

PIX/ASA 7.x with Syslog Configuration Example

Document ID: 63884

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Basic Syslog

- Configure Basic Syslog using ASDM
- Send Syslog Messages Over a VPN to a Syslog Server

Advanced Syslog

- Use the Message List
- Use the Message Class
- Log ACL ACE Hits

Capture VPN Traffic Syslog Messages

Verify

Troubleshoot

- %ASA-3-201008: Disallowing new connections
- Solution

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This sample configuration demonstrates how to configure PIX/ASA Security Appliance 7.x 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.x for the complete system log messages guide.

Refer to Setting Up PIX Syslog for more information on how to configure syslog in Cisco Secure PIX Software Releases 4.0.x.

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) in order 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 in order 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
```

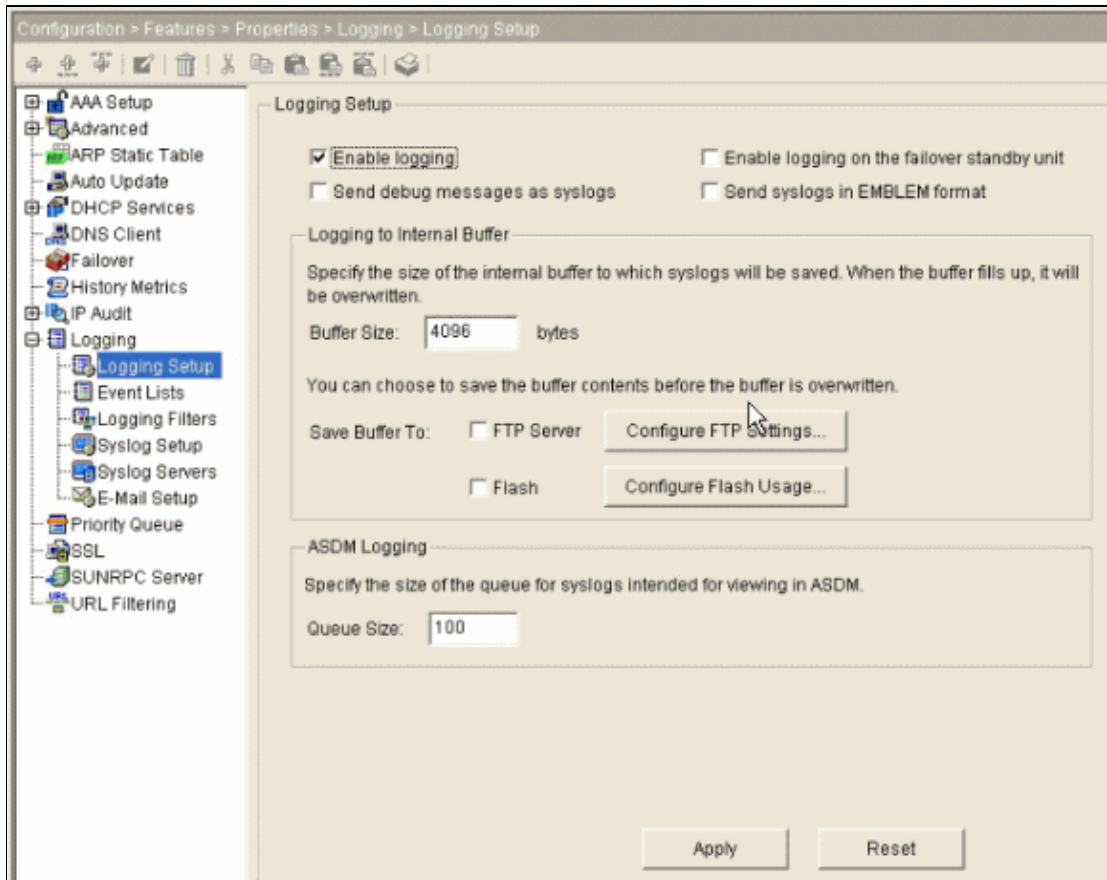
This is sample output.

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

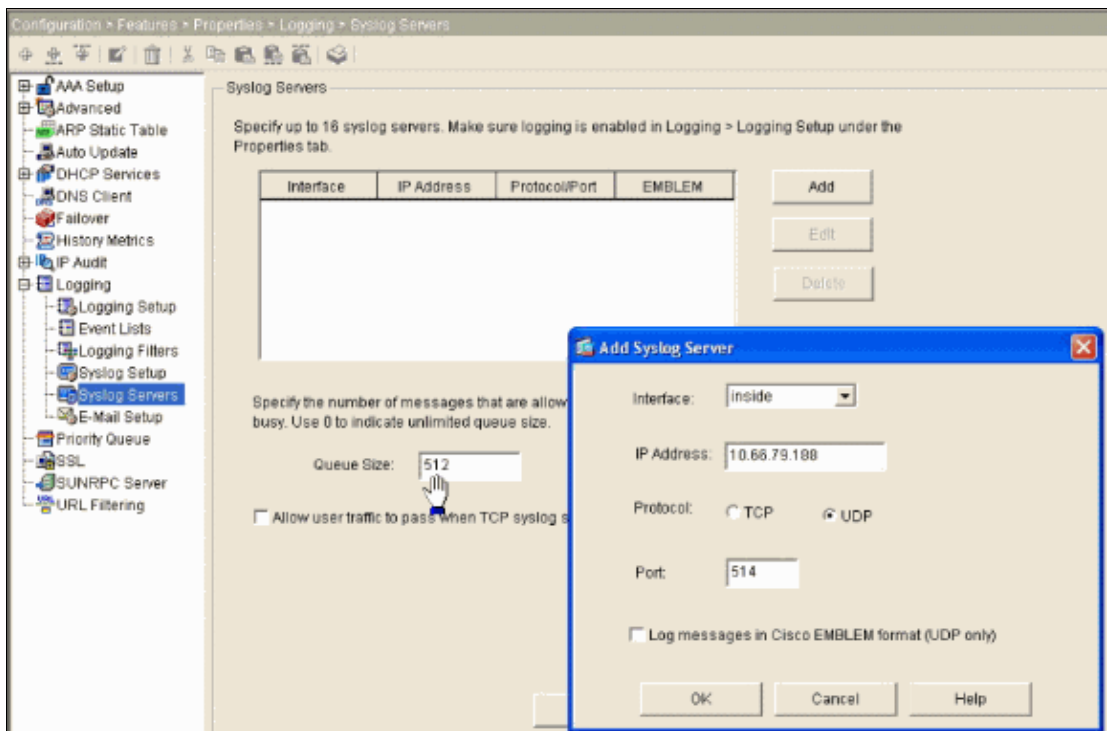
Configure Basic Syslog using ASDM

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

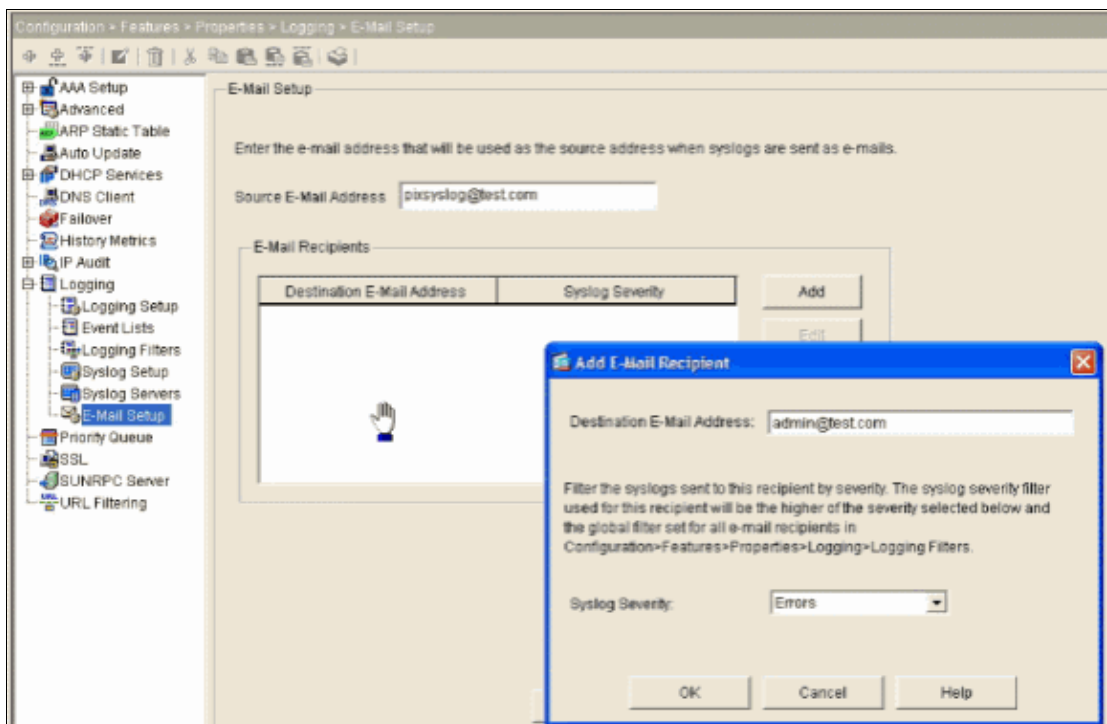
1. Go to the ASDM Home window.
2. Choose **Configuration > Features > Properties > Logging > Logging Setup**.
3. Check **Enable logging** in order to enable syslogs.



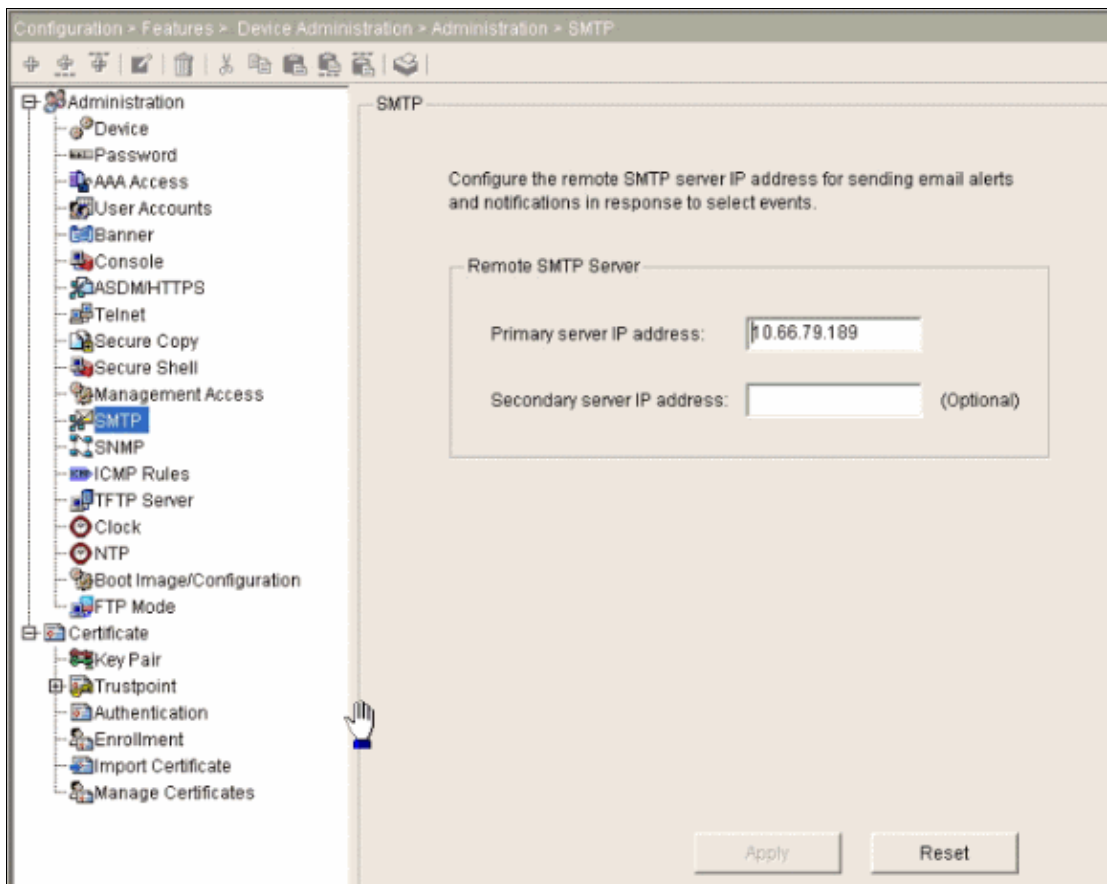
4. Choose **Syslog Servers** in Logging and click **Add** in order to add a syslog server.
5. Enter the syslog server details in the Add Syslog Server box and choose **OK** when you are done.



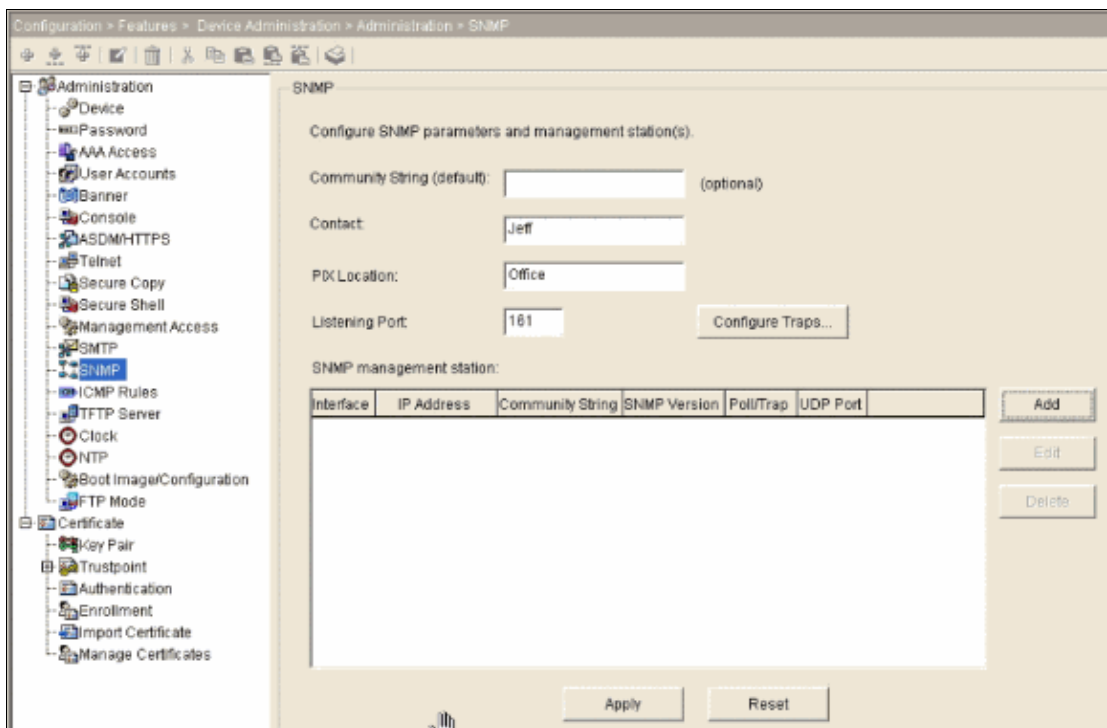
6. Choose **E-Mail Setup** in Logging in order to send syslog messages to e-mails.
