DATA SHEET

MANAGED SERVICES: CISCO IOS FIREWALL

This data sheet provides an overview of the Managed Services Cisco IOS Firewall security solution.

Cisco IOS Software-Based Technologies for Managed Services

The managed network services opportunity is projected to increase significantly in the coming years. A recent Cisco Systems® survey of 500 large corporations found substantial interest in managed IP services. At the top of the list were IP VPNs as a foundation for the integration of older networks and the addition of new services. Business customers—from the largest global corporations to midsize and smaller firms—are focusing on achieving cost efficiencies while adding new services. Recognizing the value of the network as a strategic tool, many companies are turning to service providers to manage their networks so they can focus more resources on their businesses. The IP VPN allows integration of older networks (such as ATM and Frame Relay) and provides a foundation for many new services. Examples include managed core services offerings and managed WAN and LAN services, which have been augmented by improved Web-based, user-friendly tools; service-level agreements (SLAs) and guarantees; and many newer IP-based applications, such as voice over IP (VoIP).

Cisco IOS® Software technologies make possible a secure, highly available, cost-effective managed services environment within an IP VPN. Partnering with Cisco®, service providers can streamline their infrastructures to avoid unnecessary overhead, offer more services more efficiently, and position these service offerings successfully with the established Cisco global enterprise customer base. Features such as Enhanced Interior Gateway Routing Protocol (EIGRP) make routing more efficient and turn IP/Multiprotocol Label Switching (MPLS) VPNs into a simpler, benefit-rich addition to customer networks.

Cisco IOS Software technologies for managed services environments serve as the foundation for high-speed routing and IP/MPLS, scalable IP VPNs, and robust network security, all integrated through a next-generation network management interface. These operate within several network topologies to fit the needs of different customers. Products in the Cisco IOS Software Family bring customizable networking solutions to headquarters, branch offices, and campuses, and extend full network capability to mobile workers, telecommuters, and remote data centers.

Cisco IOS Firewalls in Managed Services

More companies are realizing that the network is at the heart of their operations, and are making security a top priority. Small and medium-sized businesses (SMBs) are joining larger organizations to put appropriate safeguards in place. Service providers are taking up the security challenge, dedicating significant resources and personnel to selling managed security services. Cisco network security solutions that are embedded within IP VPNs allow service providers to meet the security requirements of a wide range of business

customers. Integral to the Cisco security portfolio, Cisco IOS Firewall and Cisco IOS Intrusion Prevention System (IPS) give service providers comprehensive solutions to address growing network security concerns.

Cisco IOS Firewall gives providers of managed services the ability to offer router-based, advanced firewall capabilities and intrusion detection and authentication. Cisco IOS Firewall is supported on multiple Cisco router platforms, from the Cisco 800 to Cisco 7301 Series routers. The Per-User Firewall feature of Cisco IOS Firewall allows service providers to offer a managed firewall solution through download of firewall, access control lists (ACLs), and other settings on a per-user basis, using a profile in the authentication, authorization, and accounting (AAA) server. AAA services streamline management of security solutions for network and cost efficiencies.

These and other security features from Cisco provide service providers with technologies that can generate ongoing managed services revenue while maintaining securely managed networks for large enterprises and smaller customers.

PRODUCT OVERVIEW

Cisco Systems is redefining best-in-class routing with integrated security solutions. The Cisco IOS Firewall is a stateful inspection firewall option available for Cisco routers. Developed from market-leading Cisco PIX® Firewall technologies, Cisco IOS Firewall is an ideal single-box security and routing solution for protecting the WAN entry point into the network. Although the hub is a common location to block and inspect traffic for attacks, it is not the only location to consider when deploying security. Branch offices are also an important location in your network to both block and inspect traffic for attacks.

The primary features of Cisco IOS Firewall include:

- Stateful firewall, including denial-of-service (DoS) protection
- Enhanced application, traffic, and user awareness to identify, inspect, and control applications
- Advanced protocol inspection for voice, video, and other applications
- Per-user, interface, or subinterface security policies
- Tightly integrated identity services to provide per-user authentication and authorization
- Ease of management through features such as Role-Based Access/CLI Views, which allows secure, logical separation of the router between network operations, security operations, and end users, and Firewall Policy View in Cisco Router and Security Device Manager (SDM)

The Cisco IOS Firewall not only helps enable a single point of protection at the perimeter of a network, it also makes security policy enforcement an inherent component of the network itself. The flexibility and cost-effectiveness of both dedicated and integrated policy enforcement facilitates security solutions for extranet and intranet perimeters and Internet connectivity for a branch or remote office. Integrated into the network through Cisco IOS Software, the Cisco IOS Firewall provides customers the unique advantage of using advanced quality-of-service (QoS) features in the same router.

CISCO IOS FIREWALL

As network security becomes increasingly critical to securing business transactions, businesses must integrate security into the network design and infrastructure itself. Security policy enforcement is most effective when it is an inherent component of the network.

The Cisco IOS Firewall is a security-specific option for Cisco IOS Software. It integrates robust firewall functions and intrusion detection and prevention for every network perimeter. It adds greater depth and flexibility to existing Cisco IOS Software security solutions (that is, authentication, encryption, and failover) by delivering state-of-the-art security features: stateful, application-based filtering, dynamic per-user authentication and authorization, URL filtering, and others. When combined with Cisco IOS IP Security (IPSec) and Cisco IOS Software technologies, such as Layer 2 Tunneling Protocol (L2TP) tunneling and QoS, Cisco IOS Firewall provides a complete, integrated VPN solution.

WHAT IS A FIREWALL?

A firewall is a physical software or hardware barrier to prevent access between parts of an internal network (for example, a barrier to prevent access to human resources) and to prevent access to and from external networks. This barrier is unique because it allows predefined traffic to pass through the firewall while being monitored for protocol anomalies. The difficult part is determining the criteria by which the packets are granted or denied access through the device. The access policy to be enforced must be determined in advance so that the firewall reflects the appropriate level of protection. This could be based upon user ID and password authentication, source address, protocol type, or other criteria.

As mentioned, the firewall blocks some traffic and permits other types of traffic to traverse. The performance of the firewall depends on the implementation, because it is restricted by the base platform on which it is implemented. A dedicated device that is not a network router, also known as an appliance, is restricted by its support of many Internet networking protocols and applications. This document does not detail the merits of an appliance versus an integrated firewall router; the user must consider the characteristics of both during the selection process. Some firewalls place a greater emphasis on blocking traffic, whereas others emphasize permitting traffic. A firewall implements an access control policy, as defined by each individual user. Firewalls are not just ACLs; rather, they are a stateful-inspection application.

CISCO IOS FIREWALL DESCRIPTION

Router-Based Firewall Functions

Cisco IOS Firewall is available on a wide range of Cisco IOS Software releases. It offers sophisticated security and policy enforcement for connections within an organization (intranet) and between partner networks (extranets), as well as for securing Internet connectivity for remote and branch offices.

The Cisco IOS Firewall is the best choice for integrating multiprotocol routing with security policy enforcement and enabling managers to configure a Cisco router as a firewall. It scales to allow customers to choose a router platform based on bandwidth, LAN and WAN density, and multiservice requirements; simultaneously, it benefits from advanced security.

Refer to the following guidelines when choosing the right Cisco router for varied security environments:

- Small or home offices: Cisco 800 to Cisco 1800 series routers
- Branch and extranet environments: Cisco 2600 to Cisco 3800 series routers
- VPN and WAN aggregation points or other high-throughput environments: Cisco 7200, 7301, and 7500 series routers; and the Cisco Catalyst® 5000 and Catalyst 6000 series switches

Key Benefits

The Cisco IOS Firewall interoperates transparently with Cisco IOS Software, providing outstanding value and benefits:

- Flexibility—Installed on a Cisco router, Cisco IOS Firewall is an all-in-one, scalable solution that performs multiprotocol routing, perimeter security, intrusion detection, VPN functions, and per-user authentication and authorization.

