Installation and Configuration for Common Criteria EAL4 Evaluated Cisco Adaptive Security Appliance, Version 7.0(6)

March 2007

Contents

This document describes how to install and configure the Cisco PIX Security Appliance Version 7.0(6) and the Cisco ASA 5500 Series Security Appliance 7.0(6) as certified by Common Criteria Evaluation Assurance Level 4 (EAL4).

In this guide, “security appliance” and “adaptive security appliance” apply to all models of the Cisco PIX Security Appliance Version 7.0(6) and the Cisco ASA 5500 Series Security Appliance 7.0(6), unless specifically noted otherwise.

Note Failure to follow the information provided in this document will result in the adaptive security appliance not being compliant with the evaluation and may make it insecure.

This document includes the following sections:

Americas Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

A printed version of this document is an uncontrolled copy. Company Confidential

OL-12987-01

Introduction

This document is an addendum to the Cisco PIX Security Appliance Version 7.0(6) and the Cisco ASA 5500 Series Security Appliance 7.0(6) documentation set, which should be read before configuring the security appliance.

Cisco product documentation includes:

- Release Notes
  - *Cisco PIX Security Appliance Release Notes*
  - *Cisco ASA 5500 Series Release Notes*
- Quick Start Guides
  - *Cisco PIX 515E Security Appliance Quick Start Guide*
  - *Cisco ASA 5500 Quick Start Guide*
- Hardware Installation Guides
  - *Cisco PIX Security Appliance Hardware Installation Guide*
  - *Cisco ASA 5500 Hardware Installation Guide*
- Regulatory Compliance and Safety Information Guides
  - *Cisco PIX Security Appliance Regulatory Compliance and Safety Information*
  - *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- Command Line Configuration Guide
  - *Cisco Security Appliance Command Line Configuration Guide*
- Command Reference Guides
  - *Cisco Security Appliance Command Reference*
- System Log Messages Guide
  - *Cisco Security Appliance System Log Messages*

The security appliance documentation is available on CD-ROM, in printed-paper form, and online (in both HTML and PDF formats). This document should be used in conjunction with the August 2005 edition of the CD-ROM based documentation.

Audience

This document is written for administrators configuring the Cisco PIX Security Appliance Version 7.0(6) and the Cisco ASA 5500 Series Security Appliance 7.0(6) software. This document assumes you are familiar with networks and network terminology, that you are a trusted individual, and that you are trained to use the Internet and its associated terms and applications.

Supported Hardware and Software Versions

Only the following combinations of hardware listed in Table 1 are compliant with the security appliance 7.0(6) EAL4 evaluation. Using hardware not specified invalidates the secure configuration. Likewise, using any software version other than the Cisco PIX Security Appliance Version 7.0(6) and the Cisco ASA 5500 Series Security Appliance 7.0(6) will invalidate the secure configuration.

Table 1 Supported Hardware for the Certified PIX Firewall

Models	Optional Hardware Modules	Maximum Number of Interfaces
PIX 515[1]/515E[1]	PIX-1FE PIX-4FE	6
PIX 525[1]	PIX-1FE PIX-4FE PIX-1GE-66	8
PIX 535[1]	PIX-1FE PIX-4FE PIX-1GE-66	10

1. These models may have AC or DC power supplies.

Table 2 Supported Hardware for the Certified Cisco ASA 5500 Series Security Appliance

Models	Optional Hardware Modules	Maximum Number of Interfaces
ASA 5510	4GE SSM	9
ASA 5520	4GE SSM	9
ASA 5540	4GE SSM	9

The PIX Firewall Syslog Service (PFSS) version that is included in this evaluation is 5.1(3).

Security Information

In addition to the *Regulatory Compliance and Safety Information* documentation, the sections that follow provide additional security information for use with a Common Criteria Certified adaptive security appliance.

Organizational Security Policy

Ensure that your security appliance is delivered, installed, managed, and operated in a manner that maintains an organizational security policy. The *Cisco Security Appliance Command Line Configuration Guide* provides guidance on how to define a security policy.

Security Implementation Considerations

The sections that follow provide implementation considerations that need to be addressed to administer the security appliance in a secure manner.

Certified Configuration

Use only the security appliance software Version 7.0(6). Only the hardware version combinations listed in Table 1 and Table 2 can be used to implement an evaluated configuration. Changing the software to a different version invalidates the evaluated status of a particular hardware platform.

The Certified Common Criteria adaptive security appliance 7.0(6) does not support the following features:

- Cut-through proxies
- Routing Information Protocol (RIP)
- Simple Network Management Protocol (SNMP)
- Dynamic Host Configuration Protocol (DHCP) Server
- Virtual Private Networks (VPNs)

All other hardware and software features and functions of the security appliance are included in the evaluated product configuration as long as they are configured, operated, and managed in accordance with this document.

The Cisco PIX Security Appliance Version 7.0(6) and the Cisco ASA 5500 Series Security Appliance 7.0(6) Target of Evaluation relies on a Windows 2000 or Windows XP computer to act as an audit server. Windows 2000 or Windows XP is configured in the EAL 4 evaluated configuration to support this evaluation. Microsoft Windows 2000 or Windows XP evaluated configuration documentation can be found at the following links:

Windows 2000 Documentation

- Windows 2000 Common Criteria Evaluated Configuration User's Guide: http://www.microsoft.com/technet/security/prodtech/Windows2000/w2kccug/default.mspx
- Windows 2000 Common Criteria Evaluated Configuration Administrator's Guide: http://www.microsoft.com/technet/security/prodtech/windows2000/w2kccadm/default.mspx
- Windows 2000 Common Criteria Security Configuration Guide: http://www.microsoft.com/technet/security/prodtech/windows2000/w2kccscg/default.mspx

Windows XP Documentation

- Windows XP Common Criteria Evaluated Configuration User's Guide: http://download.microsoft.com/download/d/3/0/d304ab38-567c-4fad-a368-a3661ca1a16d/wxp_common_criteria_user_guide.zip
- Windows XP Common Criteria Evaluated Configuration Administrator's Guide: http://download.microsoft.com/download/e/8/9/e897a1ee-0273-4694-b155-ad02f7b2b4d5/wxp_common_criteria_admin_guide.zip
- Windows XP Common Criteria Security Configuration Guide: http://download.microsoft.com/download/5/3/b/53b53a3e-39d5-4d30-86f2-146aa2c7be45/wxp_common_criteria_configuration_guide.zip

The configuration of the security appliance should be reviewed on a regular basis to ensure that the configuration continues to meet the organizational security policy in the face of the following:

- Changes in the security appliance configuration
- Changes in the organizational security policy
- Changes in the threats presented from the untrusted network(s)
- Changes in the administration and operation staff or the physical environment of the security appliance

Physical Security

The security appliance must be located in a physically secure environment to which only a trusted administrator has access. The secure configuration of the security appliance can be compromised if an intruder gains physical access to the security appliance. Similarly, the audit server used to store and manage the security appliance system log messages must be protected physically and with suitable identification/authentication mechanisms to ensure that only trusted administrators have access.

