Table of Contents

PIX Firewall 7.x and Later with Syslog Configuration Example	
Document ID: 63884	1
Introduction	
Prerequisites	1
Requirements	
Components Used	
Conventions	
Configure Basic Syslog using ASDM	
Basic Syslog	
Advanced Syslog	
Use the Message List	
Use the Message Class	
Verify.	
Troubleshoot	
NetPro Discussion Forums – Featured Conversations	
Related Information.	

PIX Firewall 7.x and Later with Syslog Configuration Example

Document ID: 63884

Introduction Prerequisites Requirements Components Used Conventions Basic Syslog Configure Basic Syslog using ASDM Advanced Syslog Use the Message List Use the Message Class Verify Troubleshoot NetPro Discussion Forums – Featured Conversations Related Information

Introduction

This sample configuration demonstrates how to configure PIX Firewall version 7.0 with syslog.

PIX 7.0 has introduced very granular filtering techniques to allow only certain specified syslog messages to be presented. The Basic Syslog section of this document demonstrates a traditional syslog configuration. The Advanced Syslog section of this document shows the new syslog features in 7.0.

Refer to Cisco Security Appliance System Log Messages Guide, Version 7.0 for the complete system log messages guide.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- PIX 515E with PIX Software version 7.0
- Cisco Adaptive Security Device Manager (ASDM) version 5.01

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Basic Syslog

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Use these commands to enable logging, view logs, and view configuration settings.

- logging enable Enables the transmission of syslog messages to all output locations.
- no logging enable Disables logging to all output locations.
- show logging Lists the contents of the syslog buffer and the current logging configuration.

PIX can send syslog messages to various destinations. Use the commands in these sections to specify the location to which messages should be sent:

Internal Buffer

logging buffered severity_level

External software or hardware is not required when you store the syslog messages in the PIX internal buffer. Use the **show logging** to view the stored syslog messages.

Syslog Message Server

logging host interface_name ip_address [tcp[/port] | udp[/port]] [format emblem]
logging trap severity_level
logging facility number

A server that runs a syslog application is required in order to send syslog messages to an external host. PIX sends syslog on UDP port 514 by default.

E-mail Address

logging mail severity_level
logging recipient-address email_address
logging from-address email_address
smtp-server ip_address

An SMTP server is required when you send the syslog messages in e-mails. Correct configuration on the SMTP server is necessary in order to ensure that you can successfully relay e-mails from the PIX to the specified e-mail client.

Console

logging console severity_level

Console logging enables syslog messages to display on the PIX console (tty) as they occur. Use this command when you debug problems or when there is minimal load on the network. Do not use this command when the network is busy as it can degrade performance.

Telnet/SSH Session

logging monitor severity_level

terminal monitor

Logging monitor enables syslog messages to display as they occur when you access the PIX console with Telnet or SSH.

ASDM

logging asdm severity_level

ASDM also has a buffer that can be used to store syslog messages. Use the **show logging asdm** command to display the content of the ASDM syslog buffer.

SNMP Management Station

```
logging history severity_level
    snmp-server host [if_name] ip_addr
    snmp-server location text
    snmp-server contact text
    snmp-server community key
    snmp-server enable traps
```

Users need an existing functional Simple Network Management Protocol (SNMP) environment in order to send syslog messages using SNMP.

Refer to Commands for Setting and Managing Output Destinations for a complete reference on the commands you can use to set and manage output destinations

Refer to Messages Listed by Severity Level for messages listed by severity level.

Example 1

This output shows a sample configuration for logging into the console with the severity level of debugging.

logging enable logging buffered debugging

This is sample output.

```
%PIX|ASA-6-308001: console enable password incorrect for number tries (from 10.1.1.15)
```

Configure Basic Syslog using ASDM

This procedure demonstrates the ASDM configuration for all available syslog destinations followed by the configuration for Example 1.

- 1. Go to the ASDM Home window.
- 2. Select Configuration > Features > Properties > Logging > Logging Setup.
- 3. Check Enable logging to enable syslogs.