7. Specify the source e-mail address in the Source E-Mail Address box and choose **Add** in order to configure the destination e-mail address of the e-mail recipients and the message severity level. Click **OK** when you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



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



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



10. Choose **Add** in order to add an SNMP management station. Enter the SNMP host details and click **OK**.

Interface Name: inside

IP Address: 10.66.79.189

UDP Port: 162

Community String: public

SNMP Version: 1

Server Poll/Trap Specification

Select a specified function of the SNMP Host.

Poll

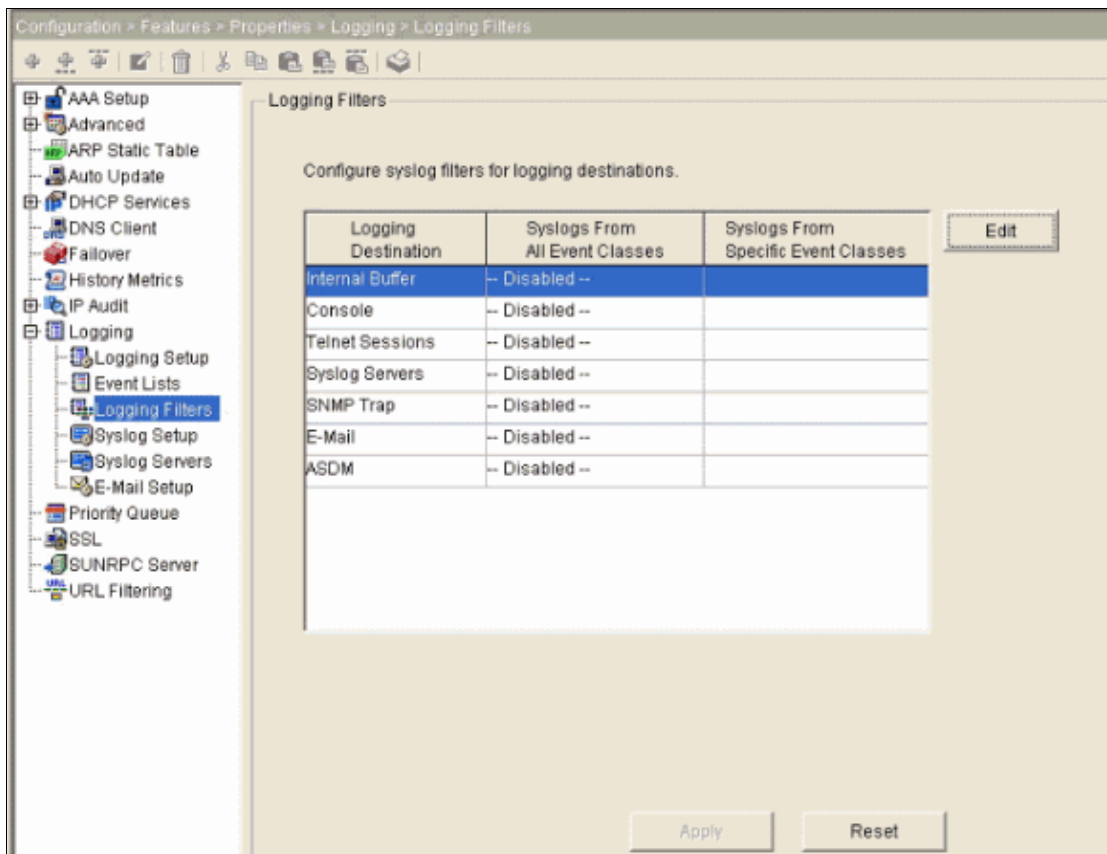
Trap

OK Cancel Help

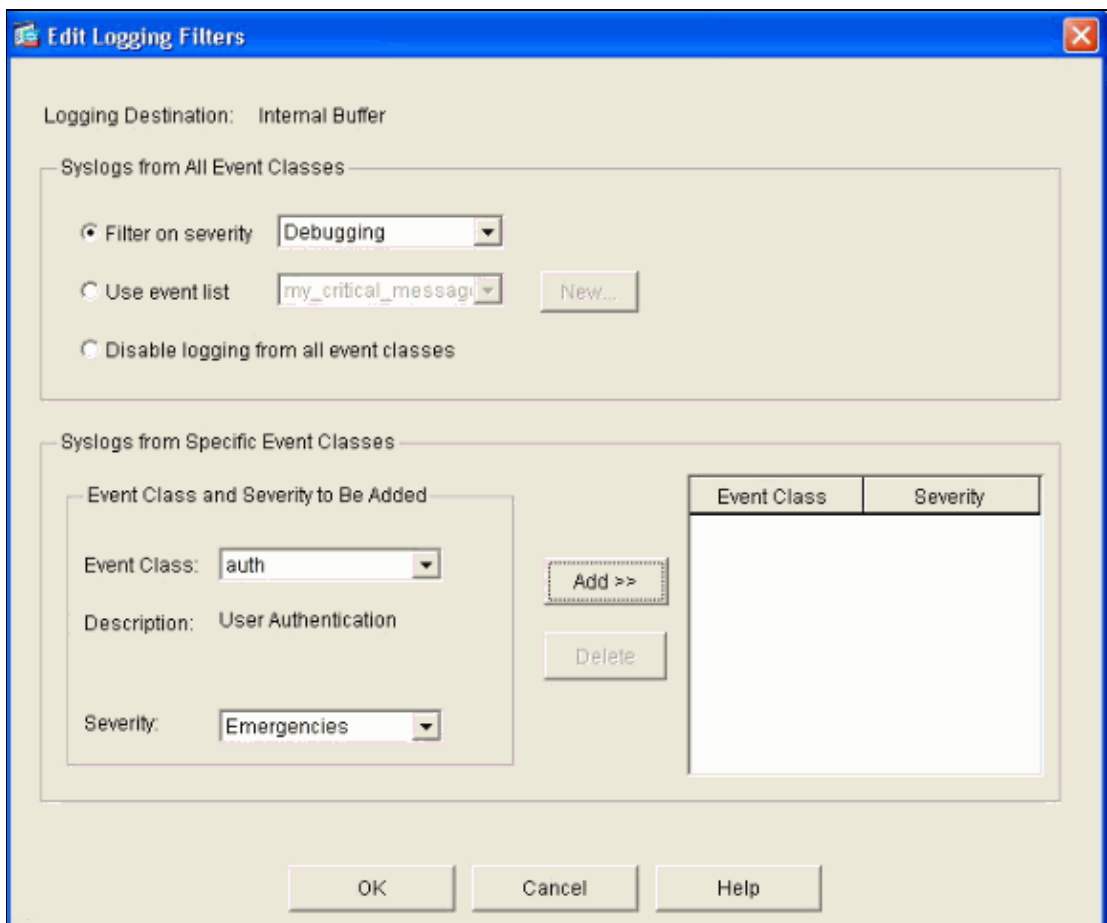
11. Click **Properties** under Configuration and choose **Logging Filters** in Logging in order to select the destination of the syslog messages.
12. Choose the desired Logging Destination and click **Edit**.

