



STATEFUL INSPECTION FIREWALL FEATURES

Cisco® PIX® Security Appliances deliver advanced firewall services that protect enterprise networks from threats lurking on the Internet and in today's network environments. The state-of-the-art Cisco Adaptive Security Algorithm (ASA) provides rich stateful inspection firewall services, tracking the state of all authorized network communications and preventing unauthorized network access. Cisco ASA tracks the source and destination address, TCP sequence numbers, port numbers, and additional TCP flags. Cisco ASA applies the security policy to connection table entries, which house the information, and controls all inbound and outbound traffic. Access is permitted through a Cisco PIX Security Appliance only for connections that have been validated.

Cisco PIX Security Appliances deliver an additional layer of security through intelligent, "application-aware" security services that examine packet streams at Layers 4-7, using inspection engines specialized for many of today's popular applications, including HTTP, FTP, Simple Mail Transport Protocol (SMTP), H.323 Versions 1-4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), and Media Gateway Control Protocol (MGCP). Additionally, Cisco PIX Security Appliances can block Java, Javascript, and ActiveX applications. Administrators can easily create custom security policies for firewall traffic by using the flexible access control methods and the more than 100 predefined applications, services, and protocol support that Cisco PIX Security Appliances provide.

Cisco PIX Security Appliances provide "cut-through proxy" functionality for HTTP, HTTPS, FTP, and Telnet. Once a user has authenticated via one of these methods, network traffic from the user may begin to traverse the firewall. All subsequent traffic is still bound by firewall policies and is subject to inspection.

Cisco PIX Security Appliances also provide site-to-site and remote-access VPN services, enabling businesses to create secure connections across public networks. Data can be encrypted using Data Encryption Standard (DES), Triple DES (3DES), or Advanced Encryption Standard (AES). VPN connections can be authenticated using a variety of methods such as X.509 certificates, one-time passwords, and shared secrets.

INTRUSION DETECTION

Cisco PIX Security Appliances provide real-time, in-line monitoring, interception, and response to network misuse through broad support for the most common attack intrusion detection signatures. These intrusion detection capabilities enhance the Cisco PIX Security Appliance's best-of-breed stateful inspection firewall features by providing an additional layer of network protection. Appropriate action can be taken on packets and traffic flows that violate a security policy or represent malicious network activity.

The in-line intrusion detection capabilities provide real-time traffic analysis and customized responses by type of attack. This real-time

analysis and detection of unauthorized activity enables administrators to quickly respond to network security issues. The intrusion detection capabilities operate as an in-line sensor for deep packet inspection of network traffic as they travel through the Cisco PIX device's interfaces. Network traffic is analyzed in real time against a database of more than 55 common attack signatures that investigate policy violations or patterns of misuse. Using this wealth of advanced intrusion-detection features, including DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify, and TCP intercept, Cisco PIX Security Appliances keep a vigilant watch for attacks. Additionally, Cisco PIX Security Appliances support virtual packet reassembly, searching for attacks that are hidden over a series of fragmented packets.

Upon attack detection, the Cisco PIX Security Appliance's response is fully customizable. Alarms may be sent to administrators or to a management console in real time, with the ability to customize the severity level of the alarm based on the type of attack—providing administrators with tremendous flexibility and control. In addition to sending alarms, Cisco PIX Security Appliances can be configured to respond to attacks by dropping all traffic from the attack source or sending out TCP-reset packets to break any established connections from the attack source.

The in-line intrusion detection capabilities found in Cisco PIX Security Appliances complement the Cisco Intrusion Detection System (IDS) Appliance family. The strong integration between Cisco IDS appliances and Cisco PIX Security Appliances enables the Cisco PIX device to automatically block all network traffic from network nodes that the IDS appliances have designated as hostile

URL FILTERING

URL filtering is the ability to restrict or monitor access to Websites that may contain sensitive information. URL filtering is provided on Cisco PIX devices through integration with Cisco AVVID (Architecture for Voice, Video and Integrated Data) partners Websense Enterprise and N2H2 Sentian URL filtering server solutions. Cisco PIX Security Appliances check inbound or outbound URL requests with the policies defined on either Websense- or N2H2-based filtering solutions, and will either permit connections to occur or block connections and display a custom error message to an end user. Additional integration with Cisco AVVID partner Websense supports the filtering of HTTPS and FTP Web requests.

URL filtering helps to provide increased levels of employee productivity, reduced network bandwidth requirements, and the mitigation of potential legal liability related to inappropriate Web surfing.