- Investment protection—Integrating firewall functions into a multiprotocol router takes advantage of an existing router investment, without the cost and learning curve associated with a new platform.

- VPN support—Deploying Cisco IOS Firewall with Cisco IOS Software encryption and QoS VPN features helps enable secure, low-cost transmissions over public networks. It helps ensure that mission-critical application traffic receives high-priority delivery.

- Scalable deployment—Cisco IOS Firewall is available for a wide variety of router platforms. It scales to meet the bandwidth and performance requirements of any network.

- Easier management—With Cisco Policy Manager software, a network administrator can configure Cisco IOS Security features from a central console over the network. Additional management tools are available, such as the CiscoWorks VPN/Security Management Solution (VMS) and products offered by some third-party partners such as Solsoft.

- Easier provisioning—Combining the Cisco CNS 2100 Series Intelligence Engine and the Cisco IOS Extensible Markup Language (XML) application helps a network administrator order any Cisco router with little or no preconfiguration to be delivered to a given destination. The router has the most current Cisco IOS Software release router configuration and its security policy configuration for the firewall when it is connected to the Internet.

Cisco IOS Firewall is supported on the Cisco 800 to Cisco 7500 series routers and Cisco Catalyst 5000 and Catalyst 6000 series switches. This breadth of supports helps it deliver important benefits, including multiservice integration (data, voice, video, and dial) and advanced security for dialup connections.

Cisco IOS Firewall Features Overview

The Cisco IOS Firewall delivers integrated firewall functions for Cisco networks and increases the flexibility and security of Cisco routers. Table 1 provides an overview of primary features.

Table 1. Cisco IOS Firewall Overview

FEATURE	DESCRIPTION
Cisco IOS Firewall Engine	The engine provides stateful packet inspection of TCP, User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP) traffic as well as protocol anomaly detection for per-application-based access control to internal users for all traffic across perimeters.
Firewall voice traversal	Voice traversal is provided by application level intelligence of the protocol as to the call flow and associated channels that are opened. Voice protocols that are currently supported are H.323v2, Skinny Call Control Protocol (Skinny), and Session Initiation Protocol (SIP).
Cisco IOS Firewall for IPv6	This feature provides stateful packet inspection of IPv6 TCP, UDP, and ICMP sessions while coexisting and providing stateful firewall inspection of IPv4 traffic.
Transparent Cisco IOS Firewall	This feature helps enable insertion of a stateful Layer 2 firewall within an existing network, without readdressing statically defined devices. It provides both Layer 2 and 3 capabilities on the same Cisco IOS Firewall router.
Extended Simple Mail Transfer Protocol (ESMTP) inspection	ESMTP dynamically supports the traversal of ESMTP messages while enabling identification of ESMTP and SMTP attacks.
Simple Mail Transfer Protocol (SMTP) mail protection	SMTP provides protocol anomaly detection while inspecting for several well-known SMTP mail attacks.
Destination URL policy management	URL filtering supports Websense and N2H2 services, and local router-table definition.
Authentication proxy	Network administrators can create specific security policies for each user with Cisco IOS Firewall LAN-based, dynamic, per-user authentication and authorization for HTTP, HTTPS, Telnet, and FTP connections.
ICMP inspection	Cisco IOS Firewall uses stateful inspection to “trust” ICMP messages generated within the private network, and to permit the associated ICMP replies
Per-user firewall	Cisco IOS Firewall also can apply an inspection policy on a per-user or subinterface basis. Broadband service providers that wish to support per-subscriber protection can implement the Cisco IOS Firewall on broadband aggregation routers.
DoS detection and prevention	DoS detection and prevention defends and protects router resources against common attacks, checks packet headers, and drops suspicious packets.
Multicast and the Cisco IOS Firewall	The Cisco IOS Software router can simultaneously support both Cisco IOS Firewall and IP Multicast services.
Dynamic port mapping	This feature allows network administrators to run Cisco IOS Firewall-supported applications on nonstandard ports.
Basic and advanced traffic filtering	• Standard and extended ACLs apply access controls to specific network segments and define which traffic passes through a network segment.

	• Lock and Key—Dynamic ACLs grant temporary access through firewalls upon user identification (username and password).
Policy-based multi-interface support	This feature provides the ability to control user access by IP address and interface, as determined by the security policy.
Redundancy and failover	This feature automatically routes traffic to a backup router if a failure occurs.
Network Address Translation (NAT)	This feature hides the internal network from the outside for enhanced security.
Time-based access lists	This feature defines a security policy based on the time of day and day of the week.
Java applet blocking	Java applet blocking offers the following: • Protects against unidentified, malicious Java applets VPNs, IP Security (IPSec) encryption, and QoS support • Operates with Cisco IOS Software encryption, tunneling, and QoS features to secure VPNs • Provides scalable encrypted tunnels on the router, while integrating strong perimeter security, advanced bandwidth management, intrusion detection, and service-level validation • Offers standards-based feature for interoperability
Peer router authentication	This feature helps ensure that routers receive reliable routing information from trusted sources.
Real-time alerts	This feature logs alerts for DoS attacks or other preconfigured conditions; it is now configurable on a per-application, per-feature basis.
Audit trail	Audit trail details transactions and records time stamp, source host, destination host, ports, duration, and total number of bytes transmitted for detailed reporting. It is now configurable on a per-application, per-feature basis.
Event logging	This feature allows administrators to track potential security breaches or other nonstandard activities in real time by logging system error message output to a console terminal or syslog server, setting severity levels, and recording other parameters.
Cisco IOS router and firewall provisioning	This feature offers zero touch provisioning of the router, versioning, and security policies such as firewall rules.
Integration with Cisco IOS Software	The Cisco IOS Firewall interoperates with Cisco IOS Software features, integrating security policy enforcement into the network.

CISCO IOS FIREWALL ENGINE

The Cisco IOS Firewall engine provides secure, per-application access control across network perimeters. It scrutinizes source and destination addresses in order to enhance security for TCP and UDP applications that use well-known ports, such as FTP and e-mail traffic. The Cisco IOS Firewall allows network administrators to implement firewall intelligence as part of an integrated, single-box solution.

Sessions with an extranet partner involving Internet applications, multimedia applications, or Oracle databases would no longer need to open a network doorway accessible through weaknesses in a partner's network. The Cisco IOS Firewall lets tightly secured networks run today's basic application traffic, in addition to advanced applications such as multimedia and videoconferencing, securely through a router.

The Cisco IOS Firewall Impact on Network Security

The Cisco IOS Firewall is a per-application control mechanism for IP traffic, including standard TCP and UDP Internet applications, multimedia applications (including H.323 and other video applications), and Oracle databases. The Cisco IOS Firewall engine inspects TCP and UDP packets and tracks their "state," or connection status, watching traffic flow for any deviation of the protocol, which when found is flagged and acted upon as a protocol anomaly.

TCP is a connection-oriented protocol. Before transmitting data, an originating host negotiates a connection with a destination in what is known as a "three-way handshake." This handshaking process helps ensure valid TCP connections and error-free transmission. During connection setup, TCP passes through several states, or phases, which are easily identifiable in packet headers. Standard and extended ACLs read states from packet headers to determine whether traffic is permitted across a link.