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

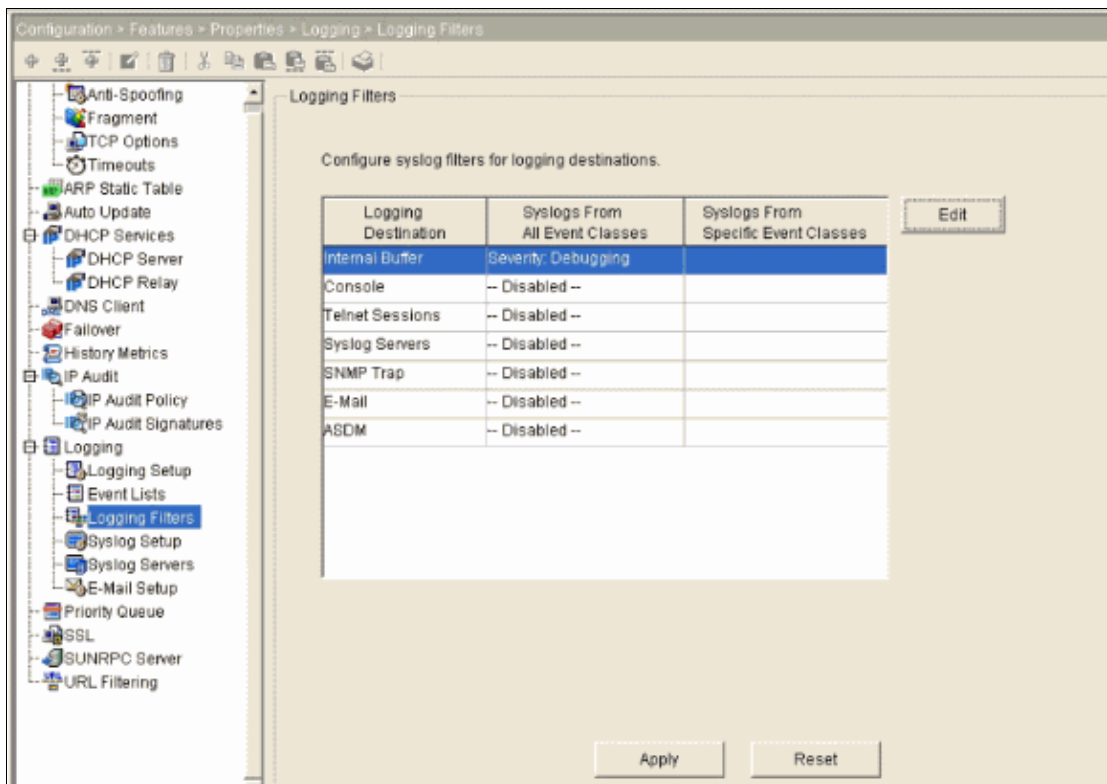
13. Choose **Internal Buffer** and click **Edit**.



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



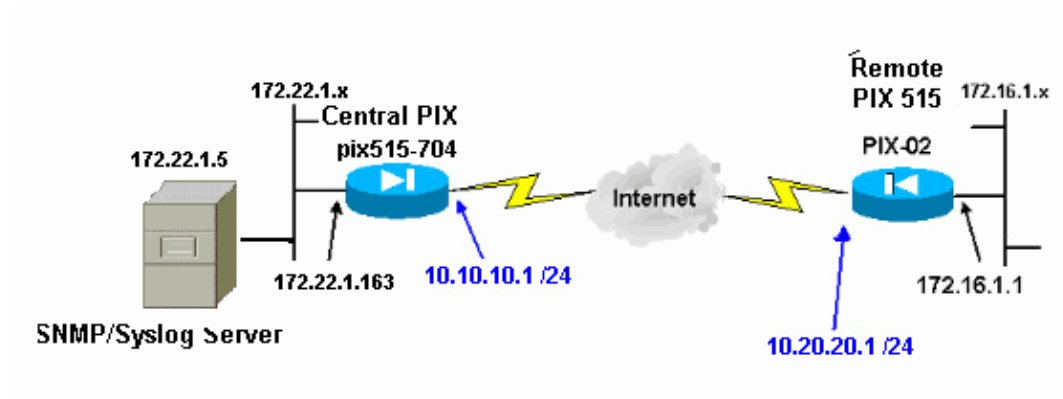
15. Click **Apply** after you return to the Logging Filters window.



Send Syslog Messages Over a VPN to a Syslog Server

In either the simple site-to-site VPN design or the more complicated hub-and-spoke design, people sometimes want to monitor all the PIX Firewalls with the Simple Network Management Protocol (SNMP) server and syslog server located at a central site.

In order to configure the site-to-site IPsec VPN configuration, refer to PIX/ASA 7.x Simple PIX-to-PIX VPN Tunnel using ASDM Configuration Example. Apart from the VPN configuration, you have to configure the SNMP and the interesting traffic for the syslog server in both the central and local site.



Central PIX Configuration

