Adaptive Security Appliance (ASA)-Syslog konfigurieren

Inhalt

Einleitung

In diesem Dokument wird die Beispielkonfiguration beschrieben, die veranschaulicht, wie auf ASA-Geräten mit Codeversion 8.4 oder höher verschiedene Protokollierungsoptionen konfiguriert werden.

Hintergrundinformationen

ASA Version 8.4 hat sehr detaillierte Filtertechniken eingeführt, um nur bestimmte Syslog-Meldungen anzeigen zu können. Im Abschnitt "Syslog-Grundlagen" dieses Dokuments wird eine herkömmliche Syslog-Konfiguration veranschaulicht. Im Abschnitt "Erweitertes Syslog" dieses Dokuments werden die neuen Syslog-Funktionen in Version 8.4 beschrieben. Eine vollständige Anleitung für Systemprotokollnachrichten finden Sie in den Leitfäden für Systemprotokollnachrichten der Cisco Security Appliance.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ASA 5515 mit ASA Softwareversion 8.4
- Cisco Adaptive Security Device Manager (ASDM) Version 7.1.6

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

> **Hinweis**: Weitere Informationen zu ähnlichen Konfigurationsdetails für ASDM in Version 7.1 und höher finden Sie unter ASA 8.2: Configure Syslog using ASDM (Konfigurieren von Syslog mithilfe von ASDM).

Syslog-Basis

Geben Sie diese Befehle ein, um die Protokollierung zu aktivieren, Protokolle anzuzeigen und Konfigurationseinstellungen anzuzeigen.

- **logging enable** - Ermöglicht die Übertragung von Syslog-Meldungen an alle Ausgabestandorte.
- **no logging enable -** Deaktiviert die Protokollierung an allen Ausgabestandorten.
- **show logging:** Listet den Inhalt des Syslog-Puffers sowie Informationen und Statistiken zur aktuellen Konfiguration auf.

Die ASA kann Syslog-Meldungen an verschiedene Ziele senden. Geben Sie die Befehle in diesen Abschnitten ein, um die Speicherorte anzugeben, an die die Syslog-Informationen gesendet

werden sollen:

Protokollierungsinformationen an den internen Puffer senden

```
logging buffered severity_level
```

Externe Software oder Hardware ist nicht erforderlich, wenn Sie die Syslog-Meldungen im internen ASA-Puffer speichern. Geben Sie den Befehl **show logging** (Protokollierung anzeigen) ein, um die gespeicherten Syslog-Meldungen anzuzeigen. Der interne Puffer hat eine maximale Größe von 1 MB (konfigurierbar mit dem Befehl **logging buffer-size**). Dadurch kann es sehr schnell einwickeln. Denken Sie daran, wenn Sie eine Protokollierungsebene für den internen Puffer wählen, da ausführlichere Protokollierungsebenen den internen Puffer schnell füllen und umschließen können.

Senden von Protokollinformationen an einen Syslog-Server

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

Ein Server, der eine Syslog-Anwendung ausführt, ist erforderlich, um Syslog-Meldungen an einen externen Host zu senden. ASA sendet standardmäßig Syslog an UDP-Port 514, es können jedoch Protokoll und Port ausgewählt werden. Wenn TCP als Protokoll ausgewählt wird, sendet die ASA Syslogs über eine TCP-Verbindung an den Syslog-Server. Wenn auf den Server nicht zugegriffen werden kann oder die TCP-Verbindung zum Server nicht hergestellt werden kann, blockiert die ASA standardmäßig ALLE neuen Verbindungen. Dieses Verhalten kann deaktiviert werden, wenn Sie **logging permit-hostdown** aktivieren. Weitere Informationen zum Befehl **logging permit-hostdown finden Sie im** Konfigurationsleitfaden.

> **Hinweis**: Die ASA ermöglicht nur Ports mit 1025-65535. Bei Verwendung anderer Ports tritt dieser Fehler auf:
> ciscoasa(config)# logging host tftp 192.168.1.1 udp/516
> WARNUNG: Die Sicherheitsstufe für die Schnittstelle Ethernet0/1 ist 0.
> **FEHLER: Port '516' liegt nicht im Bereich von 1025-65535.**

Protokollierungsinformationen als E-Mail senden

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

Ein SMTP-Server ist erforderlich, wenn Sie die Syslog-Meldungen in E-Mails versenden. Die richtige Konfiguration auf dem SMTP-Server ist erforderlich, um sicherzustellen, dass Sie E-Mails von der ASA erfolgreich an den angegebenen E-Mail-Client weiterleiten können. Wenn diese Protokollierungsebene auf eine sehr ausführliche Ebene festgelegt ist, z. B. debug oder informational, können Sie eine erhebliche Anzahl von Syslogs generieren, da jede von dieser Protokollierungskonfiguration gesendete E-Mail die Generierung von mehr als vier weiteren Protokollen verursacht.

