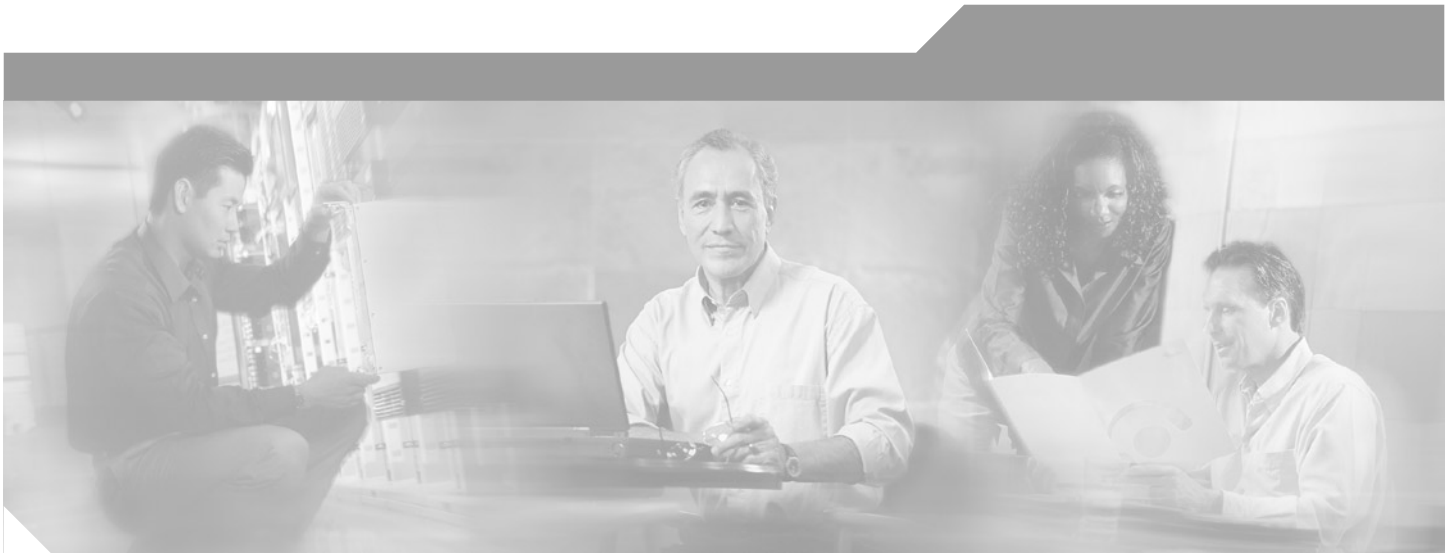

Cisco PIX Device Manager Installation Guide

Version 3.0

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

Text Part Number: 78-15483-01

This document is to be used in conjunction with the appropriate documentation for your Cisco PIX Firewall system.

Cisco PIX Device Manager Installation Guide

Preface

This preface includes the following sections:

Document Objectives

This guide describes how to install and access the Cisco PIX Device Manager (PDM) software.

Audience

This guide is for network administrators who perform the following:

- Manage network security
- Install and configure firewalls

Installation Warning

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Waarschuwing **Deze apparatuur mag alleen worden geïnstalleerd, vervangen of hersteld door bevoegd geschoold personeel.**

Varoitus **Tämän laitteen saa asentaa, vaihtaa tai huoltaa ainoastaan koulutettu ja laitteen tunteva henkilökunta.**

Attention **Il est vivement recommandé de confier l'installation, le remplacement et la maintenance de ces équipements à des personnels qualifiés et expérimentés.**

Warnung **Das Installieren, Ersetzen oder Bedienen dieser Ausrüstung sollte nur geschultem, qualifiziertem Personal gestattet werden.**

Figyelem! **A berendezést csak szakképzett személyek helyezhetik üzembe, cserélhetik és tarthatják karban.**

Avvertenza **Questo apparato può essere installato, sostituito o mantenuto unicamente da un personale competente.**

Advarsel **Bare opplært og kvalifisert personell skal foreta installasjoner, utskiftninger eller service på dette utstyret.**

Aviso **Apenas pessoal treinado e qualificado deve ser autorizado a instalar, substituir ou fazer a revisão deste equipamento.**

¡Advertencia! **Solamente el personal calificado debe instalar, reemplazar o utilizar este equipo.**

Varning! **Endast utbildad och kvalificerad personal bör få tillåtelse att installera, byta ut eller reparera denna utrustning.**

Предупреждение Установку, замену и обслуживание этого оборудования может осуществлять только специально обученный квалифицированный персонал.

警告 只有经过培训且具有资格的人员才能进行此设备的安装、更换和维修。

警告 この装置の設置、交換、保守は、訓練を受けた相応の資格のある人が行ってください。

Safety Warning Description

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the translated safety warnings that accompanied this device.

Note: SAVE THESE INSTRUCTIONS

Note: This documentation is to be used in conjunction with the specific product installation guide that shipped with the product. Please refer to the Installation Guide, Configuration Guide, or other enclosed additional documentation for further details.

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Voor een vertaling van de waarschuwingen die in deze publicatie verschijnen, dient u de vertaalde veiligheidswaarschuwingen te raadplegen die bij dit apparaat worden geleverd.

Opmerking BEWAAR DEZE INSTRUCTIES.

Opmerking Deze documentatie dient gebruikt te worden in combinatie met de installatiehandleiding voor het specifieke product die bij het product wordt geleverd. Raadpleeg de installatiehandleiding, configuratiehandleiding of andere verdere ingesloten documentatie voor meer informatie.

Varoitus **TÄRKEITÄ TURVALLISUUTEEN LIITTYVIÄ OHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä asiakirjassa esitettyjen varoitusten käännökset löydät laitteen mukana toimitetuista ohjeista.

Huomautus SÄILYTÄ NÄMÄ OHJEET

Huomautus Tämä asiakirja on tarkoitettu käytettäväksi yhdessä tuotteen mukana tulleen asennusoppaan kanssa. Katso lisätietoja asennusoppaasta, kokoonpano-oppaasta ja muista mukana toimitetuista asiakirjoista.

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez les consignes de sécurité traduites qui accompagnent cet appareil.

Remarque CONSERVEZ CES INFORMATIONS

Remarque Cette documentation doit être utilisée avec le guide spécifique d'installation du produit qui accompagne ce dernier. Veuillez vous reporter au Guide d'installation, au Guide de configuration, ou à toute autre documentation jointe pour de plus amples renseignements.

Warnung **WICHTIGE SICHERHEITSANWEISUNGEN**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewusst. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise sind im Lieferumfang des Geräts enthalten.

Hinweis BEWAHREN SIE DIESE SICHERHEITSANWEISUNGEN AUF

Hinweis Dieses Handbuch ist zum Gebrauch in Verbindung mit dem Installationshandbuch für Ihr Gerät bestimmt, das dem Gerät beiliegt. Entnehmen Sie bitte alle weiteren Informationen dem Handbuch (Installations- oder Konfigurationshandbuch o. Ä.) für Ihr spezifisches Gerät.

Figyelem! **FONTOS BIZTONSÁGI ELÕÍRÁSOK**

Ez a figyelmezetõ jel veszélyre utal. Sérülésveszélyt rejtõ helyzetben van. Mielõtt bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplõ figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található.

Megjegyzés ÕRIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Megjegyzés Ezt a dokumentációt a készülékhez mellékelt üzembe helyezési útmutatóval együtt kell használni. További tudnivalók a mellékelt Üzembe helyezési útmutatóban (Installation Guide), Konfigurációs útmutatóban (Configuration Guide) vagy más dokumentumban találhatók.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Per le traduzioni delle avvertenze riportate in questo documento, vedere le avvertenze di sicurezza che accompagnano questo dispositivo.

Nota CONSERVARE QUESTE ISTRUZIONI

Nota La presente documentazione va usata congiuntamente alla guida di installazione specifica spedita con il prodotto. Per maggiori informazioni, consultare la Guida all'installazione, la Guida alla configurazione o altra documentazione acclusa.

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette varselssymbolet betyr fare. Du befinner deg i en situasjon som kan forårsake personskade. Før du utfører arbeid med utstyret, bør du være oppmerksom på farene som er forbundet med elektriske kretssystemer, og du bør være kjent med vanlig praksis for å unngå ulykker. For å se oversettelser av advarslene i denne publikasjonen, se de oversatte sikkerhetsvarslene som følger med denne enheten.

Merk TA VARE PÅ DISSE INSTRUKSJONENE

Merk Denne dokumentasjonen skal brukes i forbindelse med den spesifikke installasjonsveiledningen som fulgte med produktet. Vennligst se installasjonsveiledningen, konfigureringsveiledningen eller annen vedlagt tilleggsdokumentasjon for detaljer.

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. O utilizador encontra-se numa situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha em atenção os perigos envolvidos no manuseamento de circuitos eléctricos e familiarize-se com as práticas habituais de prevenção de acidentes. Para ver traduções dos avisos incluídos nesta publicação, consulte os avisos de segurança traduzidos que acompanham este dispositivo.

Nota GUARDE ESTAS INSTRUÇÕES

Nota Esta documentação destina-se a ser utilizada em conjunto com o manual de instalação incluído com o produto específico. Consulte o manual de instalação, o manual de configuração ou outra documentação adicional inclusa, para obter mais informações.