Configuration > Features > Pr	operties > Logging > Logging Setup
+ £ ¥ 2 ĝ %	
AAA Setup AAA Setup Advanced AAP Static Table Auto Update DHCP Services DNS Client Failover DHCP Services DNS Client P Audit Deging Deging Setup Systog Setup Systog Setup Systog Setup Priority Queue SSL SUNRPC Server URL Filtering	Logging Setup Imable logging in the failower standby unit Send debug messages as syslogs in Emable logging on the failower standby unit Send debug messages as syslogs in Send syslogs in EMBLEM format Logging to Internal Buffer Specify the size of the internal buffer to which syslogs will be saved. When the buffer fills up, it will be overwritten. Buffer Size: 4096 bytes You can choose to save the buffer contents before the buffer is overwritten. Save Buffer To: FTP Server Configure FTP Settings Flash Configure Flash Usage ASDM Logging Specify the size of the queue for syslogs intended for viewing in ASDM. Queue Size: 100
	Abbia

- 4. Select Syslog Servers under Logging and click Add to add a syslog server.
- 5. Enter the syslog server details in the Add Syslog Server box and click **OK** when you are done.

Configuration > Features > Pr	
⊕ <u>●</u> ● ● ■ ■ ■ ■ ■	
🕀 🚽 AAA Setup	- Syslog Servers
🕀 📴 Advanced	
- ARP Static Table	Specify up to 16 syslog servers. Make sure logging is enabled in Logging > Logging Setup under the
🛃 Auto Update	Properties tab.
🛱 🍘 DHCP Services	Interface ID address Data District Data
- ADNS Client	interface in Address Protocour Emplem Add
Failover	
- 🔀 History Metrics	Edit
🕀 🔩 IP Audit	
🕀 🛅 Logging	Delste
- BLogging Setup	
- Event Lists	State Freedom Frances
- Uniters	and system in the system is the system in the system in the system is the system in the system in the system is th
- Carlos Setup	Include I
She Mail Calup	Specify the number of messages that are allow interface: inside
- Printity Queue	busy. Use 0 to indicate unlimited queue size.
	IP Address: 10.66.79.198
- SUNRPC Server	where size. 512
URL Filtering	Protocol C Tech
	Allow user traffic to pass When TCP systop s
	Port 514
	Log messages in Cisco EMBLEM format (UDP only)
	OK Cancel Help

- 6. Select **E-Mail Setup** under Logging to send syslog messages to e-mails.
- 7. Specify the source e-mail address in the Source E-Mail Address box and click **Add** to configure the e-mail recipients' destination e-mail address and the message severity level. Click **OK** when you are done.

Configuration > Features > Properties > Logging > E-Mail Setup				
● 全 爭 ■ 前 ≫ 釉 蟲 蟲 葛 ◎				
AAA Setup Ada Setup Ada Setup Ada Setup Advanced Auto Update Auto Update PDHCP Services ADNS Client PFillover PHistory Metrics P Isoging	E-Mail Setup Enter the e-mail address that will be used as the source address when syslogs are sent as e-mails. Source E-Mail Address E-Mail Recipients Destination E-Mail Address Syslog Severity Add			
Cogging Setup Cogging Setup Cogging Filters Cogging Filters Cogging Filters Cogging Setup C	Edit Edit Destination E-Mail Address: admin@test.com			
URL Filtering	Fitter the systogs sent to this recipient by severity. The systog severity fitter used for this recipient will be the higher of the severity selected below and the global fitter self or all e-mail recipients in Configuration>Features>Properties>Logging>Logging Fitters. Systog Severity: Errors OK Cancel			

8. Click **Device Administration**, select **SMTP**, and enter the server IP address in order to specify the SMTP server IP address.