Modes of Operation

Firewall

The firewall component of the product has three modes of operation: audit trail full, routed and transparent modes. The authorized administrator can configure the security appliance to run in routed or transparent mode. In either of these modes the security appliance can be configured to run as a single

context or as multiple contexts. If multiple context is chosen, all the contexts have to run as either routed or transparent, a mixture of both is not allowed. For more information, see the "Security Context Overview" section in the *Cisco Security Appliance Command Line Configuration Guide, Version 7.0*.

Routed Mode

This is the default mode set on the security appliance. The IP address of the security appliance can be seen on the outside network. The product allows for Network Address Translation to be configured in this mode.

Transparent Mode

In transparent mode the IP address of the security appliance is not visible to the outside network. Traffic being sent has to be addressed to its end destination. Network Address Translation cannot be configured in this mode. When modes are changed the security appliance clears the previously configured mode as some commands are not usable in both modes. In either routed or transparent mode access lists have to be configured to allow traffic to flow.

Audit Trail Full Mode

As a default, when the Audit Server becomes full or unavailable, any traffic arriving at a network interface will not be allowed to pass through the security appliance. Should the authorized administrator discover that traffic is passed through the appliance when the Audit Server is full or unavailable the 'logging no permit-hostdown' command must be used to reactivate Audit Trail Full Mode, otherwise auditable events may occur without being recorded in the audit trail.

Audit Server

The Audit Server has two modes of operation, PFSS Active and Log Searching. These two modes are separate from one another and can run concurrently or only one can be active at a time.

PFSS Active Mode

This mode is the PIX Firewall Syslog Server application running on the Audit Server and waiting for audit event details to be transferred from the firewall component. The application listens for TCP connections from the firewall component and records any transferred audit event details in files held by the Audit Server operating system. If the application is not running no audit event details are recorded and auditable events may occur without being noticed (see the Audit Trail Full Mode, above).

Log Searching Mode

This mode is the Search/Sort application running on the Audit Server and being used by an authorized administrator to view audit event details. The application is a standard executable that can be started and stopped by a user with the correct privileges, specifically an authorized Audit Server Administrator. If the application has not been started or has been stopped it cannot be used to view audit event details. The files held by the Audit Server operating system that contain the audit event details cannot be modified by the Search/Sort application.

Potential Insecure Configurations (Misuse)

Uncommitted Changes

The security appliance loads the saved startup configuration and automatically copies this configuration into the running configuration. As a user configures the running configuration to his specific needs he either saves the running configuration or saves the updated configuration to the startup configuration. The running configuration is held in volatile memory so if the security appliance is reloaded due to either operational reasons or operational error and any changes have not been saved these changes will be lost.

Default Flow Policy

When installed the security appliance, by default, is configured with a default DHCP address pool. The outbound interface disallows all external to internal data flows. The administrator needs to be aware of this, and ensure that the correct policy for the organization is installed and committed before users are permitted to use the security appliance. Access Lists are required to be set up to enable traffic to flow through the security appliance. Specific permit or deny rules are required to be applied to a protocol, a source and destination IP address or Network and optionally, the source and destination ports.

Audit Configuration

In order that Time-Stamping is enabled the following command must be entered by the firewall administrator: ‘logging timestamp’. Once this command is committed by the use of the command ‘write memory’ this will remain the default.

By default, auditing events are transported to remote syslog servers over UDP. To ensure that audit events are reliably delivered to the remote syslog server the TCP option should be employed. The command ‘logging host <ip-address> tcp/<port-number>’ is used to achieve this.

Administration Access

There are only two methods by which the administrator can manage the security appliance:

- Using the serial interface directly connected to the security appliance
- Using SSH access

Servers and Proxies

To ensure complete security when the security appliance is shipped, inbound access to all proxies and servers is initially disabled. After the installation, you must explicitly permit each service and enable the services necessary for your security policy. Use the **show logging** command or the Security Appliance Syslog Server to view log file messages. Refer to the *Cisco Security Appliance Command Line Configuration Guide* for information on how to configure the security appliance. Certification requires a completely controlled environment in which specified services are allowed and all others denied.

Logging and Messages

Monitoring activity in the log files is an important aspect of your network security and should be conducted regularly. Monitoring the log files lets you take appropriate and timely action when you detect security breaches or events that are likely to lead to a security breach in the future. Use the **show logging** command or the Security Appliance Syslog Server to view log files messages. Refer to the *Cisco Security Appliance System Log Messages* for information on sending messages, and archiving.

Access Lists

The **access-list** command operates on a first-match basis. Therefore, the last rule added to the access list is the last rule checked. Administrators must take note of this when entering the initial rules during the configuration, as it may impact the remainder of the rule parsing.

Trusted and Untrusted Networks

The security appliance can be used to isolate your network from the Internet or from another network. A trusted network is usually your internal network and an untrusted network may be the Internet or any other network. Therefore, the security appliance must be configured so that it acts as the only network connection between your internal network and any external networks. The security appliance will deny any information flows for which no rule is defined. Your security implementation is based on the control of traffic from one network to the other, and should support your security policy.

PFSS is the Windows Syslog service that provides the system audit store for the firewall. The PFSS shall be configured to communicate with the firewall dependent on the mode the firewall is operating in.

If the firewall is operating in single context mode, the PFSS server is required to have its own defined interface for communication. The ‘logging host’ command in this instance is configured to log messages over Syslog TCP to the audit server on the interface.

Figure 1 Single Context

If the firewall is operating in multiple context mode each context shall be defined to communicate with the audit server and configuration settings to protect the audit server from receiving any other traffic other then that which is specifically allowed per policy.

When the firewall runs in transparent mode, the outgoing interface of a packet is determined by performing a MAC address lookup instead of a route lookup. Route statements can still be configured, but they only apply to security appliance-originated traffic. For example, if your syslog server is located on a remote network, you must use a static route so the security appliance can reach that subnet.