Protokollinformationen an die serielle Konsole senden

```
logging console severity_level
```

Die Konsolenprotokollierung ermöglicht die Anzeige von Syslog-Meldungen auf der ASA-Konsole (tty), sobald diese auftreten. Wenn die Konsolenprotokollierung konfiguriert ist, ist die Protokollgenerierung auf der ASA auf 9.800 bit/s begrenzt, die Geschwindigkeit der seriellen ASA-Konsole. Dies kann dazu führen, dass Syslogs an alle Ziele verworfen werden, die den internen Puffer enthalten. Verwenden Sie deshalb keine Konsolenprotokollierung für ausführliche Syslogs.

Senden von Protokollinformationen an eine Telnet-/SSH-Sitzung

```
logging monitor severity_level
terminal monitor
```

Der Protokollierungsmonitor ermöglicht die Anzeige von Syslog-Meldungen, wenn Sie mit Telnet oder SSH auf die ASA-Konsole zugreifen und der Befehl **terminal monitor** von dieser Sitzung aus ausgeführt wird. Um das Drucken von Protokollen für Ihre Sitzung zu beenden, geben Sie den Befehl **terminal no monitor** ein.

Anzeigen von Protokollmeldungen auf dem ASDM

```
logging asdm severity_level
```

ASDM verfügt außerdem über einen Puffer, der zum Speichern von Syslog-Meldungen verwendet werden kann. Geben Sie den Befehl **show logging asdm** ein, um den Inhalt des ASDM-Syslog-Puffers anzuzeigen.

Protokolle an eine SNMP-Managementstation senden

```
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
```

Benutzer benötigen eine vorhandene, funktionale SNMP-Umgebung (Simple Network Management Protocol), um Syslog-Meldungen mit SNMP zu senden. Eine vollständige Referenz zu den Befehlen, die Sie zum Festlegen und Verwalten von Ausgabezielen verwenden können, finden Sie unter Befehle für das Festlegen und Verwalten von Ausgabezielen. Informationen zu den Meldungen nach Schweregrad finden Sie unter Meldungen nach Schweregrad.

Zeitstempel zu Syslogs hinzufügen

Um die Ausrichtung und Reihenfolge von Ereignissen zu erleichtern, können Syslogs Zeitstempel hinzugefügt werden. Dies wird empfohlen, um Probleme zeitlich zu erfassen. Um Zeitstempel zu aktivieren, geben Sie den Befehl **logging timestamp (Protokollierungszeitstempel)** ein. Im Folgenden finden Sie zwei Syslog-Beispiele: eines ohne Zeitstempel und eines mit:

```
%ASA-6-302016: Teardown UDP connection 806353 for outside:172.18.123.243/24057 to
identity:172.18.124.136/161 duration 0:02:01 bytes 313

Jul 03 2014 14:33:09: %ASA-6-302014: Teardown TCP connection 806405 for
```

```
inside:10.0.0.100/50554 to identity:172.18.124.136/51358 duration 0:00:00 bytes
442 TCP Reset-I
```

Beispiel 1

Diese Ausgabe zeigt eine Beispielkonfiguration für die Anmeldung beim **Puffer** mit dem Schweregrad **debugging**.

```
logging enable
logging buffered debugging
```

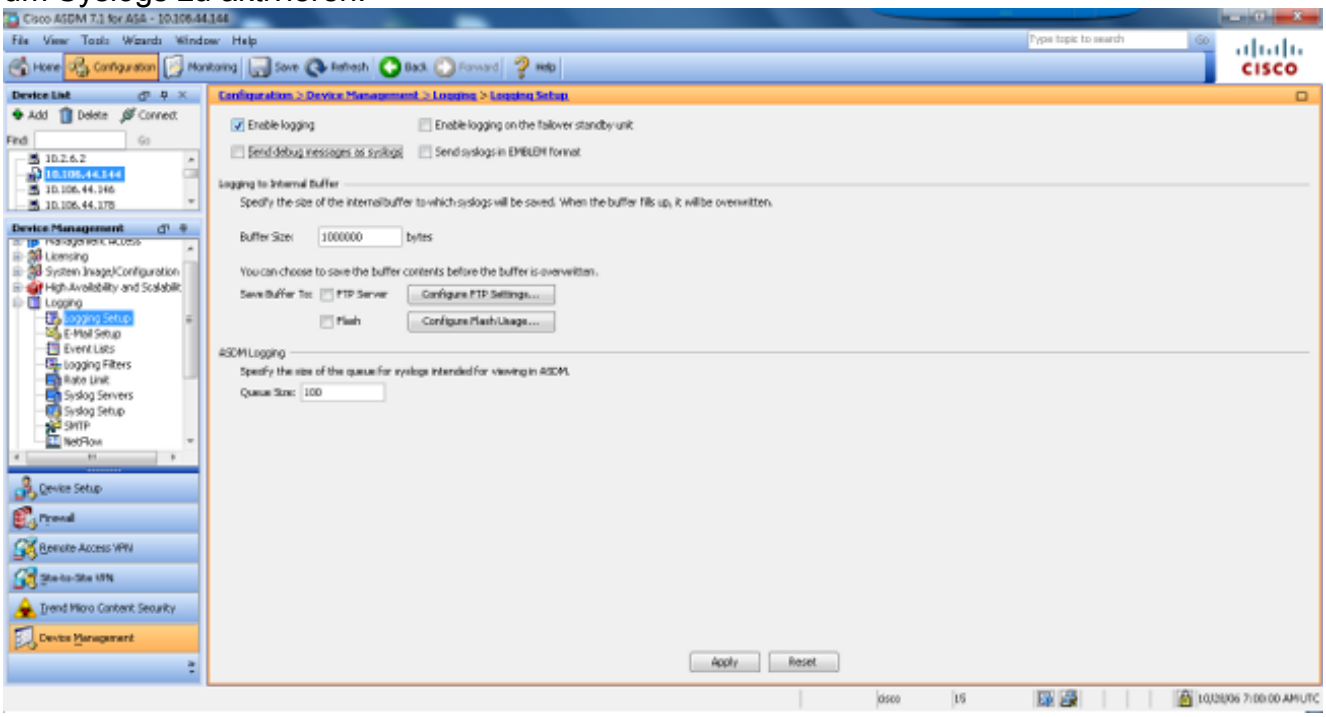
Dies ist die Beispielausgabe.