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Vea las traducciones de las advertencias que acompañan a este dispositivo.

Nota GUARDE ESTAS INSTRUCCIONES

Nota Esta documentación está pensada para ser utilizada con la guía de instalación del producto que lo acompaña. Si necesita más detalles, consulte la Guía de instalación, la Guía de configuración o cualquier documentación adicional adjunta.

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Se översättningarna av de varningsmeddelanden som finns i denna publikation, och se de översatta säkerhetsvarningarna som medföljer denna anordning.

OBS! SPARA DESSA ANVISNINGAR

OBS! Denna dokumentation ska användas i samband med den specifika produktinstallationshandbok som medföljde produkten. Se installationshandboken, konfigurationshandboken eller annan bifogad ytterligare dokumentation för närmare detaljer.

Предупреждение ВАЖНЫЕ СВЕДЕНИЯ ПО БЕЗОПАСНОСТИ

Этот символ предупреждает о наличии опасности. При неправильных действиях возможно получение травм. Перед началом работы с любым оборудованием необходимо ознакомиться с ситуациями, в которых возможно поражение электротоком, и со стандартными действиями для предотвращения несчастных случаев. Переведенный текст предупреждений содержится в соответствующем документе, поставляемом вместе с устройством.

Примечание СОХРАНЯЙТЕ ЭТУ ИНСТРУКЦИЮ
Примечание Эта инструкция должна использоваться вместе с руководством по установке конкретного изделия, входящим в комплект поставки. Дополнительные сведения см. в руководстве по установке, руководстве по настройке и другой документации, поставляемой с изделием.

警告 有关安全的重要说明

这个警告符号指有危险。您所处的环境可能使身体受伤。操作设备前必须意识到电流的危险性，务必熟悉操作标准，以防发生事故。如果需要了解本说明中出现的警告符号的译文，请参阅本装置所附之安全警告译文。

注意 保存这些说明
注意 本文件应与本产品附带的具体安装说明一并阅读。如欲了解详情，请参阅《安装说明》、《配置说明》或所附的其他文件。

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。このマニュアルに記載されている警告の各国語版は、装置に付属の「Translated Safety Warnings」を参照してください。

注 これらの注意事項を保管しておいてください。
注 この資料は、製品に付属のインストレーション ガイドと併用してください。詳細は、インストレーション ガイド、コンフィギュレーション ガイド、または添付されているその他のマニュアルを参照してください。

Document Organization

The major sections of this guide are as follows:

Chapter	Title	Description
1	Overview	Physical properties and functional overview of the Cisco PIX Device Manager (PDM) Version 3.0
2	Preparing to Install PDM	Preparations and other requirements before installing the PIX Firewall
3	Installing PDM	Installing the hardware and connecting the external network interface cables
4	Configuring PDM	Configuring PDM, using the PDM Wizard, including VPN Wizard and configuration recommendations
5	Tips and Troubleshooting	Basic troubleshooting procedures for the hardware installation
A	Using a TFTP Server	How to use a TFTP server to access PIX Firewall or PDM images

Document Conventions

Command descriptions use these conventions:

- Braces ({ }) indicate a required choice.
- Square brackets ([ ]) indicate optional elements.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Boldface indicates commands and keywords that are entered literally as shown.
- Italics indicate arguments for which you supply values.

Examples use these conventions:

- Examples depict screen displays and the command line in `screen` font.
- Information you need to enter in examples is shown in **`boldface screen`** font.
- Variables for which you must supply a value are shown in *`italic screen`* font.

Graphic user interface access uses these conventions:

- Boldface indicates buttons and menu items.
- Selecting a menu item (or screen) is indicated by the following convention:

  Click **Start >Settings>Control Panel**.

Notes, cautionary statements, and safety warnings use these conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

Terms and Acronyms

To fully understand the content of this user guide, you should be familiar with the following terms and acronyms:

- AAA—authentication, authorization, and accounting
- AES— Advanced Encryption Standard
- CA—certification authority
- CEP—Certificate Enrollment Protocol
- CLI—Command-Line Interface
- CSPM—Cisco Secure Policy Manager
- DES—Data Encryption Standard
- 3DES—Triple DES
- Explicit IV—Explicit Initialization Vector
- Gb—Gigabit
- Gbps—Gigabits per second
- ICMP—Internet Control Message Protocol
- IKE—Internet Key Exchange
- ISAKMP—Internet Security Association and Key Management Protocol
- IDS—Intrusion Detection System
- JVM—Java Virtual Machine
- MB—Megabyte
- Mbps—Megabits per second
- MD5—Message Digest 5 (MD5)
- PCI—Peripheral Component Interconnect
- PDM—PIX Device Manager
- PIX—PIX Firewall
- SCEP—Simple Certificate Enrollment Protocol
- SDRAM—Synchronous Dynamic Random-Access Memory
- SHA—Secure Hash Algorithm
- SNMP—Simple Network Management Protocol
- SSL—Secure Sockets Layer
- TFTP—Trivial File Transfer Protocol
- VAM—Virtual Private Network (VPN) Acceleration Module (VAM)

Related Documentation

Use this document with the PIX Firewall and PDM documentation sets, which are available on the PIX Firewall product CD and online at the following website:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_technical_documentation.html

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (http://www.cisco.com/tac) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

The online TAC Case Open Tool (http://www.cisco.com/tac/caseopen) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/index.html

Overview

This chapter describes the Cisco PIX Device Manager (PDM) Version 3.0 and the system requirements for this version.

Note In this guide, the term "PIX Firewall" refers to all models running PIX Firewall software Version 6.3 unless specifically noted. PIX Firewall software Version 6.3 is required for PDM Version 3.0.

This chapter includes the following sections:

Introduction

Cisco PIX Device Manager (PDM) is a graphical user interface (GUI) that manages Cisco PIX Firewalls. PDM, a signed Java applet, uses certificates and HTTPS (HTTP over SSL) to securely transmit information between PDM and the PIX Firewall. (Enter "**https**" in your browser to use HTTPS.)

PDM provides the following:

- *GUI*—Lets you configure, manage, and monitor security policies across a network.
- *PDM Startup Wizard*—Creates a basic configuration that allows packets to flow securely through the PIX Firewall from the inside to the outside network.
- *VPN Wizard*—Creates a basic configuration that lets you easily set up a remote access VPN or site-to-site VPN.
- *Monitoring and Reporting Tools*—Provides real-time and historical data, summarizing network activity, resource utilization and event logs, allowing performance and trend analysis. You can detect and interrupt unusual activity with PDM's logging and notification.
- *Graphical Tools*—Creates 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. You can view multiple graphs simultaneously to do side-by-side analysis.
  - *System graphs*: Provides detailed status information on the PIX Firewall, including blocks used and free, current memory utilization, and CPU utilization.

  - *Connection graphs*: Tracks 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.
  - *Intrusion Detection System (IDS)*: Provides 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*: Provides real-time monitoring of your bandwidth usage for each interface. Bandwidth usage is displayed for incoming and outgoing communications, such as packet rates, counts, and errors, as well as bit, byte, and collision counts.
- *Syslog Viewer*—Lets you view specific syslog message types by selecting the desired logging level.
- *Embedded Architecture*—Lets you manage the Cisco PIX Firewall from almost any computer, regardless of the operating system, and works with most browsers, including Microsoft Internet Explorer and Netscape Navigator. There is no application to install and no plug-in required.
- *Secure Communication*—Supports the Secure Sockets Layer (SSL) protocol to provide high-grade encryption from the PIX Firewall to a browser. PDM to PIX Firewall communication is securely encrypted according to these encryption standards: 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), or 128-bit Advanced Encryption Standard (AES). You can protect access with a valid username and password, either on the PIX Firewall or through an authentication server.

Data Encryption Overview

This section describes data encryption, including the IPSec, IKE, and certification authority (CA) interoperability features.

Note For additional information on these features, refer to the "IP Security and Encryption" chapter in the appropriate *Security Configuration Guide* and *Security Command Reference* publications for your specific PIX Firewall.

IPSec is a network level open standards framework, developed by the Internet Engineering Task Force (IETF) that provides secure transmission of sensitive information over unprotected networks such as the Internet. IPSec includes data authentication, antireplay services and data confidentiality services.

Cisco follows these data encryption standards:

- IPSec—IPSec is an IP layer open standards framework that provides data confidentiality, data integrity, and data authentication between participating peers. IKE handles negotiation of protocols and algorithms based on local policy, and generates the encryption and authentication keys to be used by IPSec. IPSec protects one or more data flows between a pair of hosts, between a pair of security systems, or between a security system and a host.
- IKE—Internet Key Exchange (IKE) is a hybrid security protocol that implements Oakley and Skeme key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. IKE can be used with IPSec and other protocols. IKE authenticates the IPSec peers, negotiates IPSec security associations, and establishes IPSec keys. IPSec can be configured with or without IKE.

- CA—Certification authority (CA) interoperability supports the IPSec standard, using Simple Certificate Enrollment Protocol (SCEP) and Certificate Enrollment Protocol (CEP). CEP permits PIX Firewall devices and CAs to communicate to permit your PIX Firewall device to obtain and use digital certificates from the CA. IPSec can be configured with or without CA. The CA must be properly configured to issue certificates.