Figure 2 Multiple Context

Note To ensure proper protection of the audit server the PFSS server must be placed on a trusted network and must have access-control lists applied on the firewall to only allow TCP syslog data to the PFSS.

In this example, the PFSS server is configured with IP address 1.2.3.4 and the firewall is sending system logs from 3.4.5.6. If multiple contexts are being used, additional lines will need to be added to the access-list.

```
hostname(config)# access-list INSIDE extended permit tcp host 3.4.5.6
host 1.2.3.4 eq 1470
hostname(config)# access-group INSIDE in interface inside
```

Note Separate physical switches must be used between each network attached to the firewall to ensure that the firewall will not be bypassed by any Layer 2 attacks against directly connected switches.

Table 3 In Default Configuration, Traffic Types Observe The Default Policy For Inside To Outside Traffic

Traffic Type	Single Routed Mode	Multiple Routed Mode	Single Transparent Mode	Multiple Transparent Mode
Spoofed Traffic	No (RPF enabled)	No (RPF enabled)	No (ARP inspection enabled)	No (ARP inspection enabled)
Ethernet	Yes	Yes	Yes	Yes
ARP	No(Router hop)	No(Router hop)	Yes	Yes
CTIQBE	Yes	Yes	Yes	Yes
DNS	Yes	Yes	Yes	Yes
Echo	Yes	Yes	Yes	Yes
Finger	Yes	Yes	Yes	Yes
H.323	Yes	Yes	Yes	Yes
IP	Yes	Yes	Yes	Yes
ICMP	Yes	Yes	Yes	Yes
TCP	Yes	Yes	Yes	Yes
UDP	Yes	Yes	Yes	Yes
FTP	Yes	Yes	Yes	Yes
GTP	Yes	Yes	Yes	Yes
HTTP	Yes	Yes	Yes	Yes
ILS	Yes	Yes	Yes	Yes
MGCP	Yes	Yes	Yes	Yes
POP3	Yes	Yes	Yes	Yes
RSH	Yes	Yes	Yes	Yes
RTSP	Yes	Yes	Yes	Yes
Skinny	Yes	Yes	Yes	Yes
SIP	Yes	Yes	Yes	Yes
ESMTP	Yes	Yes	Yes	Yes
SunRPC	Yes	Yes	Yes	Yes
Telnet	Yes	Yes	Yes	Yes
TFTP	Yes	Yes	Yes	Yes
XDMCP	Yes	Yes	Yes	Yes
traceroute	Yes	Yes	Yes	Yes
STP	No	No	Yes	Yes
All other Traffic	Yes	Yes	Yes	Yes

Table 4 In The Default Configuration, Traffic Types Observe The Default Policy For Outside To Inside Traffic

Traffic Type	Single Routed Mode	Multiple Routed Mode	Single Transparent Mode	Multiple Transparent Mode
Spoofed Traffic	No (RPF enabled)	No (RPF enabled)	No (ARP inspection enabled)	No (ARP inspection enabled)
Ethernet	No	No	Yes	Yes
ARP	No (Router hop)	No (Router hop)	No	No
CTIQBE	No	No	No	No
DNS	No	No	No	No
Echo	No	No	No	No
Finger	No	No	No	No
H.323	No	No	No	No
IP	No	No	No	No
ICMP	No	No	No	No
TCP	No	No	No	No
UDP	No	No	No	No
FTP	No	No	No	No
GTP	No	No	No	No
HTTP	No	No	No	No
ILS	No	No	No	No
MGCP	No	No	No	No
POP3	No	No	No	No
RSH	No	No	No	No
RTSP	No	No	No	No
Skinny	No	No	No	No
SIP	No	No	No	No
ESMTP	No	No	No	No
SunRPC	No	No	No	No
Telnet	No	No	No	No
TFTP	No	No	No	No
XDMCP	No	No	No	No
traceroute	No	No	No	No
STP	No	No	Yes (can be denied by acl)	Yes (can be denied by acl)
All other Traffic	No	No	No	No

Public Access Servers

If you are planning to host public access servers, you must decide where they will be located in relation to the security appliance. Placing servers on the network outside the security appliance leaves them open to attack. Placing servers on the internal network means you must open up your security appliance to allow access.

Using FTP

File Transfer Protocol (FTP) is used to retrieve or deposit files on a remote system. Telnet is used to access a remote server using a console like connection over the network. The Common Criteria Security Target requires that Telnet and FTP traffic through the security appliance must be authenticated before traffic is allowed to pass through. For more information on how to properly configure the security appliance to authenticate Telnet and FTP see the "Configuring Authentication for Network Access" section in the *Cisco Security Appliance Command Line Configuration Guide*.

Monitoring and Maintenance

The security appliance software provides several ways to monitor the security appliance, from logs to messages.

- Ensure you know how you will monitor the security appliance, both for performance and for possible security issues.
- Plan your backups. If there should be a hardware or software problem, you may need to restore the security appliance configuration.
- The configuration of the security appliance should be reviewed on a regular basis to ensure that the configuration meets the security objectives of the organization in the face of the following:
  - Changes in the security appliance configuration
  - Changes in the security objectives
  - Changes in the threats presented by the external network

Administrative Roles

The certified configuration contains two administrative roles for use in the evaluated configuration:

Table 5 Administrative Roles in Evaluated Configuration

Role Name	Description
Authorized Firewall Administrator	Any administrator with knowledge of the 'enable' password on the firewall. Privileged access is defined by any privilege level entering an enable password after their individual login.
Authorized Audit Administrator	The role assigned to a user that logs in and reviews the information recorded by the PFSS application.

Auditing Component Requirements

The security appliance interacts with the Windows server for the purpose of storing the audit data. The server should be running Windows 2000 with Service Pack 4 or Windows XP with Service Pack 2. The auditing machine will provide suitable audit records to the administrator, protect the stored audit records from unauthorized deletion, and will detect modifications to the audit records. It is the responsibility of the administrator to regularly review the audit records provided by the security appliance, and to take any relevant action as necessary to ensure the security of the adaptive security appliance. The location of the auditing machine and records should only be accessible to the administrator.

Password Complexity

Passwords have to be a minimum of 8 characters in length and a maximum of 16 characters in length. The minimum password lengths must be enforced by the administrator. The following is a list of characters that are allow to be used in the password:

- 26 Upper case letters (A - Z)
- 26 Lower case letter (a – z)
- 10 Numbers (0 – 9)
- !"#$%&'()*+,-./:;<@[\` {|=>?]^_}~

This is a total of 94 characters that may be used to construct a password. The use of the space character is prohibited.