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

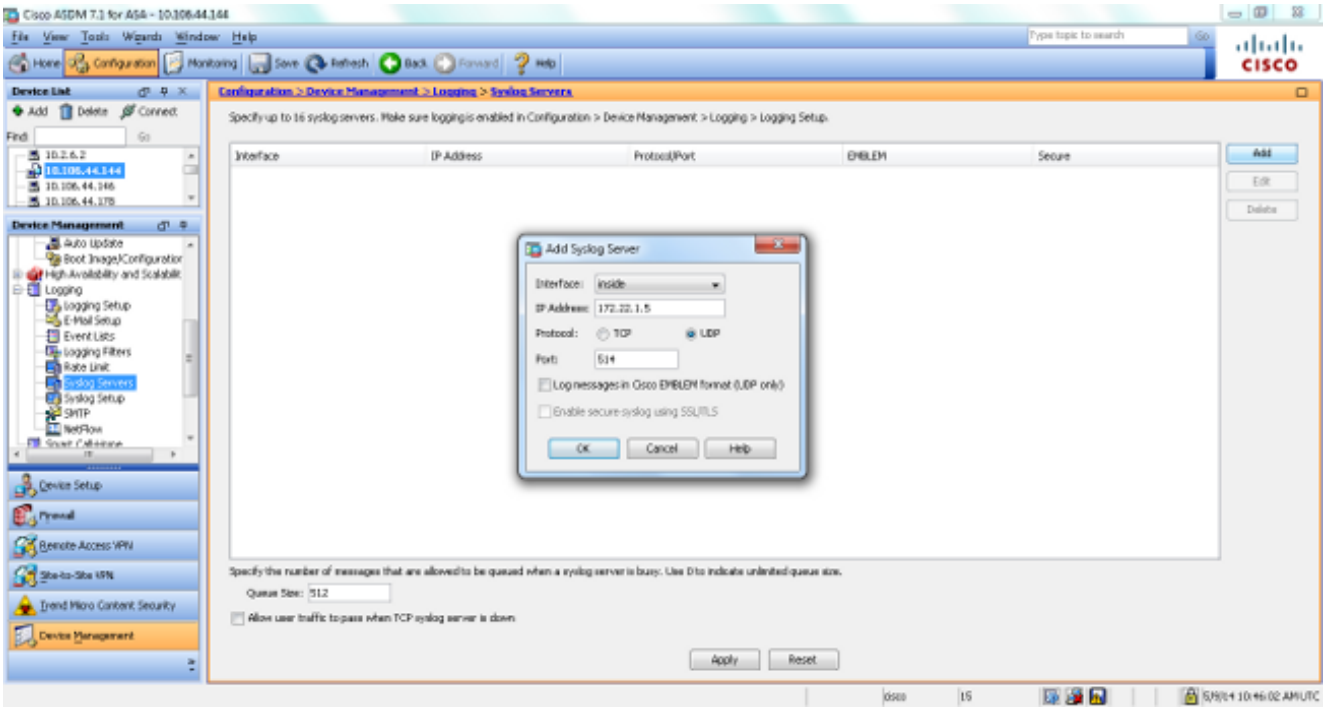
Konfigurieren von einfachem Syslog über ASDM

Dieses Verfahren veranschaulicht die ASDM-Konfiguration für alle verfügbaren Syslog-Ziele.