The Cisco IOS Firewall adds inspection intelligence to ACL capabilities by reading the entire packet for application status information. Using this information, the firewall creates a temporary, session-specific ACL entry, permitting return traffic into the trusted network. This temporary ACL effectively opens a door in the firewall. When a session times out or ends, the ACL entry is deleted, and the door closes to additional traffic. Standard and extended ACLs cannot create temporary ACL entries; until now, administrators have been forced to weigh security risks against information access requirements. Advanced applications that select from multiple channels for return traffic have been difficult to secure using standard or extended ACLs.

The Cisco IOS Firewall is more secure than current ACL-only solutions, because it accounts for application type in deciding whether to allow a session through the firewall, and it determines whether it selects from multiple channels for return traffic. Before Cisco IOS Software supported the Cisco IOS Firewall, administrators could permit advanced application traffic only by writing permanent ACLs that essentially left firewall doors open, so administrators generally opted to deny all this application traffic. With the firewall, they can now securely permit multimedia and other application traffic by opening the firewall only as needed, and closing it all other times.

For example, if the Cisco IOS Firewall is configured to allow Microsoft NetMeeting, when an internal user initiates a connection, the firewall permits return traffic. However, if an external NetMeeting source initiates a connection with an internal user, the firewall denies entry and drops the packets.

Firewall Engine Intelligence

The Cisco IOS Firewall supports a wide range of protocols by way of application layer gateways (ALGs). Prior to firewalls, statically defined ACLs were defined in the router for every potential permutation of protocol access through the device. The disadvantage of statically defined ACLs is that the system administrator kept many ports open to allow for the return of network traffic from applications that needed to respond to client requests. Opening these ports introduced a wide variety of security holes and defeated the initial intent of securing applications.

ALGs offer the intelligence of several protocols, including H.323, SIP, and other applications that are embedded in the firewall inspection engine. They inspect the data contained in the application layer of the IP protocol, usually into Layer 7. The action depends on the particular protocol, because each requires

different treatment and appropriate actions. Some protocols have flows that need to be monitored (for example, SIP and Skinny), whereas other protocols require particular data values.

The Cisco IOS Firewall dynamically applies ACLs, which open the necessary application ports based on the specific application and close these ports at the end of the application session. As mentioned, the firewall achieves this function by inspecting the application data, checking for conformance of the application protocol, extracting the relevant port information to create the dynamic ACLs, and ultimately closing these ports at the end of the session.

CISCO IOS FIREWALL FEATURE SUPPORT

General Protocol Support

When a protocol is configured for the firewall, that protocol traffic is inspected, state information is maintained, and in general, packets are allowed back through the firewall only if they belong to a permissible session. Two general statements can be made about the Cisco IOS Firewall protocol session types:

- Supports all TCP sessions, regardless of the application layer protocol (sometimes called "single-channel" or "generic" TCP inspection)
- Supports all UDP sessions, regardless of the application layer protocol (sometimes called single-channel or generic UDP inspection)

Users also can configure the firewall to specifically inspect certain application layer protocols such as the following: CU-SeeMe, FTP, H.323v2, SIP, Skinny, HTTP (Java blocking), ICMP, Microsoft NetShow, UNIX R-commands (such as rlogin, rexec, and rsh), RealAudio, Real Time Streaming Protocol (RTSP), remote-procedure call (RPC), SMTP, SQL*Net, StreamWorks, Trivial File Transfer Protocol (TFTP), and VDOLive.

RTSP Support

RTSP is the IETF standards-based protocol (RFC 2326) for control over the delivery of data with real-time properties such as audio and video streams. It is useful for large-scale broadcasts and audio and video-on-demand streaming, and is supported by a variety of vendor products of streaming audio and video multimedia, including the Cisco IP/TV® system, RealNetworks RealAudio G2 Player, and Apple QuickTime 4 software.

For more details about this support, refer to the Cisco security configuration guides and command references.

H.323 Support

The Cisco IOS Firewall supports H.323 Version 1 and Version 2 inspections. H.323v2 provides additional options over H.323v1, including a "fast-start" option. The fast-start option minimizes the delay between a user-initiated connection and receipt of the data (voice or video). H.323v2 inspection is backward-compatible with H.323v1.

With H.323v1, a separate channel for media control (H.245 channel) is opened after a TCP connection is established between the client and server (H.225 channel). Multimedia channels for audit and video are further negotiated through this channel.

The H.323v2 client opens a connection to the server, which is listening on port 1720. The data channel between the client and the server is dynamically negotiated using any of the high UDP ports (1024 to 65536).

The firewall uses this port information along with connection information from the client to create dynamic ACL entries in the firewall. As TCP or UDP connections are terminated, the firewall removes these dynamic entries from the appropriate ACLs.

SIP Support

SIP is an application level VoIP protocol that can establish, modify, and terminate multimedia calls. It is described in RFC 2543.

SIP signaling uses port 5060 (which is user-configurable) to set up media channels for the call. The signaling channels could have a random source port with the destination port defaulting to 5060 while media streams are dynamically allocated. SIP signaling sessions can be carried over UDP or TCP (unicast or multicast). Currently, Cisco and Broadsoft proxy servers do not support the TCP mode; therefore, the Cisco implementation supports only UDP. Every SIP transaction that is sent over UDP is carried over a new UDP packet. The source port is random and difficult to move through the firewall, because the number of responses for a specific SIP request is not predetermined.

Currently two underlying media protocols are available: Real-Time Transport Protocol (RTP) or a combination of RTP and Real-Time Transport Control Protocol (RTCP) streams.

- *RTP*—UDP packet format and set of conventions that provide end-to-end network transport functions for transmitting real-time data, such as audio, video, or simulation data over multicast and unicast networks
- *RTCP*—The control protocol designed to work in conjunction with RTP; it is standardized in RFC 1889 and 1890; in an RTP session, participants periodically send RTCP packets to convey feedback on quality of data delivery and information of membership

SIP signaling requests can traverse directly between gateways or through a series of proxies to the destination gateway or phone. The responses to the signaling requests can take the same path as the request or be sent directly to the destination gateways. These require the firewall to intelligently understand SIP messages and subsequently open the appropriate pinholes.

ICMP Inspection

ICMP is a standard protocol with standard protocol number (STD) 5 that includes IP and Internet Group Management Protocol (IGMP).

ICMP reports errors and information about a network. It can report errors on any IP datagram other than on the ICMP message itself, to avoid infinite repetitions. ICMP also can actively debug a network environment. For example, the "ping" application is used to discover network connectivity to or from a particular host. Ping uses an ICMP echo and echo reply message to establish connectivity.

This created the need to allow responses to ICMP packets (such as ping and traceroute) that originated inside the Cisco IOS Firewall, while still denying other ICMP traffic. ICMP is invaluable to a network administrator in trying to debug network issues. Administrators use it to expose severed communications or existing packet paths, whereas intruders use ICMP to learn the topology of a private network. Network intruders also exploit existing weaknesses in certain ICMP implementations to damage the network site. One way to restrict invasions into a private network is to block ICMP messages from entering, although this is not a desirable approach.

To address the limitation of qualifying ICMP messages into the malicious or benign category, Cisco IOS Firewall uses stateful inspection to "trust" the ICMP messages generated within the private network, and to permit the associated ICMP replies. The firewall takes advantage of the existing architecture and user interface to inspect request and reply ICMP messages and allow ICMP traffic to flow. To complement the firewall inspection, ACLs can still allow unsolicited error messages. Table 2 lists message request types and their associated replies, which are inspected.