The password guidance included in this section applies to creation and management of user passwords. Users must ensure that when creating or changing a password, the following requirements are met:

1. Passwords must:
   - be a minimum of 8 characters and a maximum of 16 characters
   - include mixed-case alphabetic characters
   - include at least 1 numeric character
2. Passwords must not include:
   - birthdays
   - names (parents, family, spouse, pets, favorite sports player)
   - sports teams
   - towns, cities or countries

AAA Server and Authentication Policy per the IT Environment

The AAA server specified for this certified configuration is included within the environment. The administrator must ensure that during installation the AAA server is capable of the following:

- Maintaining attributes for each user (identity, association of human user to with the administrator account, and password).
- Firewall administrators shall authenticate using a Single-use authentication mechanism before being allowed to access the firewall remotely.
- Human users shall authenticate using a Single-use authentication mechanism when using FTP or Telnet that passes through the firewall.

- Reusable passwords are allowed for authorized administrators to access the firewall or router console directly using the local console.
- Reusable passwords may be used for the console connection and "enable" on the security appliance.

The IT environment section from the Security Target requires the administrator to follow guidance concerning what authentication types are required for each request to administer the certified configuration.

Determining the Software Version

Use the **show version** command to verify the software version of your security appliance unit.

Installation Notes

Read the *Cisco ASA 5500 Hardware Installation Guide* before installing the security appliance.

Verification of Hardware and Software Image

Complete these steps to verify that the security appliance software and hardware was not tampered with during delivery:

Step 1 Before unpacking the security appliance, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems barcoded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Note the serial number of the security appliance on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the security appliance. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Once the security appliance is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 7 There are three alternatives for obtaining a Common Criteria evaluated software image:

- Download a Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. To access this site, you must be a registered user and you must be logged in. Software images are available from Cisco.com at the following URL: http://www.cisco.com/cisco/pub/software/portal/select.html
- The security appliance ships with a CD containing all current software images. The Common Criteria evaluated software image Version 7.0(6) is available on this CD.
- Customers can order a CD with all of the current software images from Cisco.com. There is a charge for this option.

Step 8 Download the 706-k8.bin or pix 706.bin file.

Step 9 Once the file is downloaded, verify that it was not tampered with by using an MD5 utility to compute an MD5 hash for the downloaded file and compare this with the MD5 hash for the image from this document. If the MD5 hashes do not match, contact Cisco TAC. MD5 for both files is 27164a0652cc4fe86fe35370f98fe733.

Step 10 To copy the image that was downloaded from the web to flash, enter the following commands:

a. **copy tftp:/1.2.3.4/**asa706-k8.bin **disk0:**

b. boot system **disk0:/**cdisk.bin

c. **write memory**

d. **reload**

Step 11 Start your security appliance as described in the "Getting Started" chapter in the *Cisco Security Appliance Command Line Configuration Guide*. Confirm that your security appliance loads the image correctly and completes internal self-checks. At the prompt, enter the **show version** command as follows. Verify that the version is 7.0(6). If the security appliance image fails to load, or if the security appliance version is not 7.0(6), contact Cisco TAC.

The following is a sample output from the "**show version**" command output, showing the security appliance version:

```
hostname# show version
Cisco ASA Software Version 7.0(6)
PIX (7.0.1.0) #28: Mon XXX 23 15:37:25 EDT 2005
ASA up 21 mins 44 secs
Hardware: ASA5530-K8, 2048 MB RAM, CPU Pentium 4 Celeron 2500 MHz
Internal ATA Compact Flash, 489MB
Slot 1: ATA Compact Flash, 244MB
BIOS Flash M50FW016 @ 0xffe00000, 2048KB
Encryption hardware device: Cisco ASA-55x0 on-board accelerator (revision 0x0)
Boot microcode: CNlite-MC-Boot-Cisco-1.2
SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
IPSec microcode: CNlite-MC-IPSECm-MAIN-2.01
0: Ext: GigabitEthernet0/0: media index 0: irq 9
1: Ext: GigabitEthernet0/1: media index 1: irq 9
2: Ext: GigabitEthernet0/2: media index 2: irq 9
3: Ext: GigabitEthernet0/3: media index 3: irq 9
4: Ext: Management0/0: media index 0: irq 11
5: Int: No HWIDB: media index 4: irq 11
6: Int: Control0/0: media index 1: irq 5
License Features for this Platform:
Maximum Physical Interfaces: Unlimited
Maximum VLANs: 50
Inside Hosts: Unlimited
Failover: Enabled
VPN-DES: Enabled
VPN-3DES-AES: Enabled
Cut-through Proxy: Enabled
Guards: Enabled
```

```
URL-filtering: Enabled
Security Contexts: 20
GTP/GPRS: Disabled
VPN Peers: 5000
Serial Number: P3000000002
Running Activation Key: 0x881ed361 0x447555a8 0xac73bc44 0xb3f0f888 0x8e26f18b
Configuration register is 0x11
Configuration last modified by enable_15 at 15:55:27.399 UTC Mon XXX 23 2005
```

Configuration Notes

This section contains the following topics:

Saving Your Configuration

The **write memory** command should be used frequently when making changes to the configuration of the security appliance. If the security appliance reboots and resumes operation when uncommitted changes were made, these changes will be lost and the security appliance will revert to the last configuration saved.

Using the Established Command

Administrators are advised not to use the **established** command on the certified security appliance. Incorrect use of this command may give outside users greater access to inside systems than is intended, and for this reason its use is not recommended. For more details, go to the following website:

http://tools.cisco.com/security/center/publicationListing

Enabling Timestamps

By default, all audit records are not stamped with the time and date, which are generated from the system clock when an event occurs. The certifiedsecurity appliance requires that the timestamp option is enabled. To enable the timestamp of audit events, use the **logging timestamp** command. To ensure that the timestamp option remains the default, use the **write memory** command to save the option into the startup configuration.

Enabling Reliable Logging

By default, auditing events are transported to the remote syslog server over UDP. The certified security appliance requires auditing events to be transported over TCP. The TCP option is configured using the **logging host** interface *ip_address* **tcp**/*port_number* command. With TCP logging configured, new sessions through the certified security appliance will be disallowed if log messages cannot be forwarded to the remote host.