The component technologies implemented for IPSec include:

- DES and Triple DES—The Data Encryption Standard (DES) and Triple DES (3DES) encryption packet data. Cisco IOS software implements the 3-key Triple DES and DES-CBC with Explicit IV. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.
- AES—The Advanced Encryption Standard, a next-generation symmetric encryption algorithm, used by the U.S. Government and organizations outside the U.S.
- MD5 (HMAC variant)—Message Digest 5 (MD5) is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.
- SHA (HMAC variant)—Secure Hash Algorithm (SHA) is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.

IPSec with the PIX Firewall software supports the following additional standards:

- AH—Authentication Header is a security protocol that provides data authentication and optional antireplay services.

  The AH protocol uses various authentication algorithms; PIX Firewall software has implemented the mandatory MD5 and SHA (HMAC variants) authentication algorithms. The AH protocol provides antireplay services.
- Explicit IV—Explicit Initialization Vector is a sequence of random bytes appended to the front of a plaintext message before encryption by a block cipher, which eliminates the possibility of having the initial ciphertext block the same for any two messages. For example, if messages always start with a common header (a letterhead or “From” line) their initial ciphertext would always be the same, assuming that the same cryptographic algorithm and symmetric key was used. Adding a random initialization vector eliminates this from happening.
- ESP—Encapsulating Security Payload, a security protocol, provides data privacy services, optional data authentication, and antireplay services. ESP encapsulates the data to be protected. The ESP protocol uses various cipher algorithms and (optionally) various authentication algorithms. PIX Firewall software implements the mandatory 56-bit DES-CBC with Explicit IV, Triple DES, or AES as the encryption algorithm, and MD5 or SHA (HMAC variants) as the authentication algorithms. The updated ESP protocol provides antireplay services.

For more information on PIX Firewall IPSec terms, see IPSec terms in the online Help at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdm30olh.pdf

PIX Firewall System Requirements

PDM Version 3.0 requires PIX Firewall software Version 6.3.

PDM has the following system requirements:

- PDM Version 3.0 is available on all PIX 501, PIX 506/506E, PIX 515/515E, PIX 520, PIX 525, and PIX 535 platforms running PIX Firewall software Version 6.3.
- PDM works with any configuration, whether created with the PIX Firewall command-line interface (CLI), Cisco Secure Policy Manager (CSPM) or Management Center for PIX Firewall (PIXMC). However, subsequent configuration changes using CSPM or PIXMC overwrites the PDM configuration.

Caution If you are using CSPM or PIXMC, use PDM for monitoring only. All changes made using PDM will be overwritten the next time CSPM or PIXMC synchronizes with the PIX Firewall.

For more information on earlier versions of PDM, see the appropriate installation guide at: http://www.cisco.com/en/US/products/sw/netmgtsw/ps2032/products_installation_guides_books_list.html

This section includes the following topics:

PIX Firewall System Interoperability with PDM

Table 1-1 lists the PIX Firewall System requirements for PDM Version 3.0.

Table 1-1 PIX Firewall System Requirements for PDM Version 3.0

Type	Description
Hardware	
Platform	PIX 501, 506/506(E), 515/515(E), 520, 525, or 535
Random access memory	16MB
Flash Memory	See Table 1-2
Software	
PIX Firewall operating system	Version 6.3
Encryption	DES, 3DES, or AES-enabled

The PIX Firewall system ships with PIX Firewall software Version 6.3, which includes a pre-installed DES activation key. If your PIX Firewall is not enabled for DES, 3DES, or AES, and you are a registered Cisco user, you can receive a DES, 3DES, or AES activation key by completing the form at the following URL: http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324. To become a registered Cisco user, go to http://tools.cisco.com/RPF/register/register.do

Flash Memory Requirements

Table 1-2 lists Flash memory requirements for PIX Firewall software Version 6.3 in conjunction with PDM Version 3.0 by platform.

Table 1-2 Flash Memory Requirements for PDM Version 3.0

PIX Firewall Model	Flash Memory Required
PIX 501	8 MB
PIX 506/506E	8 MB
PIX 515/515E	16 MB
PIX 520	16 MB (Some PIX 520 units may need a memory upgrade because older units had 2 MB, though newer units have 16 MB)
PIX 525	16 MB
PIX 535	16 MB

Maximum Configuration File Size

For optimum performance, we recommend a configuration file of no more than 100 KB (approximately 1500 lines) when using PDM.

PIX Firewall configuration files over 100 KB may interfere with the performance of PDM on your workstation in the following situations:

- While executing commands such as **write term** and **show conf**
- Failover (the configuration synchronization time)
- During a system reload

To determine the size of your configuration file, enter the **show flashfs** command at the PIX Firewall CLI prompt. View the output which begins with “file 1.” The number labeled “length” on the same line is the configuration file size in bytes.

For example:

```
pixfirewall# show flashfs
flash file system: version:3  magic:0x12345679
  file 0:origin:      0 length:1925176
  file 1:origin:2883584 length:2944
  file 2:origin:3014656 length:32
  file 3:origin:      0 length:0
  file 4:origin:3145728 length:131072
  file 5:origin:8257536 length:308
```

PIX Firewall platforms have different configuration file size limitations than PDM. See Table 1-3 for the maximum recommended configuration file size by platform.

Table 1-3 Maximum Recommended Configuration File Size by Platform

PIX Firewall Version	Maximum Configuration
PIX 501	256 KB
PIX 506/506E, 515/515E, 520	1 MB
PIX 525, PIX 535 [1]	2 MB

1. This applies to PIX Firewall software Version 5.3(2) and later versions. The maximum recommended configuration file size for PIX Firewall software Versions 5.3(1) and earlier is 1 MB.

Software Requirements

PIX Firewall software Version 6.3 has the following software requirements:

- The PIX Firewall image no longer fits on a diskette. If you are using a PIX Firewall unit with a diskette drive, download the Boothelper file from cisco.com http://www.cisco.com/cgi-bin/tablebuild.pl/pix) to get the PIX Firewall image.
- Before upgrading from a previous PIX Firewall version, save your configuration and write down your activation key and serial number. Refer to "Upgrading to a New Software Release" in this chapter for new installation requirements.
- Before upgrading from Version 4 or earlier, using Auto Update, IPSec, SSH, PDM, or VPN, you will need a new 56-bit DES activation key, which can be sent to you by completing the form at: http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324
- Use the **show version** command to verify the software version of your PIX Firewall unit.

Upgrading to a New Software Release

If you registered Cisco user, refer to the *Upgrading Software for the Cisco Secure PIX Firewall* document at the following URL:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a0080094a5d.shtml

PC/Workstation Requirements

PDM requirements vary depending on the platform.

Note PDM is not supported on Macintosh, Windows 3.1, or Windows 95 operating systems.

This section includes the following topic:

- Supported Platforms, page 8

Note the following when using PDM to access the PIX Firewall unit:

- *Minimum Disk Space Requirement*—PDM requires a minimum of at least 4 MB of temporary disk space to load into the browser.

- *Java Virtual Machine (JVM)*—PDM supports the native Internet Explorer JVM from Microsoft, and the native Java Development Kit (JDK), a Java Plug-in. PDM Version 3.0 supports the Java Plug-in 1.3.1, 1.4.0 and 1.4.1 (recommended).

Note Java Plug-in 1.4.0 includes some JVM bugs that cause it to display some error messages in the Java Console.

To check which Java Virtual Machine (JVM) version you have, launch PDM. In the main PDM menu, click **Help>About Cisco PIX Device Manager**. When the **About PDM** information window appears, it displays your browser specifications in a table. You can download the latest JVM version for Internet Explorer from Microsoft, and you can download the latest Java Plug-in from Sun Microsystems (www.java.sun.com).

- *Disabling the Java Plug-in*—If you are using Microsoft Internet Explorer, and it is necessary to disable the Java Plug-in for your configuration, perform the following steps:

Note This is only available if you are using the Java Plug-in 1.3.1, 1.4.0, and 1.4.1 and not a beta version.

a. Click **Tools>Internet Options**.
b. Click the **Advanced** tab.
c. In the Java (Sun) section, clear the **Use Java 2** check box.

- *HTTP 1.1*—Settings for **Internet Options>Advanced>HTTP 1.1 settings** should use HTTP 1.1 for both proxy and non-proxy connections.
- *Secure Sockets Layer (SSL)*—Browser support for SSL must be enabled. The supported versions of Internet Explorer and Netscape Navigator support SSL without requiring additional configuration.
- *Load Time Improvement*—If you are using the Java Plug-in and accessing your PIX Firewall using an IP address instead of a host name, the performance of PDM is dramatically slower. This occurs if the PIX Firewall host name is not in DNS or in the local hosts file.

  The workaround is to assure that the PIX Firewall host name is in DNS. If you are running Windows, and there is no DNS in your network or your DNS does not have the PIX Firewall entry, modify the "hosts" file.

  – On Windows NT, 2000, and XP, the hosts file is located at C:\WINNT\system32\drivers\etc\hosts.
  – On Windows 98 and ME, it is at C:\Windows\hosts.

  Each line in the hosts file is in the format "<ip> <hostname>". For example:

```
192.168.1.1   pixfirewall.example.com
```

Supported Platforms

This section includes the following topics:

Windows

Table 1-4 and Table 1-5 list the requirements for Windows platforms using PDM 3.0.