Table 2. Message Type Requests and Replies

Type	Name	Remarks
0	Echo reply	Reply to type 8
3	Destination unreachable	Reply to any type
8	Echo request	Request
11	Time exceeded	Reply to any type
13	Time-stamp request	Request
14	Time-stamp reply	Reply to type 13

Cisco IOS Firewall for IPv6

Customers in Europe, Asia, and the U.S. federal government view IPv6 as a way of negating today's address depletion issue; other advantages include a solution to the IPv4 address space issue. Because Cisco IOS Software supports dual IPv4 and IPv6 protocol stacks on the router, Cisco IOS Firewall also can inspect both simultaneously. The general trend is IPv6 tunneled over IPv4 (RFC 3056), better known as 6 to 4, as the first wave of endorsement. From the router perspective, there are scenarios in which both IPv4 and IPv6 networks sit behind a low-end router, creating the need for Cisco IOS Firewall to inspect IPv4 or IPv6 packets on one interface and to switch them out the other in the original IP version format or translate them while statefully inspecting the traffic.

Cisco IOS Firewall performs up to Layer 4 inspection (ICMP, UDP, and TCP), including IP fragment inspection of IPv6 packets. Simple TCP/IP applications, such as a Web browser and a Telnet client, also are supported. The following describes the Cisco IOS Firewall for IPv6 implementation:

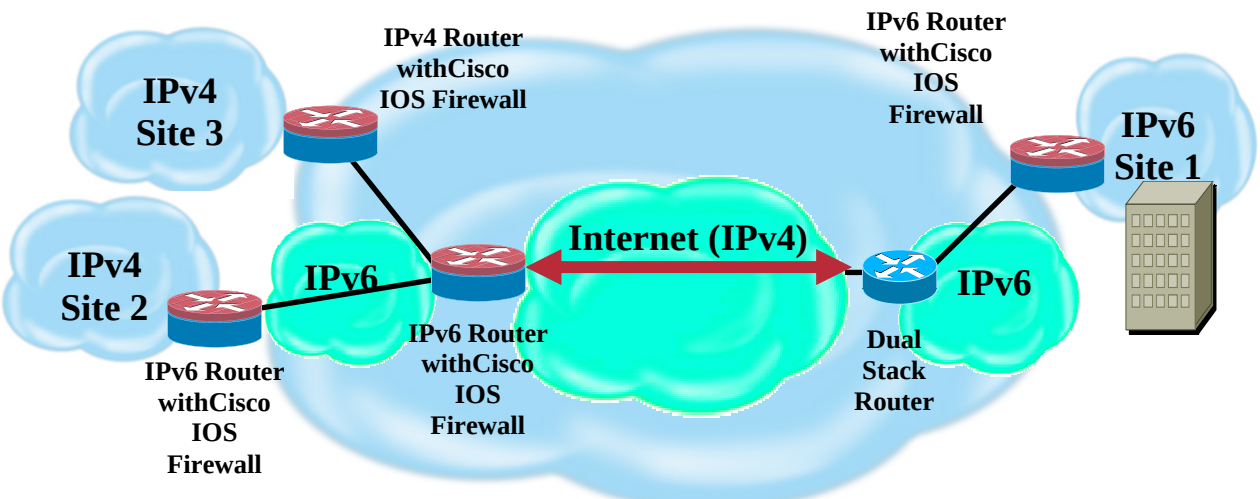
- Cisco IOS Firewall for IPv6 tracks TCP sequence numbers and drops packets not within the range.
- TCP firewall sessions are based on source and destination addresses, as well as source and destination ports.
- UDP connectionless inspection is a time-initiated filtering option. When a UDP packet is seen from the ingress interface, a Cisco IOS Firewall session is created to allow return traffic and is removed only when the specified idle timeout value is reached.
- UDP firewall sessions are based on source and destination addresses, as well as source and destination ports.
- Cisco IOS Firewall for IPv6 supports fragmented packets. The fragment header is used to trigger fragment processing. Cisco IOS Firewall virtual fragment reassembly (VFR) performs the following functions on fragments:
    - Examines out-of-sequence fragments and switches the packets in order
    - Examines the number of fragments from a single IP given a unique identifier (DoS attack)
    - Performs virtual reassembly to hand off to upper-layer protocols
- IPv6 DoS attack mitigation mechanisms are implemented in the same fashion as for the current IPv4 implementation; that is, SYN half-open connections.
- Tunnelled IPv6 packets destined for an IPv4 host are inspected by the Cisco IOS Firewall.
- ICMPv6 is used to inspect ICMP echo request and reply packets.

Table 3. Message Type Descriptions

Type value	Description
1	Destination unreachable
2	Packet too big
3	Time exceeded
4	Parameter problem
128	Echo request
129	Echo reply

Figure 1 depicts the various implementation scenarios and benefits that the customer can realize with Cisco IOS Firewall for IPv6.

Figure 1. Cisco IOS Firewall for IPv6



Cisco IOS Firewall for IPv6 helps the user implement Cisco IOS Firewall in both IPv4 and IPv6 networks. Additional benefits include:

- Provides stateful packet inspection of TCP, UDP, and ICMP sessions
- Coexists in IPv4 and IPv6 environments
- Provides the support of network attacks trying to exploit IPv4 and IPv6 fragments
- Provides stateful inspection of packets originating from the IPv4 network, terminating in an IPv6 environment by providing IPv4-to-IPv6 translation services
- Interprets or recognizes most IPv6 extension-header information, including routing header, hop-by-hop options header, and fragment header
- Supported on all dual IP stack routers

For additional information, visit:
http://cisco.com/en/US/products/sw/iosswrel/ps5207/prod_technical_documentation.html.

Transparent Cisco IOS Firewall

Transparent Cisco IOS Firewall simultaneously supports Layer 3 and Layer 2 firewalling capabilities for Cisco IOS Software routers. It minimizes deployment by removing the need to renumber statically addressed peripheral devices on the trusted network while providing protection of network assets by using a Layer 2 stateful packet inspection firewall.

Figure 2 shows a network without Transparent Cisco IOS Firewall. This is an example of a retail store environment in which wireless devices are statically addressed. They need to access the database, but the danger is that someone in the parking lot could potentially enter the network and access the corporate network with no challenge. This network is vulnerable to wireless-access-point intrusion.