To facilitate the TCP logging function, the adaptive security appliance must be configured on a secure Windows server. For details on how to obtain and configure the logging function, see the "Using the Security Appliance Syslog Server" section on page 21.

Systems Logs

Cisco Security Appliance System Log Messages provides details on the security appliance system logs. The following sections are not supported on a certified security appliance:

- Security Appliance System Log
  - Receiving SNMP requests
  - Sending SNMP Traps
- Other Remote Management and Monitoring Tools
  - ASDM
  - Cisco Secure Policy Manager
  - SNMP Traps

Note Telnet is not supported on the certified security appliance. It is disabled by default.

Server Settings

You must install the ACS server. The following document provides information on installing the Cisco Secure ACS:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_eol_notices_list.html

Configure Authentication on the Security Appliance

To create a server group, add AAA servers to it, configure the protocol and add authentication to SSH, perform the following steps:

Note Only TACACS+ and RADIUS security protocols are included in the evaluated configuration. Do not select any of the other options for protocol under aaa-server. TACACS+ and RADIUS both require a password to authenticate to the server. The administrator is required to follow the guidance in this document when creating the RADIUS or TACACS+ password.

Step 1 Identify the server group name and the protocol. To do so, enter the following command:

```
hostname(config)# aaa-server server_group protocol {radius | tacacs+}
```

For example, to use RADIUS to authenticate network access and TACACS+ to authenticate CLI access, you need to create at least two server groups, one for RADIUS servers and one for TACACS+ servers.

You can have up to 15 single-mode server groups or 4 multi-mode server groups. Each server group can have up to 16 servers in single mode or up to 4 servers in multi-mode.

When you enter a **aaa-server protocol** command, you enter group mode.

Step 2 For each AAA server on your network, follow these steps:

Identify the server, including the AAA server group it belongs to. To do so, enter the following command:

```
hostname(config)# aaa-server server_group (interface_name) host server_ip password
```

When you enter a **aaa-server host** command, you enter host mode.

After the aaa-server and group are configured, use the following commands to configure authentication.

```
hostname(config)# aaa authentication enable console [server-tag | LOCAL]
```

The security appliance allows SSH connections to the security appliance for management purposes. The security appliance allows a maximum of 5 concurrent SSH connections per context, if available, with a maximum of 100 connections divided between all contexts. SSH sessions in the evaluated configuration must be authenticated using a single use password solution, and not the local password database.

```
hostname(config)# aaa authentication ssh console [server-tag]
```

Note Enable authentication can use either the local user database or remote aaa server, and reusable passwords are permitted. SSH authentication must use remote aaa server configured for single use authentication. Use of the authentication method “none” is not permitted.

Note Only tacacs+ and radius security protocols are supported at this time.

For information on configuring SSH, see the “Allowing SSH Access” section in the *Cisco Security Appliance Command Line Configuration Guide, Version 7.0*.

Note By default SSH allows both version one and version two, always select version 2. To specify the version number enter the following command, hostname(config)# ssh version version_number.

Note Instead of entering the enable command at the “>” prompt after establishing the ssh session, the administrator shall enter “login” and then login with a local database account and password. This results in all audit events being attributed to that local user.

Configure Console Access on Firewall to use AAA (Optional)

Console access on the firewall using AAA is an option, but is not required in the evaluated configuration.

For information on how to enable authentication and command authorization for system administrators, see the AAA for System Administrators section in the *Cisco Security Appliance Command Line Configuration Guide 7.0*.

Usernames on the Security Appliance

Usernames are defined on the certified configuration and are used to separate the defined roles into separate individuals. Usernames are used for identifying to the certified configuration over the local session from the Supervisor module. Use the **username** command to assign a password and a privilege level for a user. Privilege levels range from 0 (the lowest) through 15. System administrators generally have the highest privilege level.

```
username name {nopassword | password password [encrypted]} [privilege priv_level]}
```

Note Only level 15 users are required in the evaluated configuration.

In the following example, the username is testuser:

```
username testuser password 12RsxXQnphyr/I9Z encrypted privilege 15
```

When the evaluated configuration is operating in multiple context mode, usernames are constrained to the individual context where they were created.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference, Version 7.0*

Note Local authentication is not an option for SSH authentication in the evaluation configuration. The administrator is also advised to never use the value none by itself for any authentication option. Use of the value “none” by itself removes the requirement for entering a password.

Configure AAA for Telnet and FTP

To configure AAA for Telnet and FTP using cut-through proxies you must configure the AAA server group and authentication settings first. After those settings are in effect, enable authentication of Telnet and FTP using the ‘aaa authentication include {telnet, ftp} command.

Note Running ftp and telnet servers on non-standard ports will result in those flows not requiring RADIUS or TACACS+ authentication and is not to be allowed in the evaluated configuration.

```
hostname(config)# aaa-server aaasrvgrp protocol radius
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server aaasrvgrp host 10.30.1.20
hostname(config-aaa-server-host)# authentication-port 1645
hostname (config-aaa-server-host)# timeout 10
hostname (config-aaa-server-host)# retry-interval 2
hostname (config-aaa-server-host)# exit
hostname (config)# aaa authentication include telnet outside 0 0 0 0 aaasrvgrp
hostname (config)# aaa authentication include ftp outside 0 0 0 0 aaasrvgrp
hostname (config)# aaa authentication include telnet inside 0 0 0 0 aaasrvgrp
hostname (config)# aaa authentication include ftp inside 0 0 0 0 aaasrvgrp
```

To ensure that separate sessions from a multi-user machine are not able to piggy-back on an existing authentication request, ensure that the timeout for authentication is set to 0, for no caching of authentication data.

```
hostname (config)# timeout uauth 0:00:00
```

Configuring Failover

Note When using failover, be sure to configure an authentication password to be used between the two firewall units. The command is "failover key {secret | hex key}". Ensure that the password used for the key complies with the "Password Complexity" guidance within this document.

For more information see the, "Configuring Failover" chapter in the *Cisco Security Appliance Command Line Configuration Guide, Version 7.0*.

Inspect ICMP

To configure the ICMP inspection engine, use the **inspect icmp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. The **inspect icmp** command is required to prevent ICMP traffic from passing through the firewall in the event the PFSS audit server should fail.

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

Inspect ARP

To configure the ARP inspection engine, use the arp-inspection command in global configuration mode. ARP inspection is required when a firewall context is operating in transparent mode, to prevent IP spoofing of traffic.