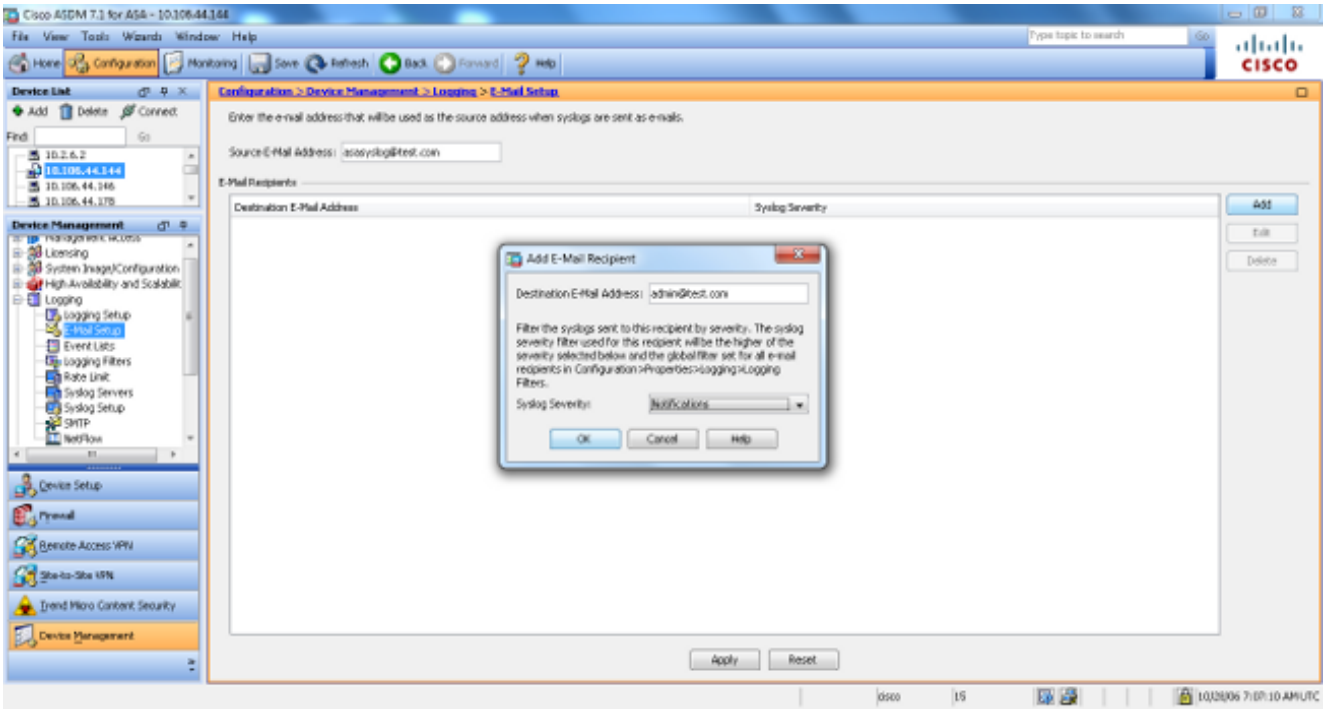
1. Um die Protokollierung auf der ASA zu aktivieren, konfigurieren Sie zunächst die grundlegenden Protokollierungsparameter. Wählen Sie **Configuration > Features > Properties > Logging > Logging Setup**. Aktivieren Sie das Kontrollkästchen **Enable logging**, um Syslogs zu aktivieren.