Figure 2. Without Transparent Cisco IOS Firewall

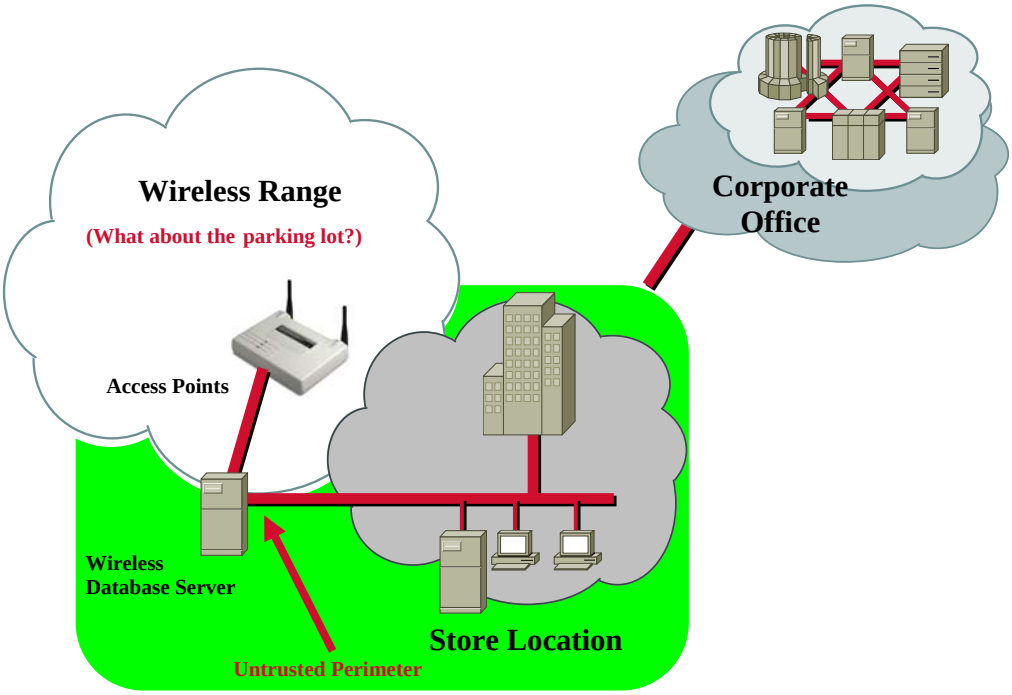
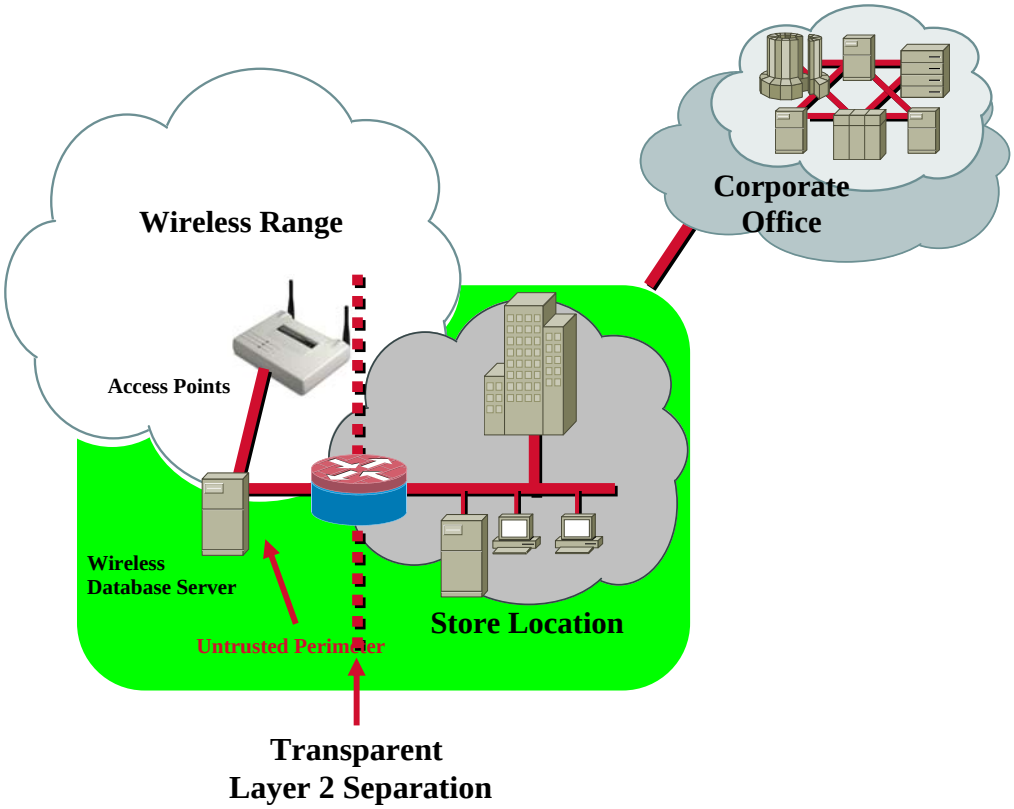


Figure 3 illustrates the effect of Transparent Cisco IOS Firewall on a network. If a hacker tries to compromise the wireless side of the network, Cisco IOS Firewall can block access while providing access to other devices. Admission can be accomplished by applying the appropriate Layer 2 MAC ACLs and Layer 3 IP ACLs.

Figure 3. With Transparent Cisco IOS Firewall



Transparent Cisco IOS Firewall is configured with Layer 3 firewall inspection rules using the **ip inspect** command. The **inspect in/out** command can be configured on any of the bridged interfaces for Layer 2 protection while also being configured on any LAN or serial interfaces to provide traditional Layer 3 protection. The transparent firewall operates on bridged packets, and the Layer 3 firewall continues to operate on routed packets.

Note the following caveats:

- Authentication proxy does not work for interfaces that have the Transparent Cisco IOS Firewall configured.
- The transparent firewall inspects only TCP, UDP, and ICMP traffic.
- Non-IP traffic is bridged without interference from the transparent firewall.
- The transparent firewall supports 802.1Q VLAN trunks.
- The transparent firewall does not support Inter-Switch Link (ISL) encapsulation. ISL VLANs work when subinterfaces are created and placed in the bridge group.

Transparent Cisco IOS Firewall benefits include the following:

- It offers the ability to insert a stateful Layer 2 firewall within an existing network.
- It eliminates the need to manually readdress previous statically defined devices, a tedious and resource-intensive task.

- Users can allow selected devices from a subnet to traverse the firewall while denying access to other devices on the same subnet.
- It provides both Layer 2 and Layer 3 firewall capabilities on the same router.
- Cisco IOS Software bridging supports any number of interfaces or subinterfaces in a bridge group.
- It supports multiple interfaces.

SMTP

The firewall inspects SMTP traffic by detecting and blocking known SMTP attacks or illegal commands. The Cisco IOS Firewall detects a limited number of SMTP attack signatures, as described in the following paragraph [IS THIS CORRECT? AVOID "below"]. When malicious SMTP activity is identified by the Cisco IOS Firewall, the connection is reset and a syslog message is generated indicating the protocol anomaly was found.

Cisco IOS Firewall SMTP inspection scans for a set of hard-coded attack signatures. As mentioned, the detection of a signature causes the Cisco IOS Firewall to raise an alert message and close the SMTP session. Table 4 lists the supported Cisco IOS Firewall SMTP signatures.

Table 4. Supported Cisco IOS Firewall SMTP Signatures

Signature	Description
Mail: bad rcpt	This triggers on any mail message with a "pipe" (|) symbol in the Recipient field.
Mail: bad from	This triggers on any mail message with a "pipe" (|) symbol in the From: field.
Mail: old attack	This triggers when **wiz** or **debug** commands are sent to the SMTP port.
Mail: decode	This triggers on any mail message with a ":decode@" in the header.
Majordomo	A bug in the Majordomo program allows remote users to execute arbitrary commands at the privilege level of the server.

ESMTP Support

Cisco IOS Firewall now supports the inspection of ESMTP by inspecting ESMTP commands for anomalies. The commands inspected include the AUTH, DATA, EHLO, ETRN, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML and VRFY commands. All others are considered anomalies.

Destination URL Policy Management

The Internet has been unexplored territory, with very few borders and rules that dictate traffic flow. In this age of cost cutting, it is important to carefully manage resources. It is critical to avoid productivity and bandwidth drains, which result from inappropriate Internet surfing in the workplace.

This area also has legal implications. Network administrators, human resource managers, and governmental agencies are asking for tools that restrict and control Internet access. Many companies, governmental agencies, and telecommuters are now aware that there are few regulations and tools to prohibit employees from browsing the Internet during business hours; similarly, there is little safety for children who surf the Internet at the library. The Cisco IOS Firewall can now offer a highly flexible management option that is tightly integrated with Cisco routers that are enabled with a firewall and use a more accurate database and scalability.

Destination URL policy management (or URL filtering or Internet management) uses specialized servers that have gained detailed knowledge of the Internet and have categorized many URLs. URLs fall into one of more than 80 categories, including gaming, pornography, MP3s, and freeware and shareware. The server is typically implemented somewhere in the enterprise or service provider network.