To complete the configuration of ARP inspection the administrator must create static ARP entries for each host protected by the firewall context.

```
hostname(config)# arp inside 1.2.3.4 0050.abcd.1234
hostname(config)# arp-inspection outside enable
hostname(config)# arp-inspection inside enable
```

Unicast RPF

To enable Unicast RPF, use the **ip verify reverse-path** command in global configuration mode. Unicast RPF guards against IP spoofing (a packet uses an incorrect source IP address to obscure its true source) by ensuring that all packets have a source IP address that matches the correct source interface according to the routing table. Unicast RPF is only applicable when a context is operating in routing mode.

```
hostname(config)# ip verify reverse-path interface outside
hostname(config)# ip verify reverse-path interface inside
```

STP and Transparent Mode

Spanning tree protocol (STP) is passed through the firewall by default in transparent mode. This default operation of the product can be mitigated by creating an access list to block the traffic.

```
hostname(config)# access-list layer2 ethertype deny bpdu
```

Same Security Traffic

The ‘same-security-traffic’ command is not allowed in the evaluated configuration. When this command is enabled traffic is allowed to pass between interfaces with the same security level, regardless of current security policy. When ‘same-security-traffic’ is enabled, any AAA statements configured using include are bypassed.

Using the Security Appliance Syslog Server

The security appliance syslog server also referred to in this document as PFSS lets you view syslog messages from a Windows system. If you have a Windows system, use of the security appliance syslog server gives you the additional benefit of reliability through receiving TCP event messages, receiving time-stamped messages, and the ability to monitor whether the server is up or down from thesecurity appliance. The security appliance syslog server is available without cost from Cisco.com. Installation instructions for the security appliance syslog server are provided in the *Installation Guide for the Cisco Secure PIX Firewall, Version 5.2*.

Your security appliance must send syslog messages via TCP to a security appliance syslog server (also called the audit server). If the security appliance syslog server system disk becomes full, the security appliance will stop all new connections.

Ensure that the security appliance syslog server log files are backed up regularly to minimize the possibility of running out of disk space.

For more information on using the security appliance syslog server, refer to the *“Configuring System Log Message Search Functions Using the Security Appliance System Log Message Search”* section in this document.

Note Synchronize the time between the firewall and the Windows server to ensure that audit records can be correlated.

This section contains the following topics:

Configuring Security Appliance Syslog Server

Complete these steps to configure the security appliance to use the syslog server:

Step 1 In the evaluated configuration, TCP is the only allowable protocol for communication between the security appliance and the PFSS Audit Service:

```
logging host interface ip_address tcp/port_number
```

Replace interface with the interface on which the server exists, *IP-address* with the IP address of the host, and *port-number* with the TCP port (if different than the default value of 1468). You can verify that the security appliance traffic is disabled due to a syslog server disk-full condition by using the **show logging** command and looking for the "disabled" keyword in the display.

Only one UDP or TCP command statement is permitted for a server. A subsequent command statement overrides the previous one. Use the **write terminal** command to view the **logging host** command statement in the configuration. In the configuration, the UDP protocol appears as "17" and TCP as "6."

Step 2 Create a logging list to specify messages by various criteria (logging level, event class, and message IDs). The list that you create must ensure these events are logged; 106023, 109001 to 109014, 109021, 109023 to 109028, 111008, 111009, 113001, 113003, 113006, 113007, 160000-169999, 106014, 199002, 302013, 302014, 302020, 302021, 609001, 609002, 199001, 199005, 199006, 201008, 502101 to 502103, 605004, 605005 and 611101 to 611104. Use the **logging list** command in global configuration mode:

```
logging list name {level level [class event_class] | message start_id[-end_id]}
hostname(config)# logging list CC-config message 106023
hostname(config)# logging list CC-config message 109001-109014
hostname(config)# logging list CC-config message 109021
hostname(config)# logging list CC-config message 109023-109028
hostname(config)# logging list CC-config message 111008-111009
hostname(config)# logging list CC-config message 113001
hostname(config)# logging list CC-config message 113003
hostname(config)# logging list CC-config message 113006-113007
hostname(config)# logging list CC-config message 199001
hostname(config)# logging list CC-config message 199005-199006
hostname(config)# logging list CC-config message 201008
hostname(config)# logging list CC-config message 502101-502103
hostname(config)# logging list CC-config message 605004-605005
hostname(config)# logging list CC-config message 611101-611104
hostname(config)# logging list CC-config message 160000-169999
hostname(config)# logging list CC-config message 106014
hostname(config)# logging list CC-config message 199002
hostname(config)# logging list CC-config message 302013
hostname(config)# logging list CC-config message 302014
hostname(config)# logging list CC-config message 302020
hostname(config)# logging list CC-config message 302021
hostname(config)# logging list CC-config message 609001
hostname(config)# logging list CC-config message 609002
```

Step 3 Use the **logging trap** command in global configuration mode to specify which syslog messages the security appliance sends to a syslog server by using the logging list that you created in Step 2:

```
logging trap [logging_list | level]
hostname (config)# logging trap CC-config
```

We recommend that you use the debugging level during initial setup and during testing. Thereafter, set the level from debugging to errors for production use.

Step 4 If needed, set the **logging facility** command to a value other than its default of 20. Most UNIX systems expect the messages to arrive at facility 20, which receives the messages in the local4 receiving mechanism.

Step 5 Start sending messages with the **logging enable** command. To disable sending messages, use the **no logging enable** command.

If you want to stop sending a message to the syslog server, use the **no logging** *message syslog_id* command. Replace *syslog_id* with a syslog message ID.

Step 6 You must send time-stamped messages to the syslog server, use the **clock set** command to set the security appliance system clock and the **logging timestamp** command to enable time stamping. For example:

```
clock set 14:25:00 oct 1 2005
logging timestamp
```

In this example, the clock is set to the current time of 2:25 pm on October 1, 2005, and time stamping is enabled.

Step 7 Use the **no logging permit-hostdown** command in global configuration mode to prevent traffic from passing if the syslog server is down or otherwise unavailable. By default, if you have enabled logging to a syslog server that uses a TCP connection, the firewall does not allow new network access sessions when the syslog server is unavailable for any reason. “no logging permit-hostdown” is the default behavior for PIX/ASA. You will not see this command appear in the configuration file when it is applied

```
hostname(config)# no logging permit-hostdown
```

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference.*

Changing the Syslog Server Parameters at the Windows System

You can change the syslog server parameters at the Windows system by choosing **Start>Settings>Control Panel>Services**.

All the syslog server parameter values can be viewed by examining the sass.log file, which the syslog server creates in the same directory as the syslog server log files.