```
!--- This access control list (ACL) defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two PIXes.
!--- It also includes the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind the PIX 515.
```

```
access-list 101 permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0
```

```
!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS(TCP/UDP port - 162)
!--- and syslog traffic (UDP port - 514) from SNMP/syslog server
!--- to the outside interface of the remote PIX.
```

```
access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 514
logging on
logging trap debugging
logging history debugging
```

```
!--- Define logging host information.
```

```
logging facility 16
logging host inside 172.22.1.5
```

```
!--- Define the SNMP configuration.
```

```
snmp-server host inside 172.22.1.5
snmp-server community test
snmp-server enable traps
```

Remote PIX Configuration

```
!--- This ACL defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two PIXes.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind PIX 515.
```

```
access-list 101 permit ip 172.16.1.0 255.255.255.0 172.22.1.0 255.255.255.0
```

```
!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS (TCP/UDP port - 162) and
!--- syslog traffic (UDP port - 514) sent from this PIX outside
!--- interface to the SYSLOG server.
```

```
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 514
```

```
!--- Define syslog server.
```

```
logging facility 23
logging host outside 172.22.1.5
```

```
!--- Define SNMP server.
```

```
snmp-server host outside 172.22.1.5
```

```
snmp-server community test
snmp-server enable traps
```

Refer to Monitoring Cisco Secure PIX Firewall Using SNMP and Syslog Through VPN Tunnel for more information on how to configure PIX 6.x.