The system administrator makes the following decisions:

- Allowable URL categories
- Which users or groups can access the content
- When content can be accessed
- Additional content restrictions (for example, content is permitted by a time-based quota, with a warning message)
- If the filtering will be enforced or just monitored and stored in a database

The policy management process follows:
The CPE routers or the headend corporate gateway routers receive an HTTP request to a URL destination. They forward a query to the server with the requested URL destination. The server replies with a permit or deny to the router that is based on the eight different management options available in the server host (permit, deny, continue with exception, quota time, etc.). The router then replies to the user that the connection is denied or the router allows the connection.

Cisco has improved this process with two additional processes. Before the router queries the server, the router has the ability to maintain two locally configured permit or deny tables. These tables are locations or URLs where all users are always permitted access, or where all users can never receive access permission. If no entries or matches are found, the router checks its local cache to determine if the request has been made at an earlier time. If so, it studies the results.

- The Cisco IOS router can store a preconfigured table of always-permitted locations and always-denied locations. These locations are not complete URLs; they are strings that trigger the permit or deny action by the router directly, when there is a match.
- Next, if no matches are found, it looks in the local cache.
- The router forwards the connection to the desired URL destination but does not present the target host Webpage response until a permit or deny decision has been made.

For performance reasons the call is always processed. Connection requests are always forwarded to the desired URL destination if nothing triggers the local mechanisms. If the router has not received permission or denial by the time the destination URL replies with a Webpage, the router does not forward it and drops the page.

When the router does receive permission, the discarded Webpage is retransmitted. If the response from the server is denied, the router resets the connection to the destination URL and notifies the user of this denied access.

Websense Inc.
Websense Inc. (NASDAQ: WBSN) is the worldwide leader of employee Internet management (EIM) solutions. Websense Enterprise software enables businesses to monitor, report, and manage how their employees use the Internet. This supports an organization's efforts to improve employee productivity, conserve network bandwidth, and mitigate legal liability. Founded in 1994, the company serves more than 17,500 customers, ranging in size from 100-person firms to global-sized corporations.

Websense Enterprise integrates tightly with Cisco IOS Software, helping network administrators monitor and control network traffic. Running on a separate server, Websense Enterprise tells the router to block or permit outbound Internet requests based on flexible filtering policies configured within Websense. Websense Enterprise runs on Windows NT and 2000, Solaris, or Linux. Additional information is available at http://www.websense.com/,
by phone at 800 723-1166 or 858 320-8000, or fax at 858 458-2950.

N2N2 Inc.
N2H2 software solutions empower organizations of any size to control, manage, and understand their Internet use. N2H2's versatile Sentian filtering products help companies control costs by limiting potential legal liability, increasing productivity, and conserving bandwidth—delivering only the most relevant Web content. N2H2's Bess filtering products help teachers and parents protect children at school, and are the most trusted name in education for Internet content filtering. An independent study by the U.S. Department of Justice and eTesting Labs confirms what hundreds of N2H2 customers have known all along. The effectiveness of N2H2's filtering list received a Correct Blocking Ratio testing score of 98 percent.

Since 1995, N2H2's unique combination of powerful technology and expert human review has yielded the finest categorized database of Internet content. Comprising millions of entries, N2H2's categorized database is at the heart of every product and service that the company provides. N2H2 is a global Internet content-filtering company. N2H2 software helps customers control, manage, and understand their Internet use by filtering Web content, monitoring Internet access, and delivering concise reports on user activity. These safeguards enable organizations of any size to limit potential legal liability, increase user productivity, and optimize network bandwidth. N2H2's Bess and Sentian product lines are powered by N2H2's premium-quality filtering database—a list consistently recognized by independent and respected third parties as the most effective in the industry. Additional information is available at <http://www.n2h2.com> or by calling 206 336-1501 or 800 971-2622.

Authentication Proxy
Network administrators can create specific security policies for each user with Cisco IOS Firewall LAN-based, dynamic, per-user authentication and authorization. Previously, user identity and related authorized access was determined by a user's fixed IP address, or a single security policy had to be applied to an entire user group or subnet. Per-user policy can now be downloaded dynamically to the router from a TACACS+ or RADIUS authentication server using Cisco IOS Software AAA services.

Users can log into the network or onto the Internet with HTTP, and their specific access profiles are automatically downloaded. Appropriate dynamic individual access privileges are available as required, protecting the network against a more general policy that is applied across multiple users. Authentication

and authorization can be applied to the router interface in either direction to secure inbound or outbound extranet, intranet, and Internet usage.

HTTPS
Authentication proxy supports a secured channel for HTTP authentication by way of the Secure Sockets Layer (SSL). The Cisco implementation of HTTPS provides encryption between the client and Cisco IOS Software router during the username and password exchange. The HTTPS service uses SSL v3.0 and HTTP 1.1.

Authentication Proxy Accounting for HTTP
Accounting is a method for tracking the actions of a user or group of users. Accounting information typically consists of the user's action and the duration over which that action lasted. The accounting information is sent to accounting servers, where it is saved as a record.

System administrators use accounting information for security, billing, or resource allocation. The accounting provides start and stop record accounting with enough information to be used for billing or security auditing purposes. The addition of AAA accounting to the authentication proxy helps customers monitor the actions of users who use the authentication proxy service.

How did Cisco implement this firewall feature? When an authentication proxy cache and associated dynamic ACLs are created, the authentication proxy begins to track the traffic from the authenticated host. The AAA accounting saves data about this event. An accounting record (start record) may be generated at this time, if the accounting start option is enabled. A user command to view this data is also provided. When an authentication proxy cache is expired and deleted, additional data (for example, elapsed time) is added to the accounting information, and the stop record is always sent to the server. At this point, the information is deleted from the AAA accounting.

Authentication Proxy Accounting for Telnet and FTP
Authentication proxy supports Telnet- and FTP-type connections by intercepting traffic from FTP or Telnet hosts for user authentication and authorization. When Cisco IOS Firewall receives either an FTP or Telnet packet (port 21 or 23, respectively), it determines whether the user has already been authenticated. If the user has been authenticated, that user is allowed to communicate with the FTP or Telnet server. If the user has not been previously authenticated, authentication proxy challenges the user with a prompt for both a username and password request.

For the Telnet protocol, the login method involves two steps. First, the user is prompted to enter the proxy's username and password.

When the authentication succeeds, the destination server prompts the user again for the Telnet server username and password.

Logging in the FTP authentication proxy requires only one step. The Cisco IOS Firewall prompts the user for a username and password.

Authentication proxy verifies the user's profile against the AAA server user database. When authentication is complete, the Cisco IOS Firewall passes the FTP (remote) username and password on to the FTP destination or server for the application server authentication.

DoS Detection and Prevention

Enhanced DoS detection and prevention defends networks against popular attack modes, such as SYN (synchronize or start) flooding, port scans, and packet injection, by inspecting packet sequence numbers in TCP connections. If numbers are not within expected ranges, the router drops suspicious packets. When the router detects unusually high rates of new connections, it issues an alert message, and subsequently drops half-open TCP connection state tables. This prevents system resource depletion.

When the Cisco IOS Firewall detects a possible attack, it tracks user access by source or destination address and port pairs. It also details the transaction, creating an audit trail.

Multicast and Cisco IOS Firewall

Most firewall appliances support multicast by opening pinholes and tunneling the traffic through the device. The firewall appliance is not inspecting the traffic, but simply letting the traffic through the device. Because it is only tunneling the traffic, the firewall appliance is not participating in the multicast routing structure. Some appliances minimally support Protocol Independent Multicast (PIM) or sparse mode, which barely qualifies the device as a multicast participant. Multicast is fully supported on Cisco IOS Software routers that have enabled Cisco IOS Firewall.