The syslog server starts immediately after installation. You can use the Services control panel to enter new parameters, pause the service and then resume the service, or to stop and start the service.

Choose one or more parameters from the following:

- d%_disk_full—The maximum percentage of how full the Windows system disk can become before the syslog server causes the security appliance to stop transmissions. This is an integer value in the range of 1 to 100. The default is 90.
- t tcp_port—The port that the Windows system uses to listen for TCP syslog messages, the default is 1468. If you specify another port, it must be in the range of 1024 to 65535.
- u udp_port—The port that the Windows system uses to listen for UDP syslog messages, the default is 514. If you specify Another port, it must be in the range of 1024 to 65535.
- e disk_empty_watch_timer—The duration, in seconds, that the syslog server waits between checks to see if the disk partition is still empty. The default is five seconds, the range is any number greater than zero.
- f disk_full_watch_timer—The duration, in seconds, that the syslog server waits between checks to see if the disk partition is still full. The default is three seconds, the range is any number greater than zero.

Complete these steps to set%_disk_full to 35 percent and the disk-full timer to 10 seconds:

Caution These parameters are only applied once, unless the registry is edited (modify the "ImagePath" for "syslogd".

Step 1 View the service properties for PIX Firewall Syslog Service.

Step 2 Stop the service.

Step 3 Type the parameters to change (**-d 35 -f 10**); start the service; click **OK**.

Note In the example shown, the settings are only affected for the current instance of the server and changes are only permanent when the registry values for the service are updated.

Note The syslog server truncates syslog messages longer than 512 characters in length.

Recovering from the Security Appliance Syslog Server Disk-Full

When you send syslog messages via TCP, the Windows disk may become full and the security appliance unit will stop its traffic. If the Windows file system is full, the Windows system beeps and the syslog server disables all TCP connections from the security appliance unit(s) by closing its TCP listen socket.

The security appliance tries to reconnect to the syslog server five times, and during the retry, it stops all new connections through the security appliance. You then need to back up all the log files to another disk or across the network. (While the syslog server is receiving messages, the log files must reside on the local disk.)

Complete these steps to recover from the disk-full condition:

Step 1 Back up the files on the Windows system.

Step 2 On the security appliance, check that syslog is disabled with the **show logging** command. If the syslog server has disabled the connection, the display contains the "disable" keyword.

Step 3 Disable logging to the syslog server with the **no logging host** command:

```
no logging host dmz1 10.1.1.2
```

Step 4 Restart logging with the **logging host** command:

```
logging host dmz1 10.1.1.2 tcp/1468
```

Step 5 Check that the server is now enabled with the **show logging** command. The "disabled" keyword should no longer be visible.

Configuring System Log Message Search Functions Using the Security Appliance System Log Message Search

You can search and sort system log messages based on dates and times, by syslog ID, and by source and destination IP Addresses. You can also use the advanced Option feature to search for system log messages based on port numbers, services, and interface names. Before you can use the procedures in this section, be sure to install the security appliance syslog server. For more information about installing the security appliance syslog server, go to the following URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/

This section contains the following topics:

Setting Up the Security Appliance System Log Message Search Display

This section provides an overview of the security appliance system log message search display.

Complete these steps to access the security appliance system log message search application:

Step 1 Click the PFSS Search.exe shortcut icon on your desktop. The security appliance system log message search application opens and displays the main window.

Step 2 In the View menu, choose **Select Column**.The Select Column dialog box appears.

Step 3 In this dialog box, check the appropriate check box to display optional column selections in the right window pane. Click in any column heading to sort items in ascending or descending order.

Searching System Log Messages Based on Date and Time

You can configure to search for system log messages, based on specific dates and times. You can specify a single date or time, or you can specify a range of dates and times.

Complete these steps to configure to search for system log messages, based on specific dates and times:

Step 1 Click the **PFSS Search.exe** shortcut icon on your desktop. The security appliance system log message search application opens and the main window appears.

Step 2 Check the **Date** check box and use the drop-down lists in the **Between** field and the **And** field to enter a single date, or a range of dates.

Step 3 Check the **Time** check box and use the drop-down lists in the **Between** field and the **And** field to enter a specific time, or a range of times.

Step 4 Click **Search Now**.

Searching System Log Messages Based on System Log Message ID

You can search for system log messages, based on specific system log message IDs.

Complete these steps to configure to search for system log messages, based on specific system log message IDs:

Step 1 Click the **PFSS Search.exe** shortcut icon on your desktop. The security appliance system log message search application opens and the main window appears.

Step 2 In the Syslog ID field, enter the stringname of the system log message you want to include in the search.

Step 3 Click **Search Now**.

Searching System Log Messages Based on IP Address

You can search for system log messages from a specific source IP address to a specific destination address. You can specify either a single IP address to search for, or a range of addresses.

To search for system log messages from a source IP address to a destination address, perform the following steps:

Step 1 Click the **PFSS Search.exe** shortcut icon on your desktop. The security appliance system log message search application opens and the main window appears.

Step 2 Click **IP Address**. The IP Address dialog box opens in the left display pane. (You may have to scroll to view the IP Address fields.)

Step 3 To specify a single IP address as the search criteria:

- **a.** In the Source IP Address From field, enter the single IP address.
- **b.** In the Destination IP Address From field, enter the same IP address.

Step 4 To specify a range of IP addresses as the search criteria:

- **a.** In the Source IP Address From field, enter the lower IP address range value.
- **b.** In the Source IP Address To field, enter the higher IP address range value.
- **c.** In the Destination IP Address From field, enter the lower IP address range value.
- **d.** In the Destination IP Address To field, enter the higher IP address range value.

Step 5 Click **Search Now**.

Searching Windows Audit Events

For information on using the Event Viewer to view audit records, see the "Audit Management" section in the *Windows 2000 EAL 4 Administrator Guidance* document.

Searching System Log Messages with Advanced Option Feature

You can configure to search for system log messages using the advanced Option feature. The advanced Option feature allows you to search for system log messages based on port numbers, services, and interface names. You can specify either a single port as search criteria, or a range of ports.

To search for system log messages using the advanced Option feature, perform the following steps:

Step 1 Click the **PFSS Search.exe** shortcut icon on your desktop. The security appliance system log message search application opens and the main window appears.

Step 2 Click **Advanced Option**. The Advanced Option dialog box opens in the left display pane. (You may have to scroll the left pane to view the Advanced Option fields.)

