Cisco's PIX Firewall series efficiently leverages a relatively small registered address space to serve the Internet connectivity needs of a much larger user population. In the course of expanding the private network, Internet access is available to the new hosts without reconfiguration.

Static Translations and Conduits

Unlike clients, internal hosts acting as Internet servers (e-mail, anonymous FTP, WWW, and others) require a predictable registered address and a different access policy. Cisco's PIX Firewall series offers optional static translations that hard wire an internal address to a specific global address and do not time out. Static translations default to a "wide open" state, allowing any host on the Internet to connect to any port on the inside server, but security criteria for each conduit may be enforced via a cut-through proxy authentication or standard access control list.

Table 2 Access Control List

Protocol	TCP or UDP
IP Address	Remote hosts/networks permitted access
Netmask	Applied to the IP address
Port	IP port number for which access is allowed

Once conduits are created for a static translation, all connections not specifically allowed are denied. These disallowed packets are silently dropped (from the intruder's perspective) and logged for review by the systems administrator.

Sequence Number Randomization

The technique of IP address spoofing has been well known since it was first described by Robert T. Morris in 1985. Recently, a rash of such attacks on the Internet precipitated a Security Advisory from the CERT (CA-95:01). Essentially, spoofing IP addresses requires the ability to guess the sequence numbers of TCP packets. Most TCP/IP implementations use a simple additive algorithm for incrementing sequence numbers, making it a trivial matter for an intruder to guess the next number in a connection (from even a single intercepted packet) and subsequently hijack that session. Cisco's PIX Firewall series makes the process of guessing TCP sequence numbers extremely difficult, if not impossible, by using a randomizing algorithm for their generation for each session.

Reports and Alerts

All connections are logged so the PIX Firewall series can use this information to generate reports. Also, using the standard Berkeley syslog mechanism, Cisco's PIX Firewall series can log extensive security and administrative information to a designated host on the internal network. Cisco also supports SNMP traps and SNMP syslog MIBs. The syslog traps supported include:

- Security violation
- Network interface controller (NIC): link up or down

- Cold/warm start
- Failover/hot standby

Cisco's PIX Firewall series sends a syslog trap every time a security-related syslog message is generated. A failover occurrence sends a syslog trap every time the Cisco PIX Firewall series is newly activated. A message is also sent from the firewall if a failover/hot standby occurred during normal operations of the Cisco PIX Firewall. In either case, redundancy for syslog traps occur from either the primary PIX Firewall series failing, or when the secondary PIX Firewall series is activated. In either case, a syslog trap is generated.

MIB II Groups

Cisco supports the following MIB II groups: system, interfaces, and SNMP. The location and contact fields in system are settable using a command line interface and HTML.

Setting Values

Cisco's PIX Firewall series does not allow "state" to be changed via SNMP. All "set" requests are rejected. These syslog messages enable detailed monitoring of attempted security violations and network resource usage.

Strong Security, Low Cost of Ownership, and High Performance Make Cisco's PIX Firewall Series Shine

Cisco's PIX Firewall series provides companies with an elegant solution for security and IP address depletion. Working in tandem with routers and Cisco IOS software, Cisco's PIX Firewall series provides a second layer of protection that keeps unauthorized users from accessing a corporate network. Most valuable, Cisco's PIX Firewall series is much less complex than a proxy server. It is easier to install and does not require the overhead needed to maintain proxy servers.

In addition to securing the network, Cisco's PIX Firewall series also helps companies that face IP address depletion. No longer must companies manually renumber their networks. Instead, Cisco's PIX Firewall series automatically maps reusable IP addresses to globally unique addresses—providing company hosts with full, transparent access to Internet sites.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
World Wide Web URL:
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic-Batiment L1/L2
16, Avenue du Quebec
BP 706-Villebon
91961 Courtaboeuf Cedex
France
Tel: 33 1 6918 61 00
Fax: 33 1 6928 83 26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
Tel: 408 526-7660
Fax: 408 526-4646

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
Tel: 81 3 5219 6000
Fax: 81 3 5219 6010

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Connection Online Web site at http://www.cisco.com.

Argentina · Australia · Austria · Belgium · Brazil · Canada · Chile · China (PRC) · Colombia · Costa Rica · Czech Republic · Denmark Finland · France · Germany · Hong Kong · Hungary · India · Indonesia · Ireland · Israel · Italy · Japan · Korea · Malaysia · Mexico The Netherlands · New Zealand · Norway · Philippines · Poland · Portugal · Russia · Singapore · South Africa · Spain · Sweden Switzerland · Taiwan, ROC · Thailand · United Arab Emirates · United Kingdom · Venezuela