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 in order 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 in order 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 in order to add additional messages to the message list just created.
3. Enter the **logging** *destination message_list* command in order to specify the destination of the message list created.

Example 2

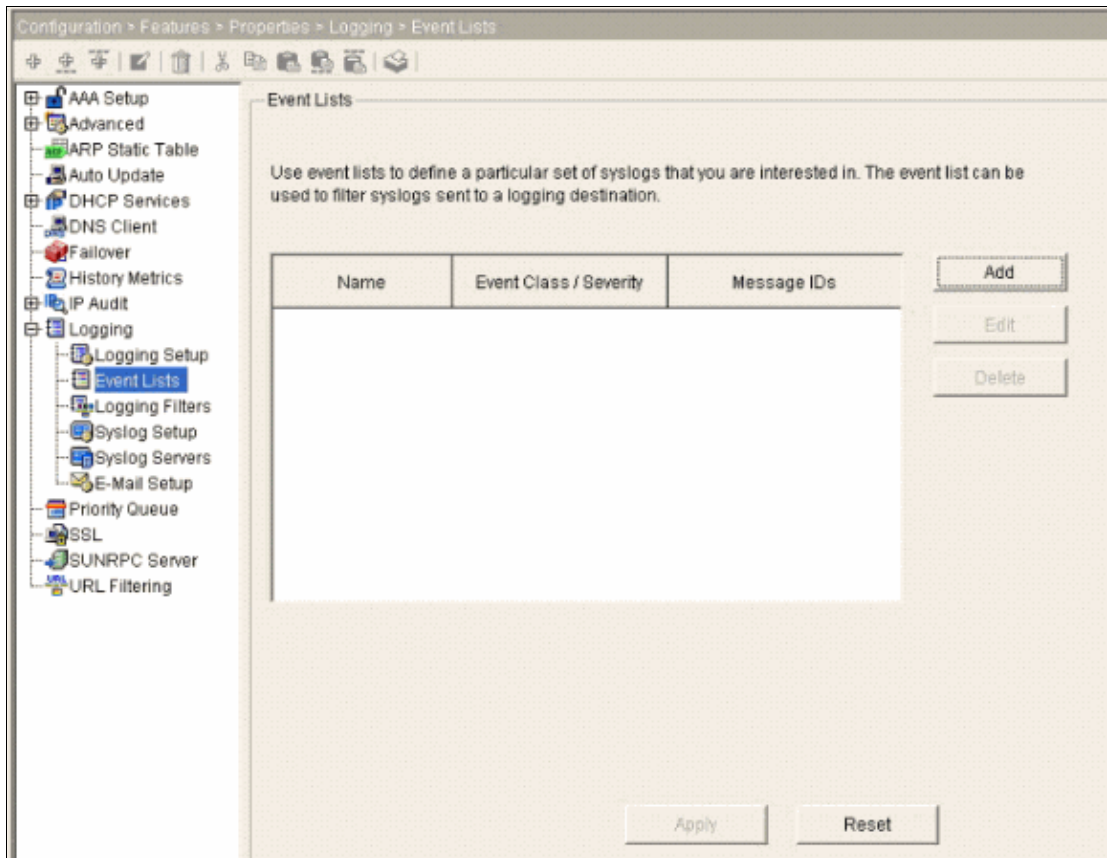
Issue these commands in order to create a message list, which includes all the severity 2 (critical) messages with the addition of message 611101 to 611323, and also have them sent to the console:

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

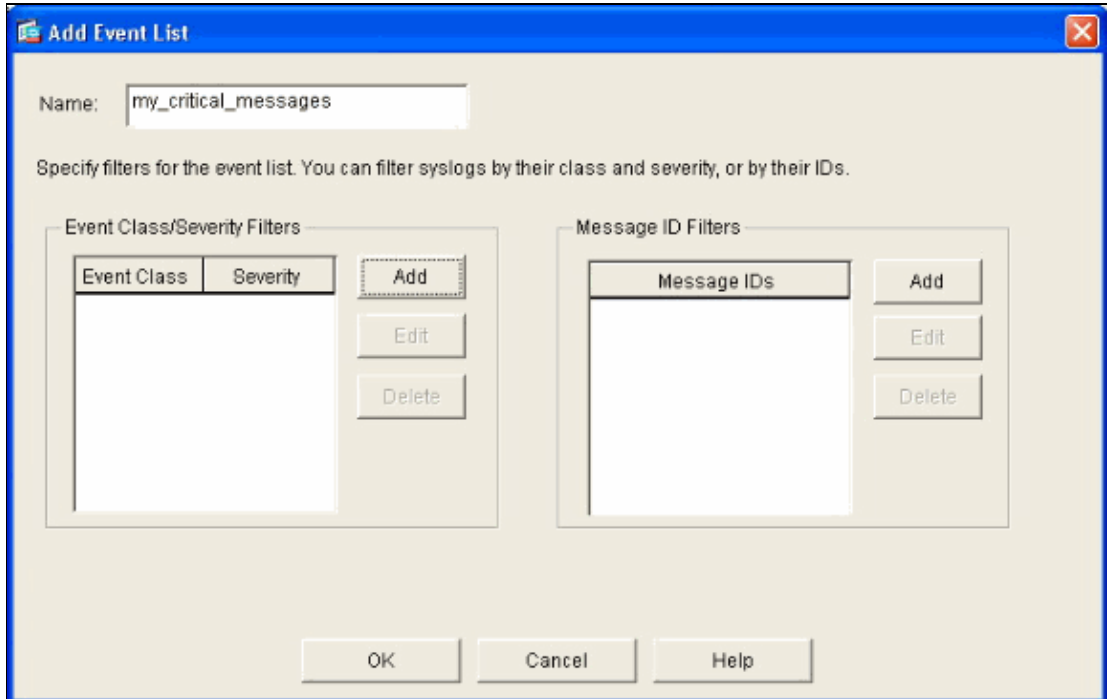
ASDM Configuration

This procedure shows an ASDM configuration for Example 2 with the use of the message list.

1. Choose **Event Lists** under Logging and click **Add** in order to create a message list.



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.



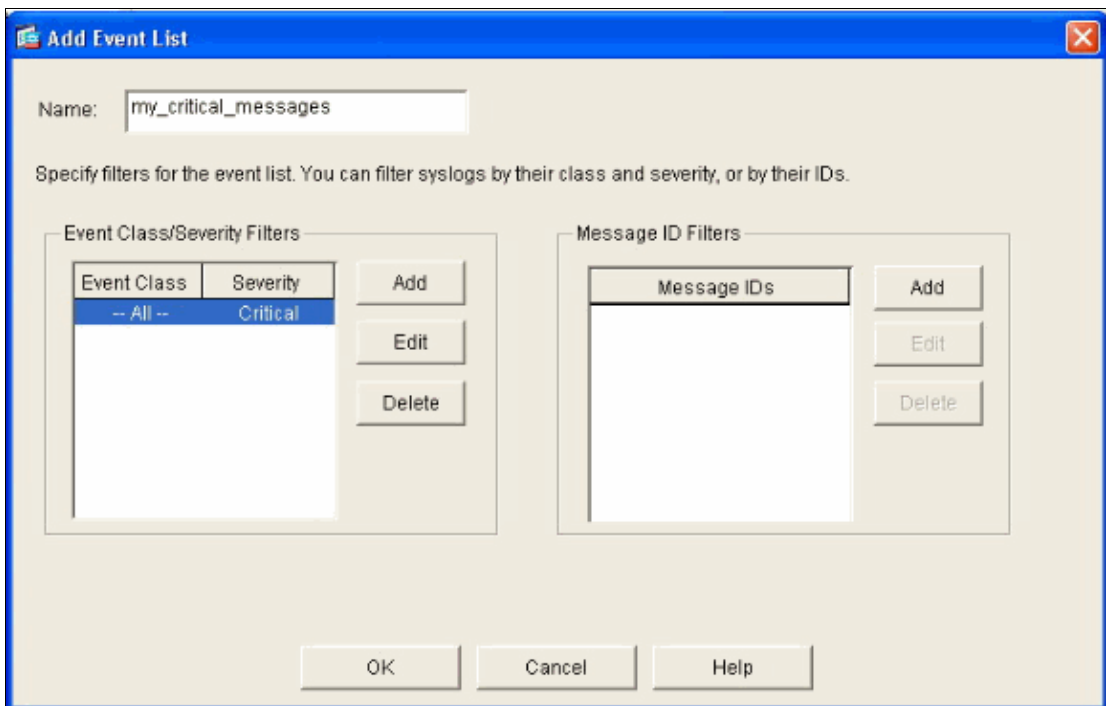
3. Choose the Event Class and Severity from the drop-down menus.

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



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

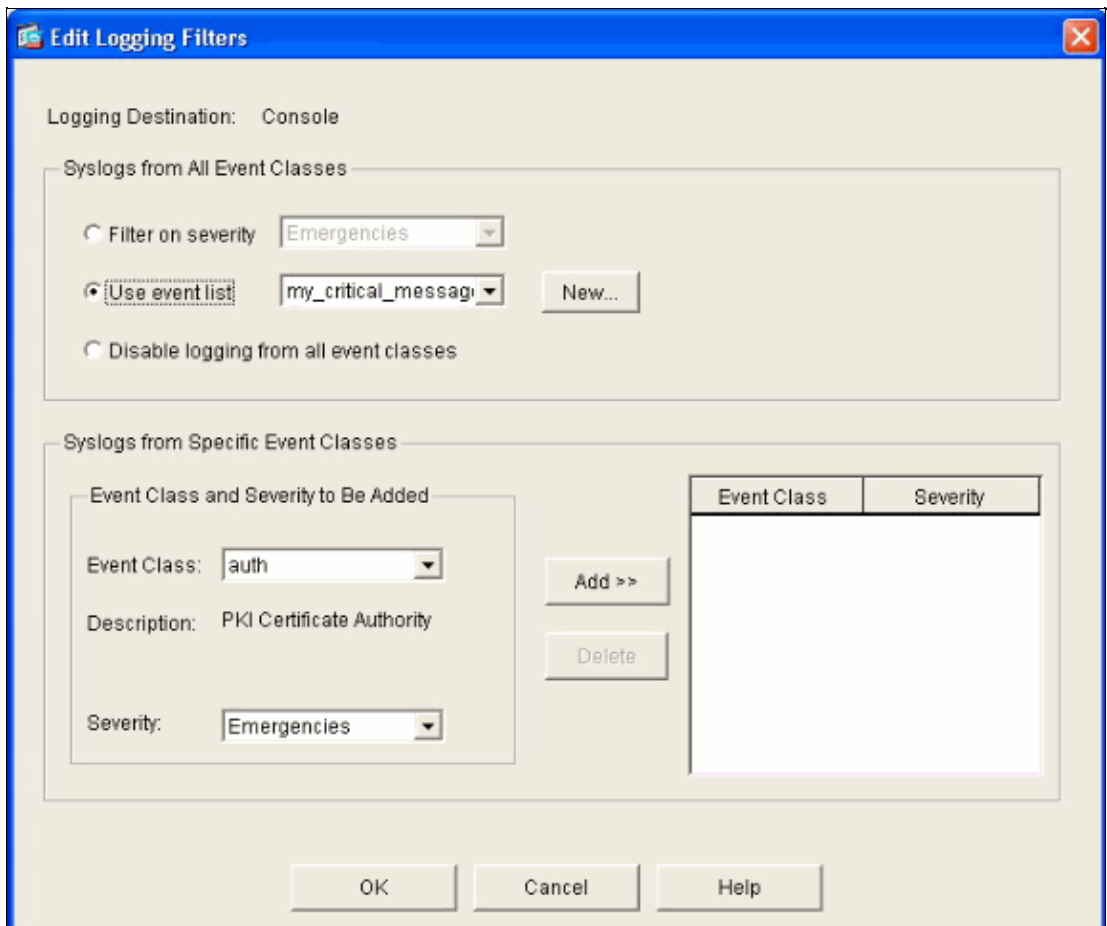
In this case, you need to put in messages with ID 611101–611323.



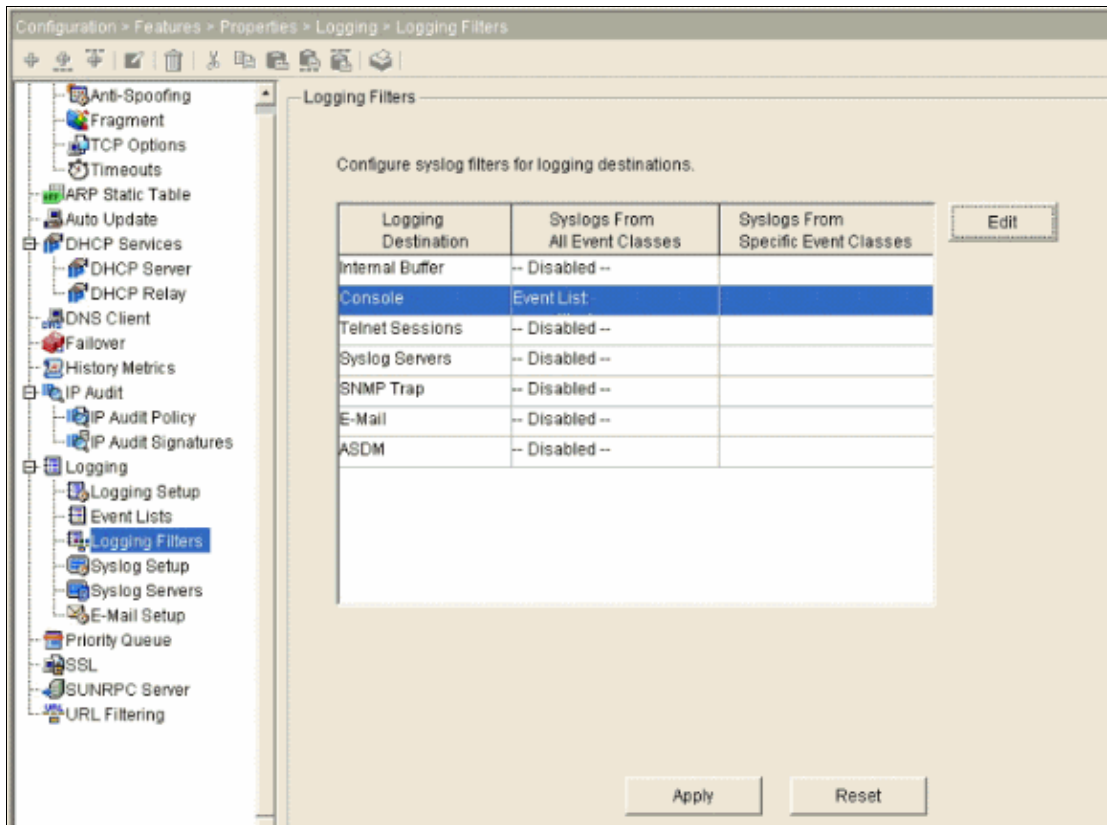
5. Put in the ID range in the Message IDs box and click **OK**.



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



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 in order 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 in order to send all ca class messages with a severity level of emergencies or higher to the console.