9. Select **SNMP** in order to specify the address of the SNMP management station and properties.

Configuration > Features > Device Administration > Administration > SNMP				
● 金 筆 ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■				
	SNMP			
- ⁹ Device				
BEEPassword	Configure SNMP parameters and management station(s).			
- 🎝 AAA Access				
- 📆 User Accounts	Community String (default):			
- 🕼 Banner	(chrone)			
Console	Contact Leff			
- SASDM/HTTPS	Jen Jen			
# Teinet	Port section			
- 😫 Secure Copy	Poleotauon. once			
- Secure Shell	Listenice Data			
- Management Access	Listening Port Tel Conigue Traps			
- W ² SMTP				
-JISNMP	SNMP management station:			
ICMP Rules	Interface IP Address Community String SNMP Version Poll/Trap UDP Port Add			
Charle				
Click	Edit			
- Second Impage Configuration				
CTP Mode	Delete			
E Certificate	Disco -			
- Silkey Pair				
E Trustpoint				
- En Authentication				
Enrollment				
Elmport Certificate				
2 Manage Certificates				
	Apply Reset			

10. Click Add to add an SNMP management station. Enter the SNMP host details and click OK.

🚰 Add SNMP Host Access Ent	iry
Interface Name:	inside 💌
IP Address:	10.66.79.189
UDP Port:	162
Community String:	public
SNMP Version:	1
Server Poll/Trap Spe	cification
Select a specified fu	inction of the SNMP Host.
🔽 Poll	
🔽 Trap	
2	
ок с	ancel Help

- 11. Click **Properties** under Configuration and select **Logging Filters** under Logging To select the destination of the syslog messages.
- 12. Choose the desired Logging Destination and click Edit.

For this procedure, Example 1 logging buffered debugging is used.

13. Select Internal Buffer and click Edit.



14. Choose **Filter on severity** and select **Debugging** from the drop–down menu. Click **OK** when you are done.

💼 Edit Logging Filters		X
Logging Destination: Internal Buffer Syslogs from All Event Classes © Filter on severity Debugging © Use event list my_critical_messagive New © Disable logging from all event classes		
Syslogs from Specific Event Classes Event Class and Severity to Be Added Event Class: auth Description: User Authentication Delete Severity: Emergencies	Event Class	Severity
OK Cancel	Help	

15. Click **Apply** after you return to the Logging Filters window.

Configuration > Features > Properties > Logging > Logging Filters				
* 2 平 F () () () () () () () () () (
Fragment	Logging Filters Configure syslog filter	rs for logging destinations.		
Auto Update	Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes	Edit
- PDHCP Server	Internal Buffer	Severity: Debugging		
DHCP Relay	Console	Disabled		
- Failover	Telnet Sessions	Disabled		
- 🔄 History Metrics	Syslog Servers	Disabled		
🗗 🍋 IP Audit	SNMP Trap	Disabled		
- QIP Audit Policy	E-Mail	Disabled		
P I occing	ASDM	Disabled		
E Logging Setup Event Lists GLogging Filters Syslog Setup Syslog Setup				
Priority Queue SSL SUNRPC Server URL Filtering				
		Apply	Reset	

Advanced Syslog

PIX 7.0 provides several mechanisms that enable you to configure and manage syslog messages in groups. These mechanisms include message severity level, message class, message id, or a custom message list that you create. With the use of these mechanisms, you can enter a single command that applies to small or large groups of messages. When you set up syslogs this way, you are able to capture the messages from the specified message group and no longer all the messages from the same severity.

Use the Message List

Use the message list to include only the interested syslog messages by severity level and ID into a group, then associate this message list with the desired destination.

Complete these steps in order to configure a message list.

- 1. Enter the **logging list** *message_list / level severity_level [class message_class]* command to create a message list that includes messages with a specified severity level or message list.
- 2. Enter the **logging list** *message_list* **message** *syslog_id-syslog_id2* command to add additional messages to the message list just created.
- 3. Enter the **logging** *destination message_list* command to specify the destination of the message list created.

Example 2

Issue these commands to create a message list which includes all the severity 2 (critical) messages with the addition of message 611101 to 611323, and also have them sent to the console:

```
logging list my_critical_messages level 2
logging list my_critical_messages message 611101-611323
logging console my_critical_messages
```

ASDM Configuration

This procedure shows an ASDM configuration for Example 2 using the message list.