Table 1-4 Hardware Requirements and Network Connectivity for Windows Platforms for PDM 3.0

Type	Requirements
Hardware	
Processor	Pentium III or equivalent running at 450 Mhz or higher
Random Access Memory	256 MB
Display Resolution and Colors	1024 x 768 pixels and 256 colors
Network Connection	
Connection speed	56 Kbps; 384 Kbps (DSL or cable) recommended

Table 1-5 Supported and Recommended Windows Platforms for PDM 3.0

Operating System	Browser	JVM
Supported Windows Platforms		
Windows 98 Windows NT 4.0 (Service Pack 4 and higher) Windows 2000 (Service Pack 3) Windows ME Windows XP	Internet Explorer 5.5 or 6.0	Native[1] JVM (VM 3167 or higher)
	Internet Explorer 5.5 or 6.0	Java 1.3.1, 1.4.0, or 1.4.1
	Netscape 4.7x	Native[1] JVM 1.1.5
	Netscape 7.0x	Java Plug-in 1.4.0 or 1.4.1
Recommended Windows Platforms		
Microsoft Windows 2000 (Service Pack 3), or Microsoft Windows XP	Internet Explorer 6.0	Native[1] JVM (VM 3809) or Java Plug-in 1.4.1_02
	Netscape 7.0x	Java Plug-in 1.4.1_02

1. Native refers to the built-in JVM that ships with the browser.

Note PDM Version 3.0 does not support Windows 3.1 or Windows 95.

Sun Solaris

Table 1-5 and Table 1-6 list the requirements for Sun Solaris platforms using PDM 3.0.

Table 1-6 Hardware and Network Connectivity Requirements for Sun Solaris Platforms for PDM 3.0

Type	Requirements
Hardware	
Processor	SPARC
Random Access Memory	At least 128 MB
Display Resolution and Colors	At least 1024 x 768 pixels and 256 colors
Network Connection	
Connection speed	56 Kbps; 384 Kbps (DSL or cable) recommended

Table 1-7 Supported and Recommended Sun Solaris Platforms for PDM 3.0

Operating System	Browser	JVM
Supported Sun Solaris Platforms		
Sun Solaris 2.8 or 2.9 running CDE window manager	Netscape 4.78[1]	Native[2] JVM
Recommended Sun Solaris Platforms		
Sun Solaris 2.8 running CDE window manager	Netscape 4.78[1]	Native[2] JVM

1. Netscape Communicator 4.79 is not supported.
2. Native refers to the built-in JVM that ships with the browser.

Red Hat Linux

Table 1-8 and Table 1-9 list the requirements for Red Hat Linux platforms using PDM 3.0.

Table 1-8 Hardware and Network Connectivity Requirements for Linux Platforms for PDM 3.0

Type	Requirements
Hardware	
Processor	Pentium III or equivalent running at 450 Mhz or higher
Random Access Memory	At least 128 MB
Display Resolution and Colors	At least 1024 x 768 pixels and 256 colors
Network Connection	
Connection speed	56 Kbps; 384 Kbps (DSL or cable) recommended

Table 1-9 Supported and Recommended Red Hat Linux Platforms for PDM 3.0

Operating System	Browser	JVM
Supported Red Hat Linux Platforms		
Red Hat Linux 7.0, 7.1, 7.2, 7.3 or 8.0 running GNOME or KDE	Netscape 4.7x on Red Hat 7.x	Native[1] JVM
	Mozilla 1.0.1 on Red Hat 8.0	Java Plug-in 1.4.1
Recommended Red Hat Linux Platforms		
Red Hat Linux 8.0	Mozilla 1.0.1	Java Plug-in 1.4.1_02

1. Native refers to the built-in JVM that ships with the browser.

Preparing to Install PDM

If your firewall unit is new and shipped with minimum firewall software version, the PDM software is already loaded in the firewall Flash memory for you.

If you are upgrading from a previous version, you need to use TFTP from the firewall to copy the PDM image to your firewall. For instructions on how to do this, refer to Appendix A, "Using a TFTP Server".

For information about new features in the latest version of PDM, see About PDM Software in the online Help at http://www.cisco.com/application/pdf/en/us/guest/products/ps2032/c1626/ccmigration_09186a0080189166.pdf

This section includes the following topics:

Notes and Cautions

- *CLI Command Support*—PDM Version 3.0 uses the PIX Firewall CLI command syntax, which is very similar to Cisco IOS software, but not identical. Most PIX Firewall CLI commands are fully supported by PDM. If you are using PDM with an existing firewall configuration, refer to PDM Support for PIX Firewall CLI Commands for more information.
- *Multiple PDM Sessions*—PDM allows multiple PCs or workstations to each have one browser session open with the same firewall. However, only one session per browser per PC or workstation is supported for a particular firewall.
- *Minimum Version for PIX*—PDM 3.0 does not run with PIX Firewall software versions earlier than Version 6.3. PDM Version 3.0 is a single image which supports only PIX Firewall Version 6.3.
- *Java Plug-in Supported*—PDM Version 3.0 supports the Java plug-in for browsers. See PDM online Help (**Browser Requirements>JDK**) for more information.
- *JVM Bug with Solaris, Netscape 4.7*—Some actions, such as clicking a button to go to a dialog, may be delayed unless the mouse is moved after the action. This JVM bug affects all versions of PDM on Solaris. Workaround: Move mouse after clicking buttons, window controls, or other actions.
- *Caveats*—Please use Bug Navigator II on cisco.com to view current caveat information. Bug Navigator II may be accessed at the following website: http://www.cisco.com/support/bugtools

Caution

When you have a corrupted certificate database and run PDM with Netscape version 4.73, the Netscape browser may crash after you click **Grant** in the **grant privileges** dialog box. (The certificate database is a file called cert7.db, located in the your Netscape directory.)

Netscape version 4.73 can corrupt the certificate database if you do the following before you click **Grant**:

1. Run an applet that uses a digital certificate.
2. Renew the certificate.
3. Run the new applet with the updated certificate.

This occurs on Windows, Sun Solaris, and Linux platforms with the Netscape Java Virtual Machine (JVM).

A workaround is to remove the corrupted cert7.db file from your Netscape directory. A new cert7.db file is created when you run Netscape again. However, this removes all of the certificates that you have previously accepted as trusted. (This includes certificates that you accepted from other sites as well as certificates that you entered manually.)

Installation Checklist

Confirm the following before you install PDM:

- Verify that all system requirements have been met. See the requirements listed in Chapter 1, "Overview." For example, the PIX Firewall unit must be running PIX Firewall software Version 6.3 and have a DES, 3DES, or AES activation key to use PDM Version 3.0.
- Confirm that you are running PIX Firewall software Version 6.3. (If you have command line access to your PIX Firewall, you can use the CLI **show version** command to display the version currently running on your PIX Firewall.)
- If you are not running PIX Firewall software Version 6.3, see the instructions for installing PIX Firewall software in the *Cisco PIX Firewall and VPN Configuration Guide*. (After installing a PIX Firewall image, reboot your PIX Firewall to begin running the new image on the PIX Firewall.)

  If your PIX Firewall is new, it shipped with PIX Firewall software Version 6.3, and PDM Version 3.0.
- Verify that you have a TFTP or FTP server installed. See Appendix A, "Using a TFTP Server." to install a TFTP server.
- Confirm that you are a registered Cisco user. If you are not a registered user, go to http://tools.cisco.com/RPF/register/register.do, and complete the form to register.

Preparing to Install PDM

Before installing PDM, be aware of the following:

- Save or print your PIX Firewall configuration. (You can save a copy of your configuration by using the PIX Firewall CLI **write terminal** command to display your configuration. You can cut and paste the displayed configuration into a text file.)
- Write down your activation key. (View your activation key by using the PIX Firewall CLI **show version** command.)
- If you are upgrading from a previous version of the PIX Firewall software, obtain the PDM software from Cisco in the same way that you do PIX Firewall software (see http://www.cisco.com/cgi-bin/tablebuild.pl/pix), and download the image onto your PIX Firewall unit, using HTTP protocol or a TFTP server. For instructions on how to use a TFTP server, refer to Appendix A, "Using a TFTP Server."

Note For additional information on upgrading software for the PIX Firewall, see *Upgrading Software for the Cisco Secure PIX Firewall* at the following URL: http://www.cisco.com/en/US/partner/products/hw/vpndevc/ps2030/products_tech_note09186a0080094a5d.shtml

- If you plan to upgrade a PIX Firewall failover pair to use PIX Firewall software Version 6.3 and PDM Version 3.0, both the PIX Firewall image and the PDM image must be installed on your failover units.
- If you are using PDM with an existing PIX Firewall configuration, refer to the appropriate version of the *Cisco PIX Device Manager Release Notes* for information on which commands are supported and which are not.
- PDM works with any configuration, whether created with the PIX Firewall command-line interface (CLI) or Cisco Secure Policy Manager (CSPM). Subsequent changes to the PIX Firewall configuration are not communicated automatically to PDM. If you are using PDM, and make changes to your PIX Firewall configuration outside PDM, click **Refresh** in PDM to update PDM with the current PIX Firewall configuration.
- A DES (free), or 3DES/AES license is required. PDM only supports encrypted communication.
  - Registered Cisco.com users can request a DES (free), 3DES/AES activation key from the following URL:

    http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324
  - New Cisco.com users can complete the form at this URL before requesting a DES (free), 3DES/AES activation key:

    http://www.cisco.com/pcgi-bin/Software/FormManager/formgenerator.pl

  3DES/AES activation keys are available as part of a feature license upgrade and are not free.