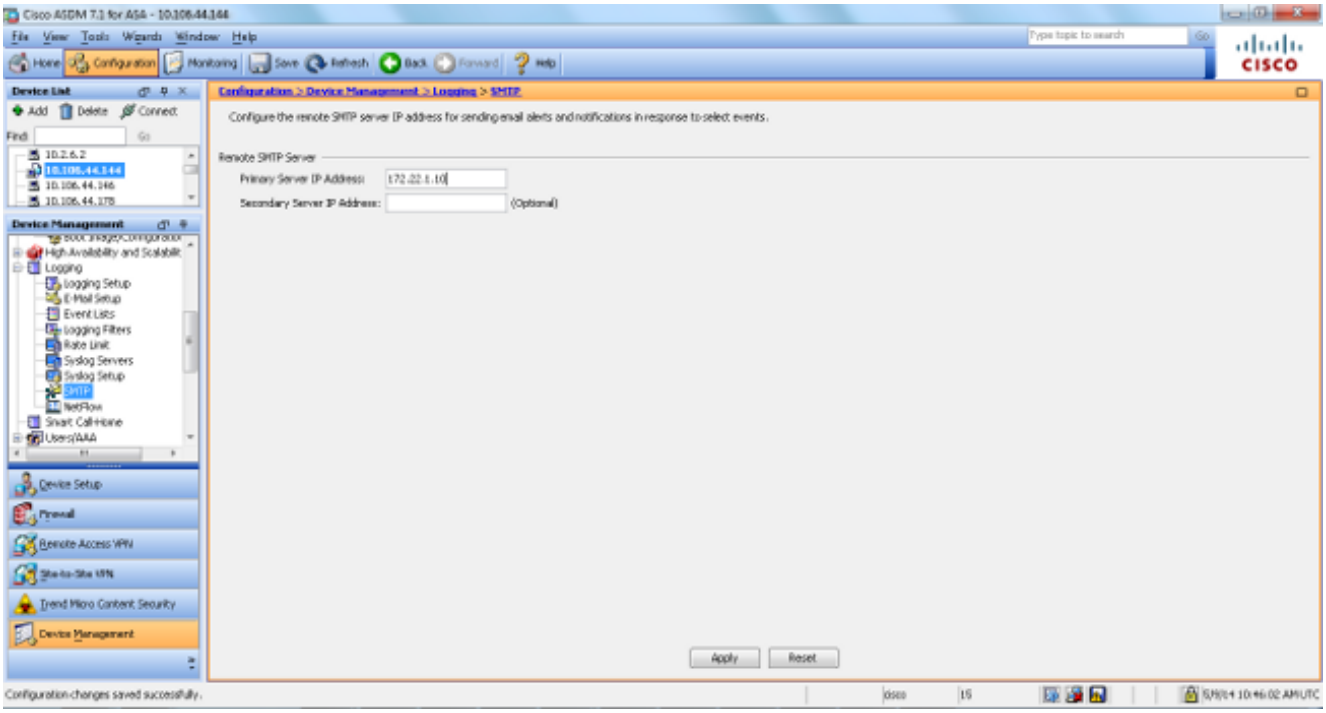
2. Um einen externen Server als Ziel für Syslogs zu konfigurieren, wählen Sie **Syslog Servers** in Logging (**Syslog-Server** in Protokollierung) aus, und klicken Sie auf **Add (Hinzufügen)**, um einen Syslog-Server hinzuzufügen. Geben Sie die Syslog-Serverdetails in das Feld Syslog-Server hinzufügen ein, und wählen Sie **OK**, wenn Sie fertig sind.



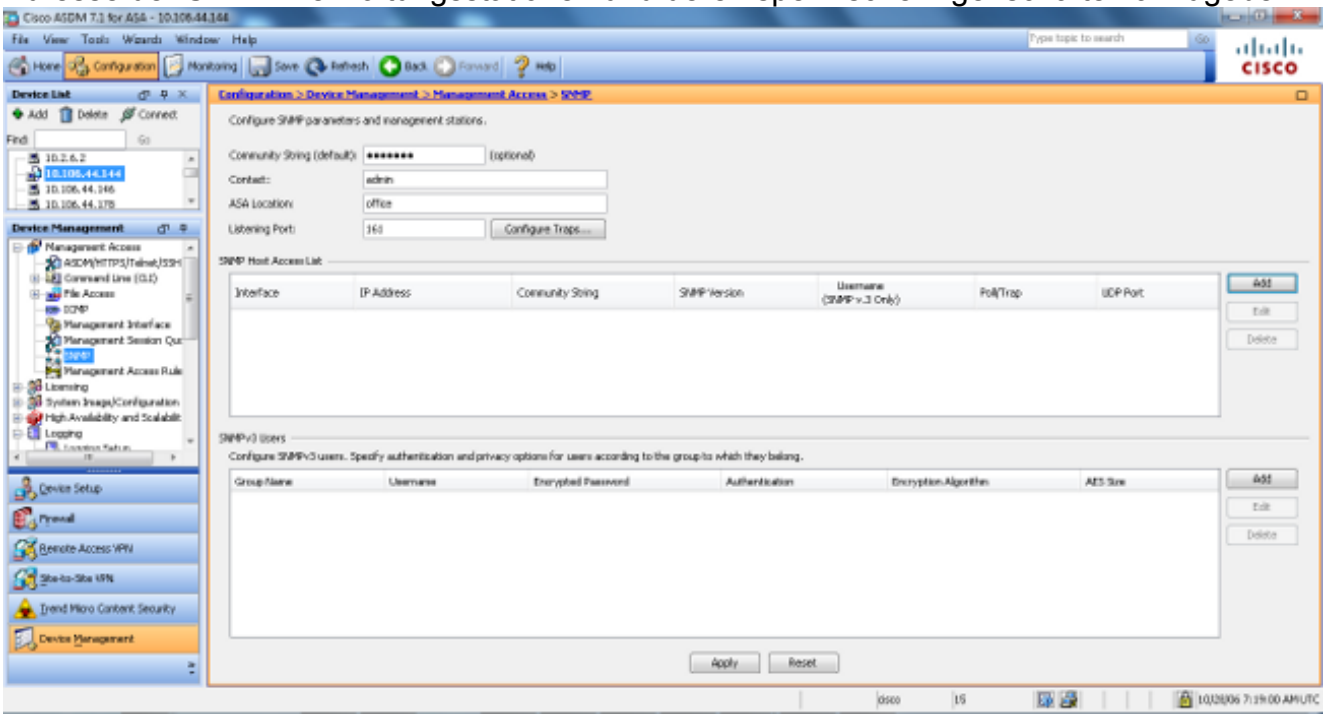
3. Wählen Sie **E-Mail Setup** in Logging (Protokollierung) aus, um Syslog-Meldungen als E-Mails an bestimmte Empfänger zu senden. Geben Sie die E-Mail-Quelladresse im Feld E-Mail-Quelladresse an, und wählen Sie **Hinzufügen,** um die E-Mail-Zieladresse der E-Mail-Empfänger und den Schweregrad der Nachricht zu konfigurieren. Klicken Sie abschließend auf **OK**.