1. Select Event Lists under Logging and click Add to create a message list.

Configuration > Features > Pr	roperties > Logging > Ev	ent Lists		
⊕ ⊈ 筆 ■ 前 湯	5 6 <u>6 6</u> 5 4			
AAA Setup AAA Setup Advanced ARP Static Table Auto Update PDHCP Services Auto CP Services Solver	Event Lists Use event lists to der used to filter syslogs	fine a particular set of syslogs that sent to a logging destination.	at you are interested in. The	event list can be
- 2 History Metrics	Name	Event Class / Severity	Message IDs	Add
E Cogging				Edit
VRL Lists		A	pply Reset	Delete

2. Enter the name of the message list in the Name box. In this case **my_critical_messages** is used. Click **Add** under Event Class/Severity Filters.

Add Event List Name: my_critical_messages Specify filters for the event list. You c	an filter syslogs by	their class and severity, or by their ID	s.
- Event Class/Severity Filters		Message ID Filters	
Event Class Severity	Edit Delete	Message IDs	Add Edit Delete
	ОК	Cancel Help	

3. Select the Event Class and Severity from the drop–down menus.

In this case, select **All** and **Critical** respectively. Click **OK** when you are done.

🖆 Add Class and Severity Filter 🛛 🔒		
Event Class:	All	•
Description:	All Event Classes	
Severity:	Critical	•
ок	Cancel	Help

4. Click Add under the Message ID Filters if additional messages are required.

📫 Add Event List	\mathbf{X}
Name: my_critical_messages Specify filters for the event list. You can filter syslogs by their class and severity, or by their IDs. Event Class/Severity Filters Message ID Filters Event Class Severity Add - All - Critical Edit Delete	
OK Cancel Help	

In this case, you need to put in messages with ID 611101–611323.

5. Put in the ID range in the Message IDs box and click **OK**.

🖆 Add Syslog Message ID Filter 🛛 🚺	
Enter the syslog message ID. Use hyphen to specify a range of syslog IDs, for example, 101001-101010.	
Message IDs: 611101-611323	
OK Cancel Help	

- 6. Go back to the **Logging Filters** menu and choose **Console** as the destination.
- 7. Click **Use event list** and select **my_critical_messages** from the drop- down menu. Click **OK** when you are done.

🖆 Edit Logging Filters	X
Logging Destination: Console Syslogs from All Event Classes	
C Filter on severity Emergencies	
œ Use event list my_critical_message ▼ New	
C Disable logging from all event classes	
Syslogs from Specific Event Classes	
Event Class and Severity to Be Added Event Class Severity	[
Event Class: auth Add >>	
Description: PKI Certificate Authority Delete	
Severity: Emergencies	
OK Cancel Help	

8. Click **Apply** after you return to the Logging Filters window.



This completes the ASDM configurations using message list as shown in Example 2.

Use the Message Class

Use the message class to send all messages associated with a class to the specified output location. When you specify a severity level threshold, you can limit the number of messages sent to the output location.

logging class message_class destination | severity_level

Example 3

Enter this command to send all ca class messages with a severity level of emergencies or higher to the console.

logging class ca console emergencies

ASDM Configuration

This procedures shows the ASDM configurations for Example 3 using the message list.

- 1. Go to the **Logging Filters** menu and choose **Console** as the destination.
- 2. Click Disable logging from all event classes.
- 3. Under the Syslogs from Specific Event Classes, choose the Event Class and Severity you want to add.

This procedure uses **ca** and **Emergencies** respectively.

4. Click Add to add this into the message class and click OK.

🚳 Edit Logging Filters	×
Logging Destination: Console Syslogs from All Event Classes C Filter on severity Emergencies C Use event list my_critical_message New C Disable logging from all event classes	
Syslogs from Specific Event Classes Event Class and Severity to Be Added Event Class: auth Emergencies Add >> Description: PKI Certificate Authority Delete Payority	
OK Cancel Help	

5. Click **Apply** after you return to the Logging Filters window.

Console now collects the ca class message with severity level Emergencies as shown on the Logging Filters window.



This completes the ASDM configuration for Example 3.

Refer to Messages Listed by Severity Level for a list of the log message severity levels.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- Cisco PIX Firewall Software
- Cisco Secure PIX Firewall Command References
- Security Product Field Notices (including PIX)
- Requests for Comments (RFCs)
- Technical Support & Documentation Cisco Systems

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Dec 05, 2005

Document ID: 63884