

Cisco PIX Device Manager Version 2.0

Overview

Cisco PIX[®] Device Manager (PDM) is a feature-rich, graphical tool providing enterprise and service providers with an easy-to-use management facility for Cisco PIX Firewalls. As part of the Cisco PIX operating system, it features an intuitive graphical user interface (GUI) with integrated online help and intelligent wizards to greatly simplify setting up and configuring your Cisco 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. Administrative and device security is assured through user passwords—with optional authentication via a Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS) server—and encrypted communications to the local or remote Cisco PIX Firewall. In short, Cisco PIX Device Manager simplifies the configuration, operation, and monitoring of Cisco PIX firewalls, making it a highly effective productivity tool for managing network security—saving both time and money.

Cisco PIX Device Manager Version 2.0 provides easy access to virtually all of the Cisco PIX Firewall functionality available in PIX OS Version 6.2. PDM v2.0 extends its firewall management capabilities with new simplified rule definitions, takes

advantage of new object grouping functionality for simplified application of rules, and includes support for more than 20 new features available in Cisco PIX Firewall Software Version 6.2. Cisco PIX Device Manager Version 2.0 also adds the ability to configure and monitor virtual private network (VPN) features through a point-and-click interface, simplifying the deployment of site-to-site or remote-access VPNs.

Intuitive User Interface

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 so that security professionals can focus on enforcing security and defining policy, rather than on mastering the tools required to get the job done.

Wizards

Startup Wizard

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



optional tasks such as configuring interface parameters, Easy VPN Remote, Auto Update, Network Address Translation/Port Address Translation (NAT/PAT), and Dynamic Host Control Protocol (DHCP) server settings. After you complete the 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.

VPN Wizard

Cisco PIX Device Manager's VPN Wizard can help you easily create VPN policy with step-by-step configuration and policy application. It can create site-to-site VPNs that securely connect a Cisco PIX Firewall to another VPN device, or remote-access VPNs (including hardware clients) that securely connect mobile users and telecommuters to a Cisco PIX Firewall.

GUI

Using Cisco PIX Device Manager, you can easily configure, manage, and monitor security policies across your network. The Cisco PIX Device Manager'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.

Object Grouping

To simplify your configuration, object grouping is supported in Cisco PIX Device Manager Version 2.0. Object grouping enables you to define groups of objects such as hosts, IP addresses, or network services. You can use these groups, for example, when you create and apply access rules. When you include a Cisco PIX Firewall object group in a PIX Firewall command, it is the equivalent of applying every element of the object group to the PIX Firewall command.

Cisco PIX Firewall Software Version 6.2 Feature Support

Cisco PIX Device Manager Version 2.0 gives you point-and-click access to virtually every feature available in this feature-packed Cisco PIX Firewall Software release. Bi-directional NAT, LAN-based failover, Easy VPN Remote, stub multicast routing, Point-to-Point Protocol over Ethernet (PPPoE), turbo access control list (ACL), and many more features are all fully integrated into the rich graphical environment of Cisco PIX Device Manager, simplifying overall systems management.

Monitoring and Reporting

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



Monitoring Tools

Cisco PIX Device Manager 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, the last 10 minutes, the last 60 minutes, the last 12 hours, or the last five days, for example) and refreshed at user-defined intervals. The ability to view multiple graphs simultaneously allows you to perform side-by-side analysis. The monitoring tools include:

- *System graphs*—Provide detailed status information on the Cisco 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. You can stay fully informed of your network connections and activities, without being overwhelmed.
- *Intrusion Detection System (IDS)*—Offers 16 different graphs 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.
- *VPN Statistics and Connection Graphs*—Display detailed information and counters for Internet Key Exchange (IKE) and IP Security (IPSec) security associations (SA), as well as Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP) VPN. You can use the VPN connection graphs to get a real-time graphical view of VPN performance statistics.

Syslog Viewer

The integrated Cisco PIX Device Manager syslog viewer allows you to view specific syslog message types by selecting the desired logging level.

Embedded Architecture

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

Secure Communication

Cisco PIX Device Manager supports the Secure Sockets Layer (SSL) protocol, providing high-grade encryption from the PIX Firewall to a browser. Your Cisco 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, Cisco PIX Device Manager enables you to protect access with a valid user name and password. This can be done either on the Cisco PIX Firewall or through an authentication server.



Licensing

Cisco PIX Device Manager Version 2.0 is included as part of Cisco PIX OS Version 6.2 and higher (Version 1.x is included with Cisco PIX Firewall Software Version 6.0 and higher). A separate license for Cisco PIX Device Manager is not required. A DES or 3DES license is required. If your Cisco PIX Firewall is not currently encryption enabled, you can request a free DES activation key by completing the following form:

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

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

Technical Specifications

Cisco PIX Firewall System Requirements

Hardware

Platform: Cisco PIX 501, 506/506E, 515/515E, 520, 525, or 535 Firewalls

Random Access Memory: 32 MB

Flash Memory: 16 MB (Cisco PIX 501 and 506/506E Firewalls require 8 MB)

Software

Cisco PIX Firewall Software: Version 6.2 (Cisco PIX Device Manager Version 1.x requires Cisco PIX Firewall Software Version 6.0 or 6.1)

Encryption: DES or 3DES-enabled

User System Requirements

Hardware

Processor: 350 MHz, 500 MHz recommended

Random Access Memory: 128 MB, 192 MB recommended

Display Resolution: 800x600 pixels, 1024x768 pixels recommended

Display Colors: 256, high color (16-bit) recommended

Software

Operating Systems	Browsers
Windows 2000 (Service Pack 1) Windows NT 4.0 (Service Pack 6a) Windows 98 (original or 2nd edition) Windows ME Windows XP	Microsoft Internet Explorer 5.01 (Service Pack 1) or higher (5.5 recommended), JDK v1.1.4 Netscape Communicator 4.5x or 4.7x
Sun Solaris 2.6 or higher running CDE or OpenWindows window manager on SPARC microprocessor	Netscape Communicator 4.5x or 4.7x
Red Hat Linux 7.0, 7.1, or 7.2 running GNOME or KDE 2.0 desktop environment	Netscape Communicator 4.7x

Network Connection

Connection Speed: 56 kbps, 384 kbps recommended

Additional Information

For more information about Cisco PIX Firewall and Cisco PIX Device Manager, visit:

<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 International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

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, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • 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

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks or trademarks of trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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.
(0208R) LW3780 10/02