Step 3 To specify a single port as the search criteria, enter the single port number in the Port No. field.

Step 4 To specify a range of ports as the search criteria:

a. In the left Port No. field (separated by a —), enter the lower port range value.

b. In the right Port No. field, enter the higher port range value.

c. Click **Search Now**.

Step 5 To specify a service name as the search criteria:

a. Enter the service name in the Services field.

b. Click **Search Now**.

Step 6 To specify an interface name as the search criteria:

a. Enter the interface name in the Interface Name field.

b. Click **Search Now**.

PIX Firewall Syslog Server (PFSS) Guidance

Installation Instructions

To install the PFSS, perform the following steps:

Step 1 Double-click the executable **pfss<ver>.exe** file (where <ver> is the PFSS version number).

Step 2 Click **Yes.** The setup will start.

Step 3 At the Welcome window, click **Next**. After the log files destination directory is selected, the setup will check to see if your file system in which the log files will reside is NTFS. If it is not, the setup will exit. If it is, it will continue. If it finds this service is already installed, then it will ask if you would like to uninstall it.

Step 4 After selecting your destination target and folder, you must choose the port numbers for the TCP Syslog Server and the UDP Syslog Server. The default values will be

TCP PORT = 1470

UDP PORT = 514

Note You must enter a port number greater than 1024 and less than 65536.

Step 5 The last window will prompt you for the "% Disk Full," "Disk Empty Watch," and "Disk Full Watch," as defined in the following:

% Disk Full —The percentage of the total disk size that is full that you wish the Syslog Server to stop (Default is 90%)

Disk Empty Watch —This is the number of seconds in interval that you wish the disk monitor to check to see if the disk is full when the disk is still empty. (The default is five seconds).

Disk Full Watch—This is the number of seconds in interval that you wish the disk monitor to check to see if the disk is empty when the disk is still full. (The default is three seconds.)

Step 6 By now your setup will be complete, and the service will have started. To stop or pause the service, go to the control panel and click **Services**. Look for PIX Firewall Syslog Server and click the button of the service you want.

Step 7 To change parameters, such as the% Disk Full, go to the service panel and type the parameters you want:

-d <% Disk Full >

-t <TCP PORT >

-u <UDP PORT>

-e <Disk Empty Watch >

-f <Disk Full Watch >

For example, to set the% Disk Full to%35 and the TCP PORT to 1470, type **-d 35 –t 1470**

Usage Instructions

The PFSS is bundled with an executable application to conduct searching and sorting of the stored system log message records. The shortcut for this application is created on the desktop and in the existing PFSS program folder. No changes can be done to the log files from the search/sort application.

The PFSS search/sort application is launched by clicking the short cut present in the desktop or the one present in the program folder. The initial screen is divided into the following three parts:

- Tool Bar
- Search Options
- Search Results Table

Buttons in Tool Bar

The following buttons are available in the toolbar:

- Open Report
- Save Report
- Search
- New
- View Message
- Print

Click **Open Report** to open the already stored report files for viewing.

Click **Save Report** to save the search results in one of the following two formats:

- *.PFSS
- *.txt

In the.PFSS format, a delimiter ($) exists in-between the fields. When you open this file from the application, the messages display in the search results table.

In the *.txt format, the system log message information is stored and opens in a text viewer.

Click **Search** to open or close the search options pane. The search pane can also be enabled by choosing **View > Search**.

Click **New** to clear the existing search values and set the search fields to default values. You can do a new search by choosing **Edit > New Search**.

Click **View Message** to select a message displayed in the search table. You can also view the system log message by double-clicking the row, as shown in the following figure.

Fields in the Search Pane

The search pane displays the following options which you can select.

- Date
- Time
- Syslog ID
- IP Address
- Advanced Option

The Date and Time range selection and the Syslog ID fields are the most commonly used. These options are enabled by default; the other two fields are disabled by default.

Click **IP Address** and **Advanced Options** in the search pane to enable and disable the source and destination IP address, services and ports. The following figures show a complete view of the search options.

Search Results

The system log messages that satisfy search conditions display in the search results pane. The following information appears:

- Syslog ID
- Date
- Time
- Host name/IP Address
- Message

In addition you can select the following columns in the search results by choosing **View > Select Columns**. The optional columns are:

- Source IP Address
- Destination IP Address
- Services
- Ports
- Interface name.

You can sort columns by clicking the column headers. For example, to sort by syslog ID, click the **Syslog ID** column header in the search results pane.

Search/Sort Menu

In the File menu, you can open, save and print the search results reports.

In the Edit menu, you can cut, copy and paste text.

Click **New Search** to clear the current search fields.

In the View menu, you can activate the toolbar, status bar, search and Select Columns. The Select Columns option is used to customize the search results. Not all the options in the search results are customizable. The syslog ID, date, time, hostname/IP address and system log message fields are always displayed. You can enable or disable the source and destination IP address, port, services and interface name fields choosing Select Columns as shown in the Figure below.

Release Notes for PIX Firewall Syslog Server 5.1(2)

- PFSS is now supported on Windows 2000 Service Pack 3, Windows NT 4.0 Service Pack 6, and Windows XP Professional Service Pack 1.
- PFSS installation/deinstallation requires an account with administrative privileges (CSCdz04526). Attempting such operations with non-administrative privileges may leave your system in an unstable state
- The PFSS application can be installed on a FAT or NTFS file system; however, the log file directory must be located on a local NTFS file system. A warning will be issued during installation if one attempts to save the log files on a FAT file system, and the installation program will exit. Use the convert program from a DOS prompt to convert a FAT file system to NTFS.

Release Notes for PIX Firewall Syslog Server 5.1(1)

For 5.1(1), per bug CSCdp45416, two changes have been made to PFSS:

- PFSS will now use the modification date when renaming files instead of the creation date of the log file.
- A backup directory will now be created within the log file directory, where the <day>.mmddyy files will reside after being renamed.

MD5 Hash Value for the Security Appliance

The MD5 File Validation feature allows you to generate the MD5 hash for the adaptive security appliance image stored on your chassis and compare it to the value posted on Cisco.com to verify that the image on your chassis is not corrupted.

You can obtain the MD5 value for your system image from the Software Center at Cisco.com, or enter the following commands to check after transferring an image file:

[**message-digest-key** *key_id* **md5** *key*]

This command enables the Message Digest 5 (MD5) authentication and specifies the numerical authentication key ID number.

A mismatch in MD5 values means the image is corrupt.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.