URL filtering delivers the following benefits:

- Protection against malicious programs—N2H2 and Websense both categorize URLs (MP3 or freeware/shareware, for example). This reduces the risk of nonstandard or malicious programs, such as worms, from entering the network.

- Reduction of misuse of company resources—URL categorization allows network administrators, corporate managers, and government agencies to restrict and control Internet access, based on multiple factors, including e-mail address and user ID.

MANAGEMENT

Cisco PIX Device Manager

Many security vulnerabilities are caused by poor configuration. Consequently, implementing security policy must be as straightforward as possible. Cisco PIX Device Manager includes wizards, point-and-click configuration, and online help to simplify administration. Cisco PIX Device Manager also provides a table showing exactly what traffic is permitted or denied between a source and destination, so that security professionals can focus on enforcing security and defining policy, rather than on mastering the tools required to get the job done.

Cisco PIX Device Manager offers robust reporting and monitoring tools that provide real-time and historical insights into usage trends, performance baselines, and security events. At a glance, administrators can view graphical reports or tables summarizing network activity, resource utilization, and event logs, allowing performance and trend analysis.

- Cisco PIX Device Manager's monitoring tools create graphical summary reports showing real-time usage, security events, and network activity. Data from each graph can be displayed in increments you select—10-second snapshot, last 10 minutes, last 60 minutes, last 12 hours, last 5 days. The ability to view multiple graphs simultaneously allows you to do side-by-side analysis.
- System graphs—Provide detailed status information on the Cisco PIX device, including blocks used and free, current memory utilization, and CPU utilization.
- Connection graphs—Track real-time session and performance monitoring data for connections; address translations; authentication, authorization, and accounting (AAA) transactions; URL filtering requests; and more, on a per-second basis. Stay fully informed of your network connections and activities, without being overwhelmed.
- Intrusion detection (IDS)—16 different graphs are available to display potentially malicious activity. IDS-based signature information displays activity such as IP attacks, Internet Control Message Protocol (ICMP) requests, and Portmap requests.
- Interface graphs—Provide real-time monitoring of your bandwidth usage for each interface. Bandwidth usage is displayed for incoming and outgoing communications. You can view packet rates, counts, and errors, as well as bit, byte, and collision counts, and more.
- Cisco PIX Device Manager's integrated syslog viewer allows you to view specific syslog message types by selecting the desired logging level.

Access Control Lists (ACLs)

An important part of any device used for threat defense is its management capabilities. For Cisco PIX Security Appliances, the following features streamline and enhance the ability to manage the ACLs, which are very important in determining what traffic is allowed to pass through the network.

- SYSLOG by ACL introduces powerful new reporting and troubleshooting capabilities that enable detailed statistics to be gathered on which ACL entries are triggered by network traffic attempting to traverse a Cisco PIX Security Appliance.
- Object grouping enables administrators to group network objects (such as devices, networks, and services) into logical groups to greatly simplify access control rule definition and maintenance.
- Dynamic ACL via Cisco Secure ACS supports dynamic downloading and enforcement of ACLs on a per-user basis, upon user authentication with the firewall.
- ACL editing provides capabilities for inserting and deleting individual ACL entries without deleting and recreating the entire ACL.

Customizable Administrative Roles

- Command-level authorization enables businesses to create up to sixteen customizable administrative roles and profiles for accessing Cisco PIX Security Appliances (for example, monitoring only, read-only access to configuration, VPN administrator, or firewall administrator). These customizable roles are available in both the Cisco PIX Device Manager and the command-line interface (CLI).
- Access to network resources can also be strongly authenticated through the Cisco PIX Security Appliance's local user database or through integration with enterprise databases, either directly using TACACS+/RADIUS or indirectly with Cisco Secure ACS.

Customizable Syslog

- Custom logging identifier allows a custom firewall identifier to be selected, such as an interface IP address, that will be included in all syslog messages to improve the centralized reporting of firewall events.

Large-Scale Management Solutions

The Cisco VPN/Security Management Solution (VMS) suite consists of several network management modules, including Management Center for Firewalls, Auto Update Server Software, and Security Monitor. These solutions provide a scalable, three-tier management infrastructure for managing up to 1000 remote Cisco PIX Security Appliances from a single server. The web-based management GUI gives administrators the ability to group appliances for simplified configuration and software image management. These solutions also provide enterprise change management, role-based administrative access, and auditing features. Other Cisco PIX Security Appliance management solutions are available, such as IP Solution Center, which are targeted at service provider environments for service and configuration management, with flexible APIs that enable integration into service provider proprietary fault, configuration, accounting, performance, and security (FCAPS) environments.