Dynamic Port Mapping

Port address mapping (PAM) is a flexible, per-application port-mapping capability that allows Cisco IOS Firewall to support applications running on nonstandard ports. This feature allows network administrators to customize access control for specific applications and services in order to meet their distinct network needs.

Java Applet Blocking

With the proliferation of Java applets available on the Internet, protecting networks from malicious applets has become an important issue for network managers. The Java-blocking feature can be configured to filter or completely deny access to Java applets that are not embedded in archives or compressed in files.

VPN, IPSec Encryption, and QoS Support

When combined with Cisco IOS IPSec technology, the Cisco IOS Firewall provides integrated VPN functions. VPNs are developing rapidly to provide secure data transfer over public lines (such as the Internet); to reduce telecommunications and management costs for remote users, branch offices, and extranets; and to enhance QoS and reliability.

The Cisco IOS Firewall operates with Cisco IOS Software encryption, tunneling, and QoS features to secure VPNs. Network layer encryption capability prevents eavesdropping or tampering with data across a network during transmission. The Cisco IOS Firewall encrypts data for private communications over distrusted networks, employing IPSec encryption standards with both 56-bit (Data Encryption Standard [DES]), 168-bit (Triple DES [3DES]), and xxx-bit Advanced Encryption Standard (AES) methods.

For maximum interoperability, Cisco IOS Software supports multiple tunneling protocol standards, working with generic routing encapsulation (GRE), Layer 2 Forwarding (L2F), and L2TP. QoS functions classify traffic, manage congestion, and prioritize applications as needed.

Cisco IOS Firewall can be deployed with platforms that support Cisco VPN, specifically the Cisco 800, 1700, 2600, 3600, and 7000 series routers, which extend an existing network to virtual private networking. Cisco understands that VPN solutions must provide more than secure encrypted tunnels over public network facilities. They must also ensure timely and reliable delivery of data, and provide robust perimeter security for the corporate portal to the public network. The Cisco IOS Firewall, combined with a Cisco 7100 Series Router, for example, provides scalable encrypted tunnels, while integrating strong perimeter security, advanced bandwidth management, intrusion detection, and service-level validation.

The Cisco IOS Firewall authentication proxy feature also provides user authentication and authorization for Cisco VPN client software.

Configurable Real-Time Alerts, Audit Trail, and Event Logging

Real-time alerts send syslog error messages to central management consoles upon detecting suspicious activity, allowing network managers to respond immediately to intrusions. Enhanced audit-trail features use syslog to track all transactions, recording time stamps, source host, destination host, ports used, session duration, and the total number of transmitted bytes for advanced, session-based reporting.

Cisco IOS Firewall alerts and audit-trail features are now configurable, enabling more flexible reporting and error tracking. The configurable audit-trail features support modular tracking of specific firewall-supported applications and Java blocking. Both the real-time alerts and audit-trail features are supported by a variety of third-party reporting tools.

When a network event occurs, it generates an alert to the logging host through the Cisco IOS Software syslog mechanism. This allows administrators to track potential security breaches or other nonstandard activities in real time, by logging system error message output to a console terminal or syslog server, setting severity levels and recording other parameters.

PER-USER FIREWALL – CISCO DIFFERENTIATOR

Features that can be implemented on a per-subscriber basis are becoming increasingly important in today's broadband environment. Implementation of such features allows network service providers to use these features for revenue generation, in addition to the monthly access fee that broadband subscribers pay.

One feature that network service providers focus on is per-user firewalls. Broadband subscribers using firewalls generally are interested in protecting themselves from outsiders to their networks. Specifically, DoS attacks can be very common with broadband subscribers. Such attacks can harm client stations and, in some cases, subscriber modems.

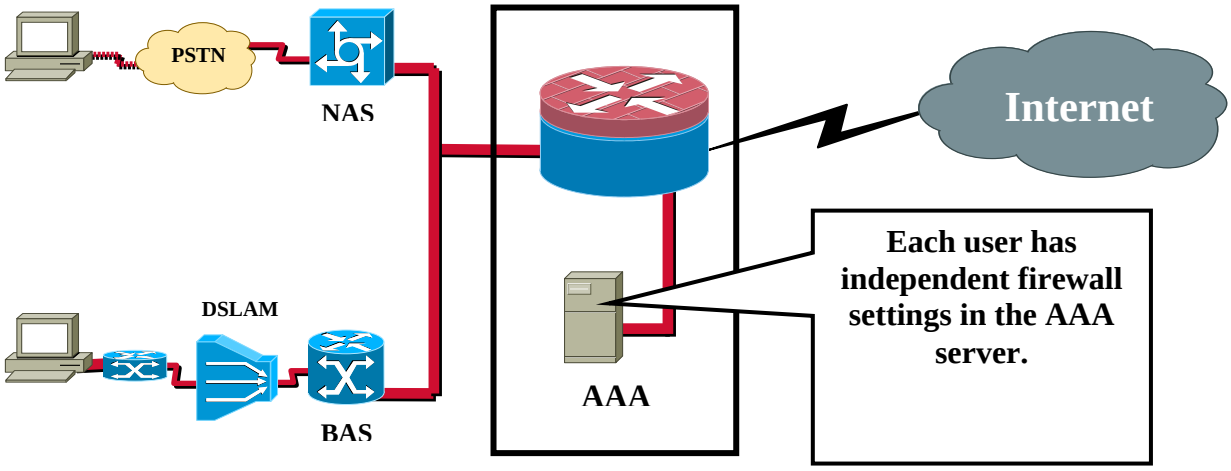
Cisco has a solution for broadband subscribers who wish to be protected from DoS attacks and other unsolicited intruders to their networks. Using the Cisco IOS Firewall, per-subscriber firewalls can be implemented on certain broadband aggregation platforms, such as the Cisco 7200, 7300, and 7400 series

routers. This solution does not require the broadband subscriber to own a firewall or understand its functions and configuration. Subscribers just want protection.

There are numerous different broadband aggregation architectures, resulting in different configurations on the Cisco 7200 and 7400 series routers. These include PPP over ATM (PPPoA), PPP over Ethernet (PPPoE), PPP in L2TP, routed bridge encapsulation (RBE), and 1483 routed ATM permanent virtual circuits (PVCs).

Figure 4 shows the network architecture.

Figure 4. Network Architecture



In the figure, the CPE is originating the PPPoX session. This is correct for PPPoA and can be appropriate for PPPoE; however, PPPoE is typically originated from a PC on the LAN off the CPE. This is DSL, so the DSL access multiplexer (DSLAM) is in this network diagram.

The AAA server authenticates users as they bring up their sessions. This portion of the architecture is very important, and the user is challenged for both user ID and password. The router makes an AAA query to the AAA server to authenticate and receive the network settings, ACL, and firewall settings.

If RFC 1483 routed PVCs were being used in the above configuration, the Cisco IOS Firewall would be applied on a per-virtual circuit (subinterface) basis. This is equally effective, assuming that:

- There is only one user on the virtual circuit.
- All users on the virtual circuit want the same Cisco IOS Firewall protection.

It is very important to understand that this example of deployment is just one scenario in which Cisco IOS Firewall can be used to implement per-user firewalls, a feature that is truly a Cisco differentiator.

NETWORK MANAGEMENT, CONFIGURATION, AND PROVISIONING

Cisco Security Device Manager

Cisco SDM is an intuitive, secure, Web-based device management tool embedded in Cisco 830, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800, and 7200 series routers and the Cisco 7301 Router. Smart wizards help enable users to quickly and easily deploy and manage a Cisco access router without knowledge of the Cisco IOS Software command-line interface (CLI). Cisco SDM offers smart wizards and advanced configuration support for LAN and WAN interfaces, NAT, stateful firewall, and IPSec VPN features. Cisco partners and customers can further fine-tune router configurations and preview the Cisco IOS Software CLI for each configuration. Cisco SDM also offers a one-step router lockdown and an innovative security auditing capability to check and recommend changes to router configurations based on ICSA Labs and Cisco Technical Assistance Center (TAC) recommendations.