```
logging class ca console emergencies
```

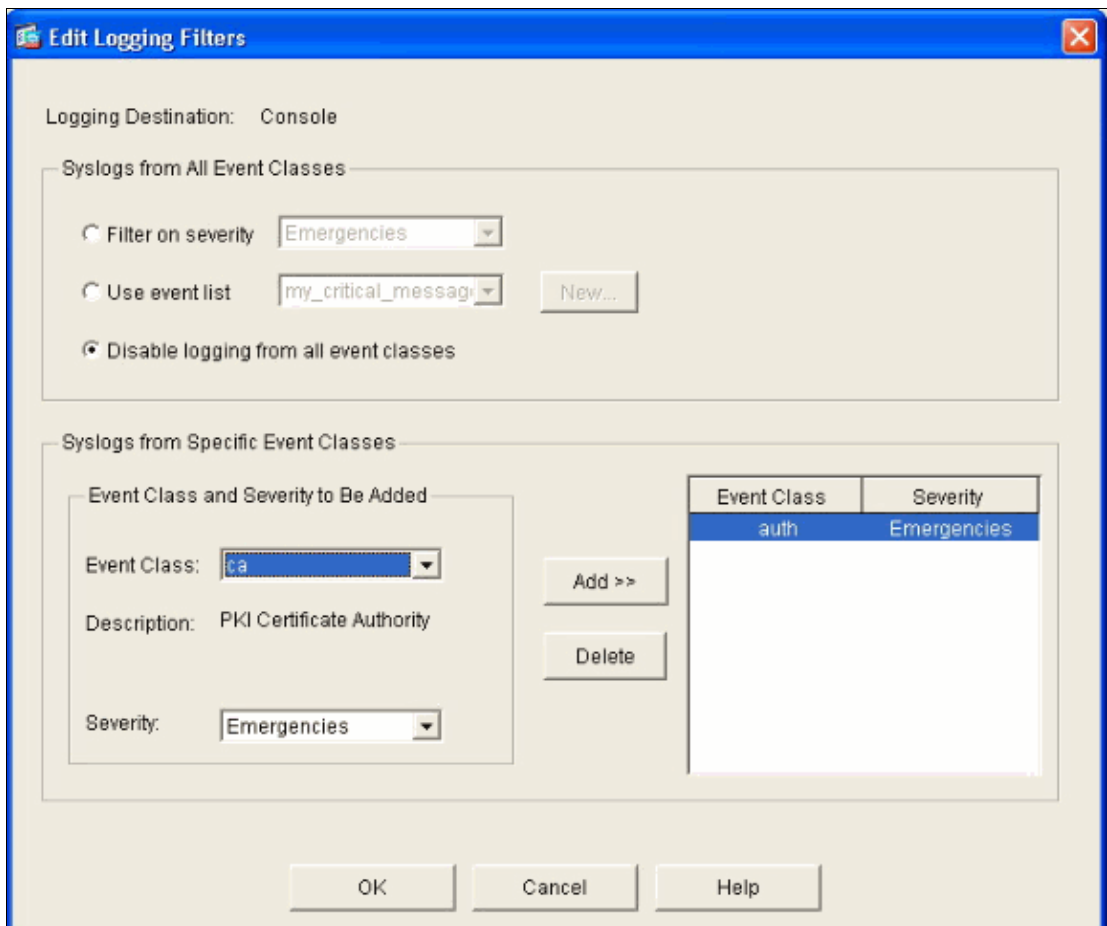
ASDM Configuration

This procedure shows the ASDM configurations for Example 3 with the use of the message list.

1. Choose 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.

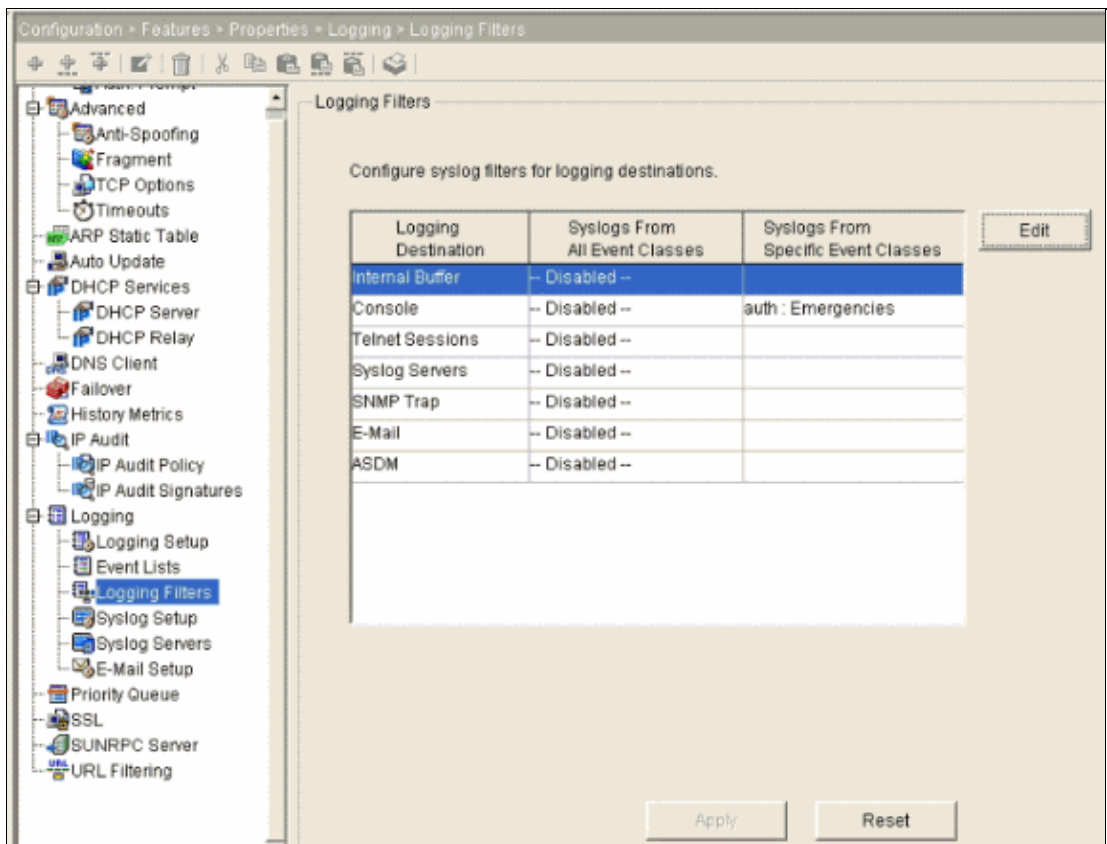
This procedure uses **ca** and **Emergencies** respectively.

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



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.

Log ACL ACE Hits

Add *log* to each access list element (ACE) you wish in order to log in order to log when an access list is hit. Use this syntax:

```
access-list id {deny | permit protocol} {source_addr source_mask}
{destination_addr destination_mask} {operator port} {log}
```

Example:

```
pixfirewall(config)#access-list 101 line 1 extended permit icmp any any log
```

When the *log* option is specified, it generates syslog message 106100 for the ACE to which it is applied. Syslog message 106100 is generated for every matching permit or deny ACE flow that passes through the PIX Firewall. The first-match flow is cached. Subsequent matches increment the hit count displayed in the **show access-list** command.

Unable to connect to remote host:, Connection timed out for the ACE, and new 106100 messages are generated at the end of the interval defined by interval seconds if the hit count for the flow is not zero. The default access list logging behavior, which is the *log* keyword not specified, is that if a packet is denied, then message 106023 is generated, and if a packet is permitted, then no syslog message is generated.

An optional syslog level (0 – 7) can be specified for the generated syslog messages (106100). If no level is specified, the default level is 6 (informational) for a new ACE. If the ACE already exists, then its existing log

level remains unchanged. If the *log disable* option is specified, access list logging is completely disabled. No syslog message, including message 106023, is generated. The *log* default option restores the default access list logging behavior.

Complete these steps in order to enable the syslog message 106100 to view in the console output:

1. Issue the **logging enable** command in order to enable transmission of system log messages to all output locations. You must set a logging output location in order to view any logs.
2. Issue the **logging message <message_number> level <severity_level>** command in order to set the severity level of a specific system log message.

In this case, issue the **logging message 106100** command to enable the message 106100.

3. Issue the **logging console message_list | severity_level** command in order to enable system log messages to display on the Security Appliance console (tty) as they occur. Set the *severity_level* from 1 to 7 or use the level name. You can also specify which messages are sent with the *message_list* variable.
4. Issue the **show logging message** command in order to display a list of system log message messages that have been modified from the default setting, which are messages that have been assigned a different severity level and messages that have been disabled.

This is sample output of the **show logging message** command:

```
pixfirewall#show logging message 106100
syslog 106100: default-level informational (enabled)
pixfirewall# %PIX-7-111009: User 'enable_15' executed cmd: show logging mess 106
100
```

Capture VPN Traffic Syslog Messages

Use the **logging list** command in order to capture the syslog for LAN-to-LAN and Remote access IPsec VPN messages alone. This example captures all VPN (IKE and IPsec) class system log messages with debugging level or higher.

Example:

```
hostname(config)#logging enable
hostname(config)#logging timestamp
hostname(config)#logging list my-list level debugging class vpn
hostname(config)#logging trap my-list
hostname(config)#logging host inside 192.168.1.1
```

Note: The **logging list** command is supported on 7.2(1) and later.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

1. If you do not receive the syslog 304001 messages, then make sure that the **inspect http** command is enabled on the ASA.
2. If you want to deny a specific syslog message to be sent to syslog server, then you must use the command as shown.

```
hostname(config)#no logging message <syslog_id>
```

Refer to the **logging message** command for more information.

%ASA-3-201008: Disallowing new connections

The %ASA-3-201008: Disallowing new connections. error message is seen when ASA is unable to contact syslog server and no new connections are allowed.

Solution

This message appears when you have enabled TCP system log messaging and the syslog server cannot be reached, or when you use Cisco ASA Syslog Server (PFSS) and the disk on the Windows NT system is full. Complete these steps in order to resolve this error message:

- Disable TCP system log messaging if it is enabled.
- If you use PFSS, free up space on the Windows NT system where PFSS resides.
- Also, make sure that the syslog server is up and you can ping the host from the Cisco ASA console.
- Restart TCP system message logging in order to allow traffic.

If the syslog server goes down and the TCP logging is configured either use the **logging permit-hostdown** command or switch to UDP logging.

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](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 21, 2007

Document ID: 63884