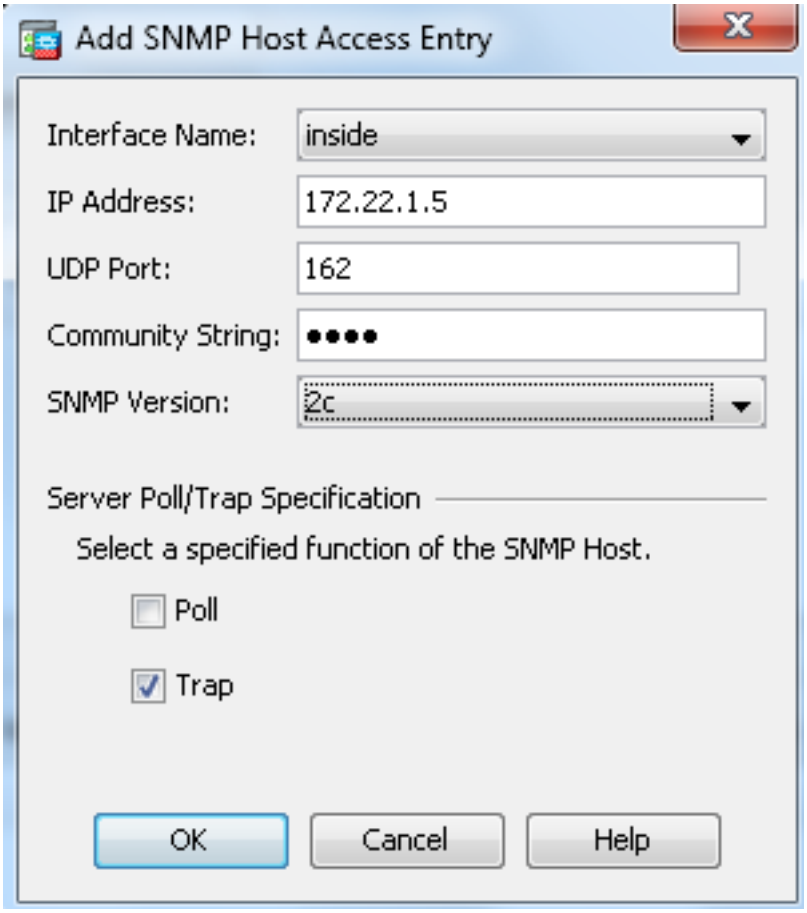
4. Wählen Sie **Device Administration (Geräteverwaltung)**, **Logging (Protokollierung),** wählen Sie **SMTP aus**, und geben Sie die IP-Adresse des primären Servers ein, um die IP-Adresse des SMTP-Servers anzugeben.