Caution If you are using CSPM, use PDM for monitoring only. All changes made using PDM will be overwritten the next time CSPM synchronizes with the PIX Firewall.

Determining the IP Address of Your Server

Loading a PIX Firewall or PDM image requires you to use TFTP server or FTP.

Note The Microsoft Windows-based TFTP server previously provided by Cisco Systems has been discontinued and is no longer supported by Cisco Systems. Persons still using the server should consider replacing it with any high quality freeware and shareware TFTP server. TFTP servers can be found by searching for "tftp server" on the Web. We do not specifically recommend any particular TFTP implementation.

Note that recent versions of Cisco IOS software support the use of FTP instead of TFTP for loading of images or configuration files. Use of FTP overcomes a number of inherent limitations of TFTP, including a lack of security and a 16 MB file size limitation.

Before using TFTP, determine the IP address of your server.

This section provides the information required to determine your IP address, and includes the following topics:

Windows NT, Windows 2000, or Windows XP

On a Windows workstation, click **Start>Accessories>Command Prompt** to launch the Windows command-line interface and then enter the **ipconfig** command as shown in the following example:

```
C:\> ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 209.165.200.225
        Subnet Mask . . . . . . . . . . . : 255.255.255.224
        Default Gateway . . . . . . . . . : 10.21.196.33

C:\>
```

In this example, the server's IP address is 209.165.200.225 with a network mask of 255.255.255.224.

Windows 98 or Windows ME

From a Windows 98 or Windows ME computer, you can view the IP address by clicking **Start**>**Run** and entering the **winipcfg** command. Windows then displays a graphical user interface (GUI) listing the IP address information.

Sun Solaris

Enter the **/sbin/ifconfig -a** command to view your IP address, as shown in the following example:

```
% /sbin/ifconfig -a
lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232
        inet 127.0.0.1 netmask ff000000
hme0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
        inet 209.165.200.225 netmask ffffffe0 broadcast 209.165.200.255
```

In this example, the IP address of the host is 209.165.200.225 with a netmask of 255.255.255.224. (ffffffe0 is the hexadecimal equivalent to 255.255.255.224.)

Linux

Enter the **/sbin/ifconfig** command to view your IP address, as shown in the following example:

```
% /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:D0:B7:5D:C0:56
          inet addr:209.165.200.225 Bcast:209.165.200.255
Mask:255.255.255.224
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:189576 errors:0 dropped:0 overruns:0 frame:0
          TX packets:414837371 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:10 Base address:0x3000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:75397725 errors:0 dropped:0 overruns:0 frame:0
          TX packets:75397725 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

In this example, the IP address of the computer is 209.165.200.225 with a netmask of 255.255.255.224. The remainder of the display provides information on the status of data transmission through the server.

Installing PDM

This chapter describes how to install Cisco PIX Device Manager (PDM) Version 3.0 on your PIX Firewall unit.

This chapter includes the following sections:

Downloading the PDM Software

You can download PDM using either of the following options:

Downloading PDM from Cisco.com

Perform the following steps to install PDM from Cisco.com (the Web):

Step 1 Go to http://www.cisco.com using a web browser.

Step 2 On the menu bar, click **LOGIN**.

Step 3 Enter your Cisco.com username and password and click **OK**.

Note To register as a Cisco.com user, and obtain a username and password, go to this URL: http://tools.cisco.com/RPF/register/register.do

Step 4 Enter **http://www.cisco.com/cgi-bin/tablebuild.pl/pix** in the web address area of your web browser and press the **Return** or **Enter** key on your keyboard. (If you are prompted again for a username and password, enter your Cisco.com username and password.)

Step 5 On the Cisco Secure PIX Firewall Software page, find the section titled "Select a File to Download", click **pdm-*nnn*.bin** (where *nnn* represents the PDM software image version that you want to install) and follow the instructions presented.

Downloading PDM Using FTP

Perform the following steps to install PDM using FTP:

Step 1 Set your FTP client to passive mode by selecting the Properties button on the Connect to FTP Site screen, selecting the Connection tab, checking **Use Passive Mode**, and clicking **Apply**.

Step 2 Start your FTP client and connect to **ftp.cisco.com**. Enter your Cisco.com username and password when prompted.

Step 3 Enter **`cd cisco`**.

Step 4 Enter **`cd ciscosecure`** and then enter **`cd pix`** to access the PIX Firewall software directory.

Step 5 Copy the **pdm-*nnn*.bin** file (where *nnn* represents the PDM version) to a folder where it can be accessed from your TFTP server. (You can use the **ls** command to view the directory contents.)

Step 6 To download PIX Firewall and PDM documentation, enter **`cd documentation`**, locate the .pdf files for the documents you want, and copy the files to your workstation. (Files with the .pdf file extension are viewed with Adobe Acrobat Reader, which is free and available at http://www.adobe.com/products/acrobat/readstep2.html.)

Step 7 Enter **`quit`** to exit.

Installing PDM

Perform the following steps to install PDM:

Step 1 Follow these steps to set up a console connection from a Microsoft Windows workstation to your PIX Firewall unit, unless you already have a console connection:

- **a.** Power off your PIX Firewall unit.
- **b.** Connect the serial port of a Microsoft Windows workstation to the console port of the PIX Firewall with the serial cable supplied in the PIX Firewall accessory kit.
- **c.** Power on the PIX Firewall unit. If a failover PIX Firewall unit is present, configure the primary unit first.

Step 2 Locate the Windows **HyperTerminal** accessory by looking for it on the Windows **Start** menu. It is usually located under **Programs**>**Accessories**>**Communications**>**HyperTerminal**.

Step 3 Click **HyperTerminal** to open the **New Connection** window; the **Connection Description** dialog box appears.

Step 4 Enter a name for the connection and click **OK**.

Step 5 In the **Connect To** dialog box, leave the area code and phone number blank.

Step 6 In the **Connect using** drop-down menu, select **Com 1** (unless you are using another serial port to connect, in which case select that port) and click **OK**.

Step 7 Set the values in the following table:

Field Name	Value to Set
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	Hardware

Step 8 Click **OK** to continue.

The HyperTerminal window is now ready to receive information from the PIX Firewall console. Wait 30 seconds for the PIX Firewall startup messages to display. These messages should appear similar to the following example:

```
Rebooting....
Cisco Secure PIX Firewall BIOS (4.0) #0: Thu Mar  2 22:59:20 PST 2000
Platform PIX-515
Flash=i28F640J5 @ 0x300

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 1507840 bytes of image from flash.
################################################################################
64MB RAM
Flash=i28F640J5 @ 0x300
BIOS Flash=AT29C257 @ 0xfffd8000
mcwa i82559 Ethernet at irq 10  MAC: 0050.54ff.3772
mcwa i82559 Ethernet at irq  7  MAC: 0050.54ff.3773
mcwa i82559 Ethernet at irq 11  MAC: 00d0.b792.409d

  ------------------------------------------------------------------------
                              ||        ||
                              ||        ||
                             ||||      ||||
                          ..:||||||:..:||||||:..
                          c i s c o S y s t e m s
                         Private Internet eXchange
  ------------------------------------------------------------------------
                         Cisco PIX Firewall

Cisco PIX Firewall Version 6.3
Licensed Features:
Failover:           Enabled
VPN-DES:            Enabled
VPN-3DES:           Enabled
Maximum Interfaces: 6
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited
```

Step 9 Press the **Enter** key if it takes more than a minute for the PIX Firewall command prompt to appear.

If irrelevant characters appear, reset the **Bits per second** to 9600 and try to connect again.

Note If it still does not appear, power off the PIX Firewall and ensure that the serial cable is attached to COM1 and not to COM2, if your computer is so equipped. Power the PIX Firewall back on and try to connect again.

Step 10 Enter the **enable** command if your PIX Firewall unit is being run for the first time.

Step 11 When prompted, enter your PIX Firewall password. (After starting a new PIX Firewall, you should change the password to secure administrative access to the unit.) If no password has been set, you can choose one and enter it at this time.

Step 12 Start your TFTP server. See Appendix A, "Using a TFTP Server." for more information on the TFTP server.

Step 13 Check the IP address of the computer running the TFTP server, as described in "Determining the IP Address of Your Server" in Chapter 2, "Preparing to Install PDM."

Loading the PDM Image

Perform the following steps to load the PDM image file onto the PIX Firewall:

Step 1 Enter the following at the command prompt to load the PDM image file:

```
pixfirewall# copy tftp://Your_TFTP_Server_IP_Address/Your_pdmfile_name flash:pdm
```

Or you can enter the generic command and follow the prompts:

```
pixfirewall# copy tftp flash:pdm
```

Step 2 Enter the following command at the prompt to enter configuration mode:

```
pixfirewall# configure terminal
```

Caution If your PIX Firewall is running a pre-existing configuration, refer to the *Cisco PIX Device Manager Release Notes Version 3.0* for information on the configuration commands supported for use with PDM.

Note If you have a PIX 501 or PIX 506/506E, you can use the factory default configuration loaded on the unit and skip to "Starting PDM with Internet Explorer" in Chapter 4, "Configuring PDM," instead of entering setup.

Step 3 To enter setup, use the **setup** command as shown in the following example:

```
pixfirewall (config)# setup
```

Step 4 Load the PDM image by following the steps in Table 3-1:

Note Press **Enter** to accept the default values.

Table 3-1 Setup Command Prompts

Step	Command	Purpose
Step 1	`Enable Password [<use current password>]:`	Enter an alphanumeric password, up to 16 characters in length, to protect the PIX Firewall privileged (access) mode. Record the password in accordance with your security policy. If you assign a password here, then it is used for authentication every time you launch PDM unless you configured your PIX Firewall to use another AAA server for authentication, in which case the AAA server provides the authentication.

Step 2	`Clock (UTC)`
	`Year [2001]:`
	`Month [Aug]:`
	`Day [27]:`
	`Time [22:47:37]:`
		Set the PIX Firewall clock to Universal Coordinated Time (UTC, also known as Greenwich Mean Time, or GMT). For example, if you are in the Pacific Daylight Savings time zone, set the clock 7 hours ahead of your local time to set the clock to UTC. Enter the year, month, day, and time. Enter the UTC time in 24-hour time as hour:minutes:seconds.

Step 3	`Inside IP address:`	Specify the IP address of the PIX Firewall unit's inside interface. Ensure that this IP address is unique on the network and not used by any other computer or network device, such as a router.
Step 4	`Inside network mask:`	Specify the network mask for the inside interface. An example mask is 255.255.255.0. You can also specify a subnetted mask, for example: 255.255.255.224. Do not use all 255s, such as 255.255.255.255. This prevents traffic from passing on the interface.
Step 5	`Host name:`	Specify up to 16 characters as a name for the PIX Firewall unit.
Step 6	`Domain name:`	Specify the domain name for the PIX Firewall.
Step 7	`IP address of host running PIX Device Manager:`	Specify the IP address of the workstation designated to run PDM.

After you enter the IP address of the workstation running PDM, PIX Firewall displays the information you just entered.

The following is a sample display:

```
The following configuration will be used:
Enable Password: ciscopix
Clock (UTC): 14:22:00 Aug 28 2001
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: accounting_pix
Domain name: example.com
IP address of host running PIX Device Manager: 192.168.1.2
```

Step 5 Enter **n** to edit the values, or enter **y** to save the information to the PIX Firewall Flash memory.

```
Use this configuration and write to flash? y
```

Or, enter **y** at the prompt to save the information to the PIX Firewall Flash memory.

Step 6 Click **Save** to save your settings.

Step 7 Click **Exit**.

Step 8 Click **Yes** to exit HyperTerminal.

Configuring PDM

This section describes how to configure your PDM. It includes the following topics:

Starting PDM with Internet Explorer

Perform the following steps to start PDM with Internet Explorer:

Step 1 On an Internet Explorer browser running on a workstation connected to the PIX Firewall unit, enter the following:

https://*pix_inside_interface_ip_address*

where *pix_inside_interface_ip_address* is the IP address of the inside interface of your PIX Firewall, entered in standard (number) format.

For the PIX 501 and PIX 506/506E, the factory default inside interface address is as follows:

```
inside IP address to 192.168.1.1
```

Enter **https://192.168.1.1** for the PIX 501 and PIX 506/506E platforms.

This launches PDM.

Note Ensure that you add the "**s**" to "**https**" or the web browser cannot connect. HTTPS (HTTP over SSL) provides a secure connection between your browser and the PIX Firewall that you are using PDM to configure or monitor.

Step 2 Accept the security certificate. (You must accept the certificate to use PDM.)

To avoid the certificate from appearing in Windows Internet Explorer when the certificate dialog (titled "**Security Alert**") is shown, perform the following steps:

a. Click **View Certificate**.

b. Click **Install Certificate**.

c. Click **next>next>Finish>Yes**.

d. Click **OK** in the certificate dialog box.

e. In the Security Alert dialog box, click **Yes**.

Note Subsequent PDM loads will not show the certificate dialog box.

Step 3 Enter your password. If no password has been set, choose and enter one at this time. Click **OK** to continue.

Step 4 Answer 'Yes' to the Security Warning asking "Do you want to install and run 'Cisco PIX Device Manager'"?

If you do not want this question to be asked next time you load PDM, check the box with the label 'Always trust content from Cisco Systems.'

Step 5 Follow the instructions on screen.

PDM starts after the certificates are accepted.

Step 6 For more information on how to use PDM, see the online Help at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdm30olh.pdf

Starting PDM with Netscape Navigator

Perform the following steps to start PDM with Netscape Navigator:

Step 1 On a Netscape Navigator browser running on a workstation connected to the PIX Firewall unit, enter the following:

```
https://172.23.59.230/
```

This launches PDM.

Step 2 Accept the security certificate. (You must accept the certificate to use PDM.)

To avoid the certificate from appearing in Netscape Navigator when the certificate dialog (titled "**Security Alert**") is shown, perform the following steps:

a. Click **Next** at the New Site Certificate screen.

b. Click **Next** at the next New Site Certificate screen.

c. Select **Accept this certificate forever (until it expires)**, and click **Next** at the next New Site Certificate screen.

d. Click **Next** at the next New Site Certificate.

e. Click **Finish** at the next New Site Certificate.

f. Click **Continue** at the Certificate Name Check.

Step 3 Enter your user name and password. Click **OK**.

Step 4 Select 'Remember this decision,' and click **Grant** at the next four Java Security screens.

PDM starts after the certificates are accepted.

Step 5 For more information on how to use PDM, see the online Help at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdm30olh.pdf

PDM Home Page

The PDM home page lets you view, at a glance, important information about your PIX Firewall such as the status of your interfaces, the version you are running, licensing information, and performance. Many of the details available on the PDM home page are available elsewhere in PDM, but this is a useful and quick way to see how your PIX Firewall is running. All information on the Home page is updated every ten seconds, except for the Device Information.

You can access the Home page any time by clicking Home on the main toolbar.

Note If the interface is configured to use DHCP or PPPoE to obtain an IP address, and running PIX Firewall Version 6.3 or higher, your IP address will be displayed in the Interface Status table. If you are running an earlier version of the PIX Firewall software, the IP address will not be displayed.

On a PIX 501, the inside interface link will always be displayed as up, because this interface acts as a built-in switch. Be sure to check for physical connectivity on the inside interface of a PIX 501.

The PDM home page displays the following fields:

Area	Description	
Device Information	This area displays the following information:	
	Host Name, **PIX Version**, **Device Type**, **License**, **PDM Version**, **Total Memory**, and **Total Flash**.	
	Licensed Features—This area displays the features your PIX Firewall is licensed to use.	Encryption
		Failover
		Max Interfaces
		Inside Hosts
		IKE Peers
		Max Physical Interfaces

Area	Description
Interface Status	**Interface**—Displays the interface name as configured in the Interfaces panel. You can click any of the table headings to sort by that value.
	IP Address/Mask—Displays the IP address of the associated interface.
	Link—Displays the link status of the interface. A red icon is displayed if the physical status of the link is down, and a green icon is displayed if the physical status of the link is up. Note that on a PIX 501, the inside interface link will always be displayed as up, because this interface acts as a built-in switch. Be sure to check for physical connectivity on the inside interface of a PIX 501.
	Current Kbps—Displays the current number of kilobits per second that cross the interface.
VPN Status	This area displays the status of your VPN tunnels, if they are configured.
Traffic Status	**Connection Per Second Usage**—Displays the information about Connections Per Second (TCP, UDP, and total) of traffic going through the device.
	outside Interface Traffic Usage (Kbps)—Displays the input and output traffic going through '**outside'** interface in Kilobits per second.
System Resources Status	**CPU**—Displays the percentage of CPU being utilized at the moment.
	CPU Usage (percent)—Displays the real time status of CPU usage and history for the last five minutes.
	Memory—Displays the total amount of memory being utilized at the moment.
	Memory Usage (percent)—Displays the real time memory usage and history for the last five minutes, in megabytes.
	Memory (MB)—Displays information about free, used and total memory in megabytes. Note that one megabyte is equal to 1,048,576 bytes.

Using the PDM Startup Wizard

By completing this wizard, your PIX Firewall is immediately enabled.

Note You can configure PDM manually using the online Help at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdm30olh.pdf

After PDM launches, you can access the PDM Startup Wizard at any time from the main PDM control panel as follows:

Step 1 On the PDM top menu, click **Wizards**>**Startup Wizard**.

Step 2 Read the **Welcome to the Startup Wizard** page and click **Next** when ready to continue.

Step 3 Fill in the configuration prompts according to your network security policies. Click **Next** at the end of each wizard page to go to the next set of prompts, or click **Back** to go back to the previous prompts.

For assistance with deciding what to enter into the Startup Wizard dialog boxes, click **Help**.

Step 4 When you have completed all the wizard pages, the **Startup Wizard Completed** page displays. To send the configuration to your PIX Firewall and exit the wizard, click **Finish**. Otherwise, click **Back** to make changes to previous pages.

VPN Wizard

Use the VPN Wizard panel to select the type of Virtual Private Network (VPN) tunnel that you are defining and to identify the interface on which the tunnel will be enabled. A VPN tunnel provides secure communication over an insecure network, such as the public Internet, by encrypting traffic between two IPSec peers, such as your local PIX Firewall and a remote PIX Firewall or VPN concentrator.

To configure a secure tunnel, first decide if you are using your PIX Firewall to provide remote access to your local area network (LAN), or to provide connectivity to a LAN in another geographic location. Next, identify the interface to use to connect to the remote IPSec peer. If your PIX Firewall has only two interfaces, this will always be the lower security interface, which is named “outside” by default. If your PIX Firewall has multiple interfaces, you should plan your VPN configuration before running this wizard and identify the interface to use for each remote IPSec peer with which you need to establish secure connectivity.

To set up your PIX Firewall as a remote access client in relation to another PIX Firewall or Cisco VPN Concentrator, select the Startup Wizard from the Wizards menu.

You can configure the VPN Wizard as follows:

- Site-to-Site VPN, page 4-5
- Remote Access VPN, page 4-5
- Select Interface, page 4-6

Site-to-Site VPN

This configuration is used between two IPSec security gateways, which can include PIX Firewalls, VPN concentrators, or other devices that support site-to-site IPSec connectivity. When you select this option, a series of panels are displayed lets you enter the configuration required for this type of VPN. With a site-to-site VPN, your local PIX Firewall provides secure connectivity between your LAN and a LAN in a different geographic location.

Remote Access VPN

This configuration is used to allow secure remote access for VPN clients, such as mobile users. A remote access VPN lets remote users securely access centralized network resources. When you select this option, the system displays a series of panels that let you enter the configuration required for this type of VPN. With a remote access VPN, your local PIX Firewall provides secure connectivity between individual remote users and the LAN resources protected by your local PIX Firewall.

Select Interface

Use the selection list to select the interface on which the current VPN tunnel will be enabled. The outside interface is the lower security interface on your PIX Firewall, while the inside interface is the higher security interface.

Configuring VPN Tunnels

If you have never configured VPN tunnels before, use the VPN Wizard to begin: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdm30olh.pdf. By completing this wizard, your PIX Firewall is immediately configured to enforce network security policy as specified by you during the wizard prompts.

For information on configuring VPN tunnels, see the online Help for VPN Wizard at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdm30olh.pdf

Configuration Recommendations

For best performance when running Windows, use Internet Explorer versions 5.5 or 6.0 without the Java plug in or with the Java Plug in, but not as the default JVM. PDM Version 3.0 supports the Java plug in for browsers.

When using Windows 2000 or later, fastest loading of PDM can be achieved by editing the Windows configuration file "`hosts`".

Step 1 Locate the hosts file. Under Windows 2000, the location of the hosts file is:

```
C:\WINNT\system32\drivers\etc\hosts
```

Step 2 Select the file, right click, and select **Open With>Notepad**.

Step 3 Follow the Microsoft instructions in the hosts file to add your PIX Firewall IP address and host name.

Step 4 Save the hosts file to the original location.

```
Copyright (c) 1993-1999 Microsoft Corp.
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.

This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.

Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.

For example:

102.54.94.97 rhino.example.com # source server
38.25.63.10 x.example.com # x client host
```

Tips and Troubleshooting

This chapter provides tips on using PDM and instructions on basic PDM troubleshooting symptoms and workarounds. Use this information prior to contacting the Technical Assistance Center (see the "Preface").

This chapter includes the following topics:

Checking Your Connection to the PIX Firewall

To communicate with the PIX Firewall, your computer should have an IP address and, if it is located on different LAN, your computer should be configured with a route to the PIX Firewall.

To set the default gateway IP address, refer to the *Cisco PIX Firewall and VPN Configuration Guide.*

If you cannot access the PIX Firewall through PDM, follow these steps:

Step 1 Enter **`show ip interface inside`** at the console command prompt to check that the IP address you typed into your web browser is the same IP address that you assigned to the inside interface of your PIX Firewall; these IP addresses must be the same to make a connection.

Step 2 Check the networking setup of your console workstation to see how it is connected to the PIX Firewall.

Step 3 Check that your network cabling is connected.

If you are connecting a workstation directly to the PIX Firewall unit's Ethernet interface, use a cross-over cable or add a hub or switch between your computer and the PIX Firewall.

Step 4 If the LEDs indicate the system is not working, ping the PIX Firewall unit's interface IP address. For example, if the inside interface's IP address is 10.1.1.1, enter the following command to ping the PIX Firewall:

```
ping 10.1.1.1
```

If the ping is unsuccessful, there is a power or network connectivity problem.

Note If your console operating system supports a **traceroute**, **tracert**, or similar command, use it to troubleshoot the route between your computer and the PIX Firewall unit.

Step 5 You can connect to PDM from a browser by entering the following command:

https://*pix_inside_interface_ip_address*

Note Remember to add the "**s**" to "**https**" or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the PIX Firewall that you are using PDM to configure or monitor.

Step 6 If you are still unable to access PDM from your browser, verify that the following conditions exist:

a. You are running PIX Firewall software Version 6.3. To determine your software version, enter the **show version** command and check the first line of the command output.

b. You have PDM Version 3.0 installed. To determine if PDM Version 3.0 is installed on your PIX Firewall unit, enter the **show version** command and check the second line of the command output.

c. You have an HTTP server enabled. To determine if you have HTTP server enabled, enter the **show http** command and check the first line of the command output.

d. Your PIX Firewall unit is allowing your PC/workstation to access PDM. To determine if your PIX Firewall unit is allowing your PC/workstation to access PDM, enter the **show http** command and check the command output.

Step 7 If you still cannot access PDM from your browser, refer to the "Preface".

Tips on Using PDM

For ease when using PDM, follow these tips:

- You can view the size of your configuration from the PIX Firewall console. Either connect a computer to the PIX Firewall unit or use Telnet to access the console.

  After entering the enable mode password, use the **show flashfs** command to view the configuration size, as shown in the following example:

```
pixdoc515(config)# show flashfs
flash file system:  version:2  magic:0x12345679
  file 0: origin:       0 length:1511480
  file 1: origin: 2883584 length:1639
  file 2: origin:       0 length:0
  file 3: origin: 3014656 length:4311804
  file 4: origin: 8257536 length:280
```

  The "file 1" line lists the number of characters in your configuration after the "length" parameter. In this example, the configuration consists of 1639 characters. Divide this number by 1024 to view the number of kilobytes. The configuration in this example is slightly more than 1.6 KB.

- The first time you use PDM with a PIX Firewall, PDM asks permission to save PDM-specific commands to your PIX Firewall configuration. These commands are necessary to update PDM's network topology information and do not change your network security policy on the PIX Firewall. When prompted, you can choose not to accept these commands, but without the network topology information, PDM can only monitor your PIX Firewall. Consequently, not accepting these commands limits your access in PDM to the Monitoring tab.

- For Microsoft Internet Explorer web browsers, when prompted to accept certificates select the **Always trust content from Cisco Systems** check box so that the certificate is automatically accepted the next time you run PDM.
- For Netscape Communicator or Navigator, select the **Remember this decision** check box so that the certificate is automatically accepted when you run PDM.
- The following conditions can affect the performance of PDM on your workstation:
  - You can run several PDM sessions on a single workstation. The maximum number of PDM sessions you can run varies depending on your workstation's resources such as memory, CPU speed, and browser type.
  - The time required to download the PDM applet can be greatly affected by the speed of the link between your workstation and the PIX Firewall unit. A minimum of 56 Kbps link speed is required; however, 3.84 Mbps or higher is recommended. Once the PDM applet is loaded on your workstation, the link speed impact on PDM operation is negligible.
  - If your workstation’s resources are running low, you should close and reopen your browser before launching PDM.

For information on PDM caveats, refer to the “Caveats” section of the *Cisco PIX Device Manager Release Notes Version 3.0*.

Troubleshooting

For information on PDM caveats, refer to the caveats section of the *Cisco PIX Device Manager Release Notes Version 3.0*.

Table 5-1 contains basic PDM troubleshooting scenarios.

Table 5-1 Common Troubleshooting Symptoms, Conditions, and Workarounds

Symptom	Conditions	Workaround
Browser asks for acceptance of the security certificate again.	The host name or domain name has changed.	This is normal. Accept the security certificates again. (If you change the host name or domain of the PIX Firewall unit, the browser asks you to accept the new security certificate.)
Browser asks for the password again.	If you change the password on the PIX Firewall unit, the browser might ask you to reenter the password for authentication. If you use the Java Plug-in, the browser will prompt you for your username and password twice.	Keep track of new and changed passwords.

Table 5-1 Common Troubleshooting Symptoms, Conditions, and Workarounds (continued)

Symptom	Conditions	Workaround
Certificate displays a message that its timestamp is in the future when connecting to the PIX Firewall.	The browser displays a message with the certificate's timestamp each time a user connects to the PIX Firewall.	To reset the PIX Firewall clock setting, go to the **Configuration>System Properties> Administration>Clock** screen on PDM. Using PDM, look at the VPN screen under **IKE>Certificate>Enrollment** to check the timestamp on the certificate. Alternatively, you can also use the **show ca certificate** command to check the timestamp on the certificate.
Browser cannot access PDM.	When you attempt to access PDM, the message "the page cannot be displayed" appears in Internet Explorer or the message "network connection was refused by the server" appears in Netscape Communicator.	1. Check that you are using "**https"** in your connection to "`https://pix_inside_interface_ip_address`" and not "http." The connection cannot be made using "http," it must be "**https**." 2. If you cannot connect, enter the **show version** command to check that you have the proper activation key to use DES or 3DES. If you do not, obtain an activation key that supports this requirement before continuing. If, after confirming that your activation key supports using DES or 3DES, you still cannot connect, refer to "Checking Your Connection to the PIX Firewall".
Clicking **Grant** causes PDM to crash.	If you are using PDM with Netscape Version 4.73 and you have a corrupted certificate database, the browser may crash if you do the following: 1. Run an applet that uses a digital certificate. 2. Renew the certificate. 3. Run the new applet with the updated certificate. 4. Start PDM. 5. Click **Grant** to launch PDM. This can happen on Windows, Sun Solaris, or Linux and is a problem in the Netscape Java Virtual Machine (JVM).	To work around this, remove the corrupted cert7.db file (the certificate database file), located in the your Netscape directory. A new cert7.db file is created when you run Netscape again. However, this removes all of the certificates that you have previously accepted as trusted. (This includes certificates that you accepted from other sites as well as certificates that you entered manually.)

Table 5-1 Common Troubleshooting Symptoms, Conditions, and Workarounds (continued)

Symptom	Conditions	Workaround
Help files appear corrupted.	This can occur when you are using Microsoft Internet Explorer 5.0 and do not have HTTP 1.1 enabled. This can occur because PDM compresses the online Help files and Internet Explorer requires HTTP 1.1 to be enabled to handle compressed files properly.	In Internet Explorer, click **Tools**>**Internet Options**>**Advanced**. Scroll down to **HTTP 1.1 settings**. Select the **Use HTTP 1.1** check box. Click **Apply**. Close and restart your browser. If you are using a proxy server, select the **Use HTTP 1.1 through proxy connections** check box.
Some graphics or icons do not display properly.	PDM is being run with a Java Plug-in that is not supported (PDM supports Java Plug-ins 1.3.1, 1.4.0, and 1.4.1).	If you have the Java Plug-in installed, confirm that it is your default Java Virtual Machine (JVM). Do the following to ensure that the Java Plug-in is your default JVM: In Internet Explorer, click **Tools**>**Internet Options**. Click the **Advanced** tab. Scroll down. Look for a **Java (Sun)** section. If there is one, confirm that **Use Java 2** is checked. In Netscape, click **Edit**>**Preferences**. Click **Advanced**. Make sure the **Enable Java Plugin** check box is checked.
User cannot access PDM.	If more than five users try to access a single PIX Firewall unit using PDM, this exceeds the maximum number of simultaneous sessions allowed. The maximum number is five users in the current version.	1. If more than five users need to access a PIX Firewall, one or more can use a PIX Firewall console session via Telnet. 2. If you know that a PDM administrator's session is idle and wish to disconnect it, access the **PDM Users** panel on the Monitoring tab. 3. If you know the IP address of the idle connection, select the row, and click **Disconnect**. Another administrator can now access PDM.

Table 5-1 Common Troubleshooting Symptoms, Conditions, and Workarounds (continued)

Symptom	Conditions	Workaround
PDM launches slowly.	The startup speed of PDM depends on the amount of available RAM in your computer and whether virus scanning software is running on your computer.	1. You can increase your available RAM by closing other applications. 2. The time required to download the PDM applet can be greatly affected by the speed of the link between your workstation and the PIX Firewall unit. A minimum of 56 Kbps link speed is required; however, 3.84 Mbps or higher is recommended. Once the PDM applet is loaded on your workstation, the link speed impact on PDM operation is negligible. 3. See Load Time Improvements in "PC/Workstation Requirements" in Chapter 1.

Performance of PDM is slow.	When using the Java Plug-in and accessing your PIX Firewall using an IP address instead of a host name, the performance of PDM is dramatically slower. This occurs if the PIX Firewall host name is not in DNS or in the local hosts file.	Assure that the PIX Firewall host name is in DNS. If you are running Windows, and there is no DNS in your network or your DNS does not have the PIX Firewall entry, modify the "hosts" file.
		• On Windows NT, 2000, and XP, the hosts file is located at C:\WINNT\system32\drivers\etc\hosts.
		• On Windows 98 and ME, it is at C:\Windows\hosts.
		Each line in the hosts file is in the format "<ip> <hostname>". For example:
		`192.168.1.1`
		`pixfirewall.example.com`

There is access only to the Monitoring tab in PDM.	The use of certain PIX Firewall CLI commands, and certain command combinations, limit access in PDM to the Monitoring tab.	For more information on these commands and command combinations, see the *Cisco PIX Device Manager Release Notes Version 3.0*.

Using a TFTP Server

This appendix describes how to use a TFTP server to access PIX Firewall or PDM images. You must have a TFTP or FTP server to install the PIX Firewall software.

You must have an activation key that enables Data Encryption Standard (DES), the more secure 3DES, or AES which PDM requires for support of the Secure Sockets Layer (SSL) protocol. If your PIX Firewall is not enabled for DES, you can have a new activation key sent to you by completing the form at the following website:
http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324

This section includes the following topics:

Obtaining a Windows TFTP Server

The Microsoft Windows based TFTP server previously provided by Cisco Systems has been discontinued and is no longer supported by Cisco Systems. This software suffers from a security bug described in (http://online.securityfocus.com/bid/2886). Persons still using the server should consider replacing it with any of the high quality freeware and shareware TFTP servers.

As a historical note, the Cisco TFTP server was released to customers in 1995 and at a time when no other freely available TFTP servers existed. Today, there are many TFTP servers available that can be easily found by searching for “tftp server” on your internet search engine. We do not specifically recommend any particular TFTP implementation.

It is also useful to note that modern versions of Cisco IOS software also support the use of FTP instead of TFTP for loading of images or configuration files. Use of FTP overcomes a number of inherent limitations of TFTP including a lack of security and a 16 MB file size limitation.

Enabling UNIX TFTP Support

The procedure for enabling TFTP access on your workstation varies depending on your operating system.

This section contains the following topics:

Enabling TFTP Access on a Sun Solaris System

Follow these steps to enable TFTP access on a Sun Solaris system:

Step 1 Log in as root.

Step 2 Add or uncomment the following line in your /etc/inetd.conf file:

```
tftp    dgram   udp     wait    root    /usr/sbin/in.tftpd  in.tftpd
```

Step 3 Specify the TFTP directory. By default it is /tftpboot unless you append "-s <directory>" in the previous step. View the in.tftpd man page for more information.

Step 4 Either reboot your system or use the following commands to find the "inetd" process and send it the SIGHUP signal to force it to reread the inetd.conf file:

```
/bin/ps -ef | grep inetd
kill -1 inetd_process_ID
```

Enabling TFTP Access on a Linux System

Follow these steps to enable TFTP access on a Linux system:

Note If you use Linux, these steps vary depend on whether or not you are using "inetd" or "xinetd." If you have the file "/etc/inetd.conf," you are using inetd. RedHat 7.0 uses "xinetd."

Step 1 Log in as root.

Step 2 If you are running Linux with "inetd," add or uncomment the following line in your /etc/inetd.conf file:

```
tftp    dgram   udp     wait    root    /usr/sbin/tcpd  in.tftpd
```

If you are running Linux with "xinetd," Edit the /etc/xinetd.d/tftp file as follows:

a. Change the line "disable = yes" to "disable = no."

b. Change the line "user = nobody" to "user = root."

c. If you want to specify a different TFTP directory, replace "/tftpboot" in the line "server_args = -s /tftpboot" with the name of your directory.

Step 3 Enter the following command:

```
/etc/init.d/xinetd restart
```

TFTP Download Error Codes

PDM cannot be downloaded via TFTP from the PIX Firewall unit's monitor mode. You must use the **copy tftp flash:pdm** command described in Chapter 3, "Installing PDM."

During a TFTP download, non-fatal errors may appear in the midst of dots that display as the software downloads. The error code appears inside angle brackets. Table A-1 lists the code values.

For example, random bad blocks appear as follows:

```
....<11>..<11>.<11>......<11>...
```

Also, the display may show "A" and "T" for ARP and timeouts, respectively. Receipt of non-IP packets causes the protocol number to display inside parentheses.

Table A-1 TFTP Error Code Numeric Values

Error Code	Description
-1	Timeout between the PIX Firewall and TFTP server.
2	The packet length as received from the Ethernet device was not big enough to be a valid TFTP packet.
3	The received packet was not from the server specified in the **server** command.
4	The IP header length was not big enough to be a valid TFTP packet.
5	The IP protocol type on the received packet was not UDP, which is the underlying protocol used by TFTP.
6	The received IP packet's destination address did not match the address specified by the **address** command.
7	The UDP ports on either side of the connection did not match the expected values. This means either the local port was not the previously selected port, or the foreign port was not the TFTP port, or both.
8	The UDP checksum calculation on the packet failed.
9	An unexpected TFTP code occurred.
10	A TFTP transfer error occurred.
-10	The image filename you specified cannot be found. Check the spelling of the filename and that permissions permit the TFTP server to access the file. In UNIX, the file needs to be world readable.
11	A TFTP packet was received out of sequence.

Error codes 9 and 10 cause the download to stop.

A

C

D

F

H

I

J

K

L

M

N

P

S

T

V

W