Cisco SDM provides two interfaces into the Cisco IOS Firewall: smart wizards and advanced mode. Firewall smart wizards are further divided into basic and advanced firewall. Basic firewall implements a standard Cisco TAC-recommended prebuilt configuration template on user-specified interfaces; this wizard takes minimal input from the user. The advanced firewall wizard allows the user to create DMZs and customize the firewall inspection rules. Day-2 users can fine-tune their Cisco IOS Firewall configurations through the ACL and inspection rule editors in the advanced mode.

Both smart wizards and advanced mode account for parameters of the existing router configuration such as ACLs, NAT, routing protocols, IPSec rules, etc. and recommend the right firewall policy to the user. Users can choose to deliver the Cisco SDM-recommended firewall policy or fine-tune the configurations through editors. For example, if the WAN interface is configured as Dynamic Host Configuration Protocol (DHCP) client in a broadband router, Cisco SDM informs the user that it can adjust the firewall configuration to allow DHCP packets. The user has the option to implement the Cisco SDM-recommended configuration. These differentiating characteristics allow Cisco IOS Firewall to be highly integrated with Cisco routing infrastructure, thus reducing instances of onsite troubleshooting related to complex network and firewall integration issues.

For additional information, visit:
http://www.cisco.com/go/sdm/.

CiscoWorks VMS

CiscoWorks VMS, an integral part of the SAFE Blueprint from Cisco for enterprise network security, protects the productivity of organizations by combining Web-based tools for configuring, monitoring, and troubleshooting VPNs, firewalls, and network- and host-based intrusion detection systems (IDSs). CiscoWorks VMS delivers VPN configuration management, firewall management, surveillance, device inventory, and software version management features. CiscoWorks VMS supports Cisco 1700, 1800, 2600, 2800, 3600, 3700, 3800, 7100, and 7200 series routers and the Cisco 7301 Router for firewall management.

Cisco IP Solution Center 3.0

Cisco IP Solution Center (ISC) security management eliminates common deployment and management issues by elevating the technology administrator's role to that of business manager, as opposed to low-level, device-specific policy manager and administrator. Cisco ISC implements a business-centric, policy-level management model that allows customers to define high-level policies, while the application of those

policies to specific network devices is offloaded to the Cisco ISC software. The Cisco ISC Security Technology module provides full support for the provisioning and management of firewall, VPN, and QoS technologies over Cisco IOS Software-based routers, Cisco VPN 3000 Series concentrators, Cisco PIX Firewall devices, and Cisco Catalyst 6500 Series switches.

Cisco ISC offers full lifecycle management, from creating the security policy to real-time provisioning, service activation, service auditing, service assurance, and policy reconfiguration. Cisco ISC was designed to effectively accommodate the dynamic nature of security technologies, facilitating fast additions of devices, device upgrades or relocations, and other changes that allow customers to responsively address the needs of corporate clients. Designed for reliability, scalability, and flexibility, Cisco ISC uniquely helps enable customers to maintain security technologies with absolutely no service disruptions.

Third-Party Partners (optional)

Solsoft NP is a UNIX-based management tool that supports the Cisco IOS Firewall. It is a multivendor, multidevice, scalable management solution that allows users to visually define, deploy, enforce, and audit security policies from a central location. For more information, visit www.solsoft.com.

Cisco IOS Router and Firewall Provisioning

The Cisco CNS 2100 Series Intelligence Engine is a network device that provides an intelligent network interface to applications and users. Fully integrated with the Cisco Systems Configuration Express ordering solution and the company's new embedded agent technology, the Cisco CNS 2100 Series provides an end-to-end, hands-free deployment solution for Cisco CPE-based network services. The Cisco CNS 2100 Series is designed to deliver immediate productivity. It is a self-contained, 1-rack unit (RU), rack-mountable unit that requires minimal configuration and can be installed within minutes of opening the box. Because the Cisco CNS 2100 Series provides an intuitive, task-oriented user interface, network engineers can immediately begin automating routine deployment and configuration tasks with minimal training. The Cisco CNS 2100 Series also provides an open publish and subscribe XML interface for easy integration into existing operations-support-system (OSS) or workflow systems. This allows customers to immediately begin creating new service offerings or enhancing existing service offerings with new functions such as ready-to-use product deployment.

The Cisco CNS Flow-Through Provisioning feature provides the infrastructure for automated configuration of network devices on a mass scale. Based on the Cisco CNS event and configuration agents, this extra function facilitates the industry's first true "zero-touch" network deployment solution eliminating the need for the traditional technician involvement associated with initial device installation.

This Cisco IOS Software infrastructure interoperates with the Cisco CNS 2100 Series Intelligent Engine, creating the foundation for a closed-loop binding of the service provider's operational systems, business systems, and Cisco's order process into a single e-business solution. The result is the first automated workflow, which ranges from initial subscriber order entry through Cisco manufacturing and shipping to final device provisioning and subscriber billing. This focuses on a root problem of today's service provider business model—use of human labor in the mass-production process of subscriber service activation.

INTEGRATION WITH CISCO IOS SOFTWARE

The Cisco IOS Firewall is a security solution integrated into the network through Cisco IOS Software. A robust security policy entails more than perimeter control or firewall setup and management—security policy enforcement must be an inherent component of the network itself. Cisco IOS Software is an ideal vehicle for implementing a global security policy. Building an end-to-end Cisco solution allows managers to enforce security policies throughout network as they grow.

The Cisco IOS Firewall is also completely interoperable with Cisco IOS Software features, including NAT, VPN tunneling protocols, Cisco Express Forwarding, AAA extensions, Cisco encryption technology, and Cisco IOS IPSec.

Who Should Consider the Cisco IOS Firewall?

- Customers who need a one-box solution that combines powerful security, intrusion prevention, per-user authentication and authorization, VPN functions, and multiprotocol routing
- Customers interested in a cost-effective method of extending perimeter security across all network boundaries, specifically branch-office, intranet, and extranet perimeters
- SMBs looking for a cost-effective router with integrated firewall and intrusion-detection capabilities
- Service provider customers who want to deploy this as a router or firewall package for a managed service
- Customers who need additional security between network segments (such as between their organizations and a less-trusted partner site)
- Organizations with intranet connections where additional security is mandated
- Branch-office sites connecting to a corporate office or Internet
- Customers who are already familiar with Cisco IOS Software and do not want a separate firewall platform
- Customers who want to implement firewall protection throughout a network infrastructure to create a defense-in-depth environment

What About Cisco Support?

In addition to its industry-leading networking solutions, Cisco Systems is known for its world-class, end-to-end support solutions to help network managers support their local- or wide-area Cisco networks. The Cisco support product portfolio features startup, maintenance, and marketing support plus advanced and custom services to maximize and protect your investment. Updates for Cisco IOS Firewall are available at any time from Cisco.com, the Cisco award-winning Website.

AVAILABILITY AND PRICING

The Cisco IOS Firewall is available as a software image option for the Cisco 800 to Cisco 7500 series routers as well as the Cisco Catalyst 5000 and Catalyst 6000 series switches. Download the software image from the Cisco Website or request it on CD-ROM. For pricing information, contact your local Cisco sales office or Cisco reseller, or visit the Cisco Website at http://www.cisco.com.

FOR MORE INFORMATION

To find out more about Cisco IOS Software and the Cisco IOS Firewall, visit the Cisco Website at: http://www.cisco.com/go/firewall.