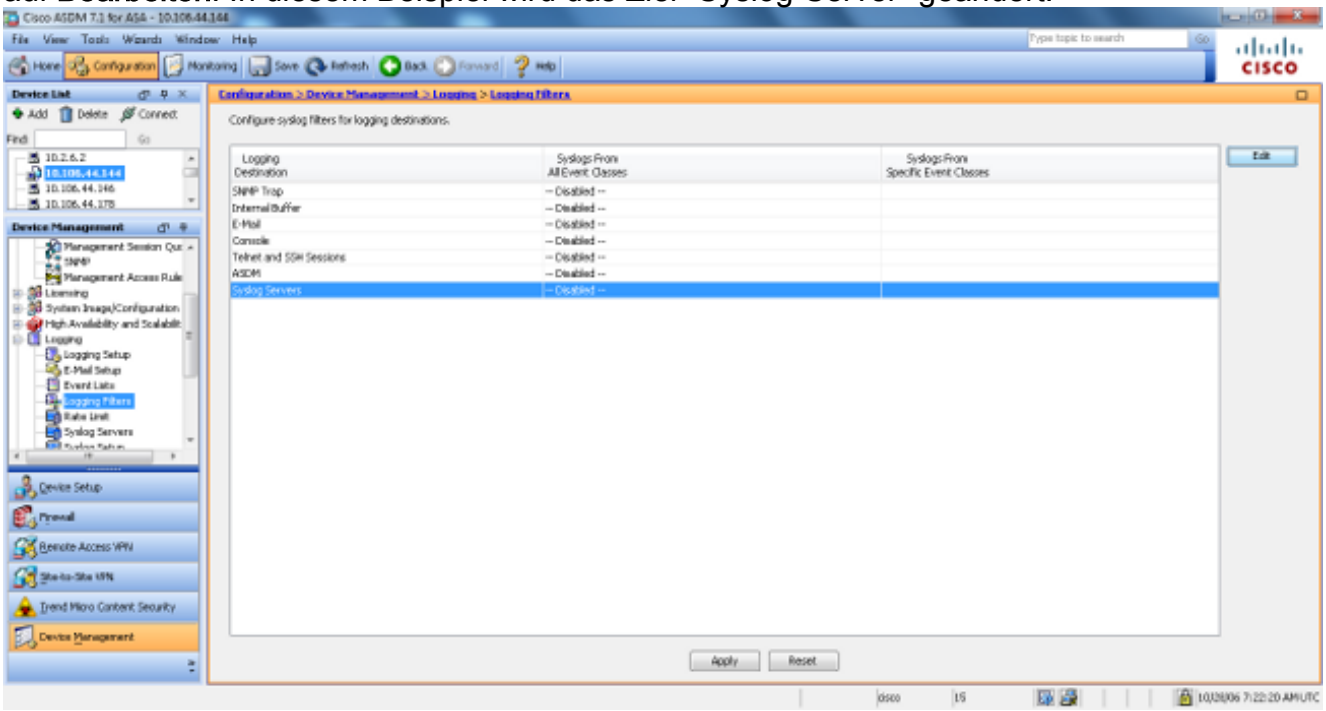
5. Wenn Sie Syslogs als SNMP-Traps senden möchten, müssen Sie zunächst einen SNMP-Server definieren. Wählen Sie im Menü **Verwaltungszugriff** die Option **SNMP aus**, um die Adresse der SNMP-Verwaltungsstationen und deren spezifische Eigenschaften anzugeben.



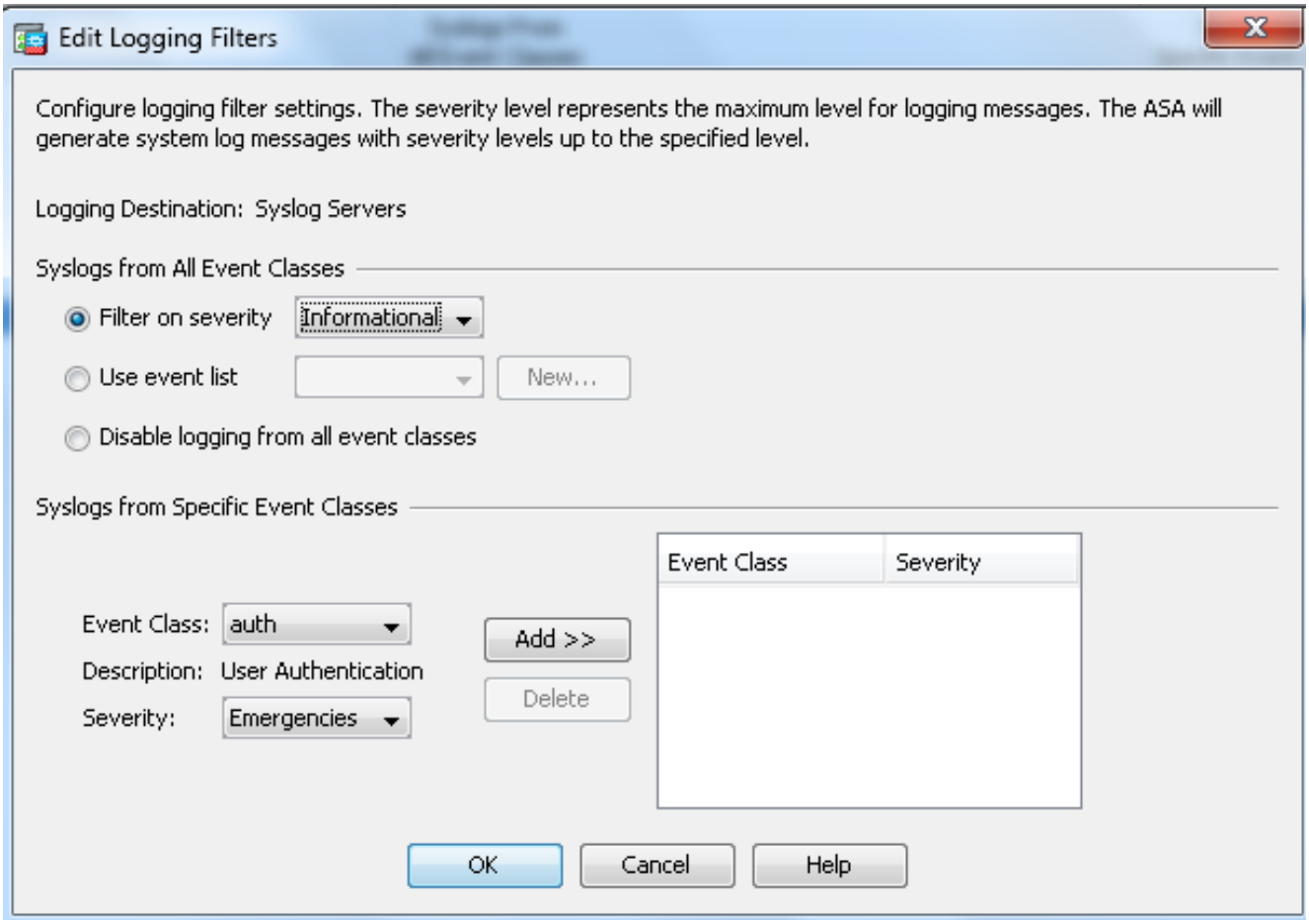
6. Wählen Sie **Hinzufügen** aus, um eine SNMP-Managementstation hinzuzufügen. Geben Sie die SNMP-Hostdetails ein, und klicken Sie auf **OK**.



