

Cisco PIX[®] Device Manager



Overview

Cisco PIX Device Manager (PDM) offers enterprise and service provider users the features they need to easily manage Cisco PIX Firewalls. It features an intuitive graphical user interface (GUI) to help you set up and configure your PIX Firewall. In addition, a wide range of informative, real-time, and historical reports provide critical insight into usage trends, performance baselines, and security events. Secure communication allows efficient management of local or remote Cisco PIX Firewalls. In short, PDM simplifies Internet security, making it a cost-effective tool that enhances productivity and network security saving both time and money.

Intuitive User Interface

Many security vulnerabilities are caused by poor configuration. Consequently, implementing security policy must be as straightforward as possible. PDM includes wizards, point-and-click configuration, and online help to simplify administration. Security professionals can focus on enforcing security and defining policy, rather than on mastering the tools required to get the job done.

Wizard

PIX Device Manager offers a helpful wizard for setting up a new PIX deployment. With just a few steps, the PDM Setup Wizard enables you to efficiently create a basic configuration that allows packets to flow through the PIX Firewall from the inside network to the outside network securely.

You can also perform optional tasks such as configuring rules to allow outside access to your Web or mail server. After you complete initial setup, intuitive pull-down menus and icons enable you to easily add and delete services and rules, as well as access other feature settings.

Graphical User Interface

Using Cisco PIX Device Manager, you can easily configure, manage, and monitor security policies across your network. PDM's Graphical User Interface (GUI) provides a familiar tabbed layout with one-click access to common tasks. The point-and-click design is simple for even novice users, reducing ramp-up time. The result is cost savings through significant reductions in management time and maximum efficiency in network security management.

Monitoring and Reporting

PDM offers robust reporting and monitoring tools that provide you with real-time and historical insights. At a glance, administrators can view graphical reports summarizing network activity, resource utilization, and event logs, allowing performance and trend analysis. PDM's logging and notification features allow security staff to detect and interrupt suspicious activity.

Graphing Tools

Cisco PDM 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) and refreshed at user-defined intervals. The ability to view multiple graphs simultaneously allows you to do side-by-side analysis.

System graphs: Provide detailed status information on the PIX Firewall, 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 System (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.

Syslog Viewer

Cisco PDM's integrated syslog viewer allows you to view specific syslog message types by selecting the desired logging level.

Embedded Architecture

The embedded design of PDM allows customers to manage their Cisco PIX firewalls from almost any computer, regardless of their operating system, - which is a critical requirement for many of today's e-businesses. Similarly, PDM provides a consistent experience by working with most of today's popular browsers, including Microsoft Internet Explorer and Netscape Navigator. With PDM, there is no application to install and no plug-in required. An authorized network administrator can securely manage and monitor their PIX firewalls from a Web browser.

Secure Communication

Cisco PDM supports the Secure Socket Layer (SSL) protocol to provide high-grade encryption from the PIX Firewall to a browser. Your PIX Firewall, combined with 56-bit Data Encryption Standard (DES) or the more secure 168-bit Triple DES (3DES), ensures that communication with remote PIX Firewalls is secure.

Similar to Telnet usage, PDM enables you to protect access with a valid username and password. This can either be on the PIX Firewall or through an authentication server.

Licensing

Cisco PIX Device Manager is included as part of Cisco PIX operating systems version 6.0 and higher. A separate license for PDM is not required. A DES or 3DES license is required, as PDM only supports encrypted communication. If your PIX is not currently encryption enabled you can request a free DES activation key by completing the following form:

<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324>

3DES keys are available as part of a feature license upgrade.

Technical Specifications

PIX Firewall System Requirements

Hardware

Platform: Cisco PIX Firewall 506, 515, 520, 525, or 535

Random Access Memory: 32 MB

Flash Memory: 16 MB (PIX Firewall 506 requires 8 MB)

Software

PIX Firewall operating system: Version 6.0 or higher

Encryption: DES or 3DES-enabled

User System Requirements

Hardware

Processor: 300 MHz, 500 MHz recommended

Random Access Memory: 128 MB, 192 MB recommended

Display Resolution: 800 x 600 pixels, 1024 x 768 pixels recommended

Display Colors: 256, 256 color recommended

Software

Operating Systems	Browsers
Windows 2000 (Service Pack 1) Windows NT 4.0 (Service Pack 6a) Windows 98 (original or 2nd edition)	MS Internet Explorer 5.01 (Service Pack1) or higher (5.5 recommended) Netscape Communicator 4.51 or higher (4.76 recommended)
Windows NT 4.0 (Service Pack 6a)	Windows 98 (original or 2nd edition)
Sun Solaris 2.6 or 2.8 running CDE or Open Windows window manager	Redhat Linux 6.2 or 7.0 running GNOME or KDE 2.0 desktop environment
Redhat Linux 6.2 or 7.0 running GNOME or KDE 2.0 desktop environment	Netscape Communicator 4.76

Network Connection

Connection speed: 56 Kbps, 128 Kbps recommended

Additional Information

For more information about Cisco PIX Firewall, go to <http://www.cisco.com/go/pix>



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

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco.com Web site at www.cisco.com/go/offices.

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

Copyright © 2001 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0104R)