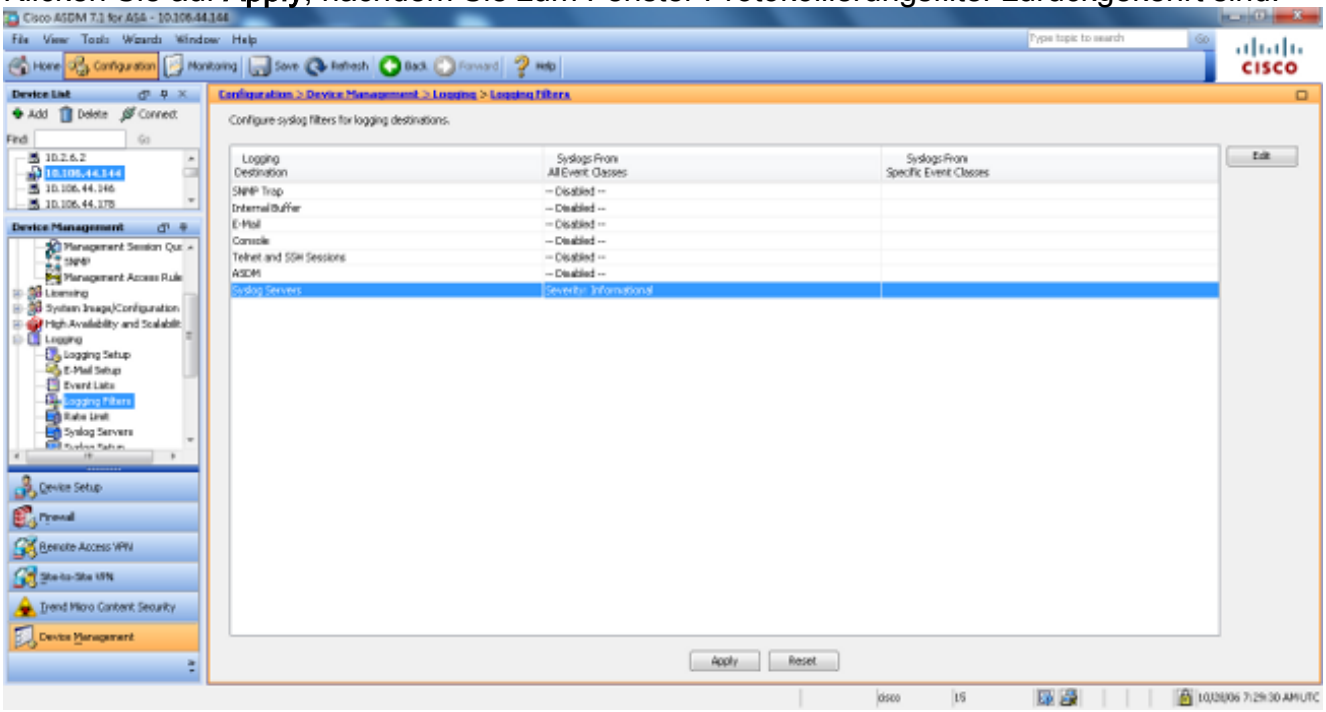
7. Um das Senden von Protokollen an eines der zuvor genannten Ziele zu ermöglichen, wählen Sie im Abschnitt "Protokollierung" die Option **Protokollierungsfilter**. Dadurch werden Ihnen jedes mögliche Protokollierungsziel und die aktuelle Ebene der Protokolle angezeigt, die an diese Ziele gesendet werden. Wählen Sie das gewünschte Protokollziel aus, und klicken Sie auf **Bearbeiten**. In diesem Beispiel wird das Ziel "Syslog-Server" geändert.



8. Wählen Sie in der Dropdown-Liste **Nach Schweregrad filtern** einen geeigneten Schweregrad aus (in diesem Fall **Informational**). Klicken Sie abschließend auf **OK**.



9. Klicken Sie auf **Apply**, nachdem Sie zum Fenster Protokollierungsfilter zurückgekehrt sind.

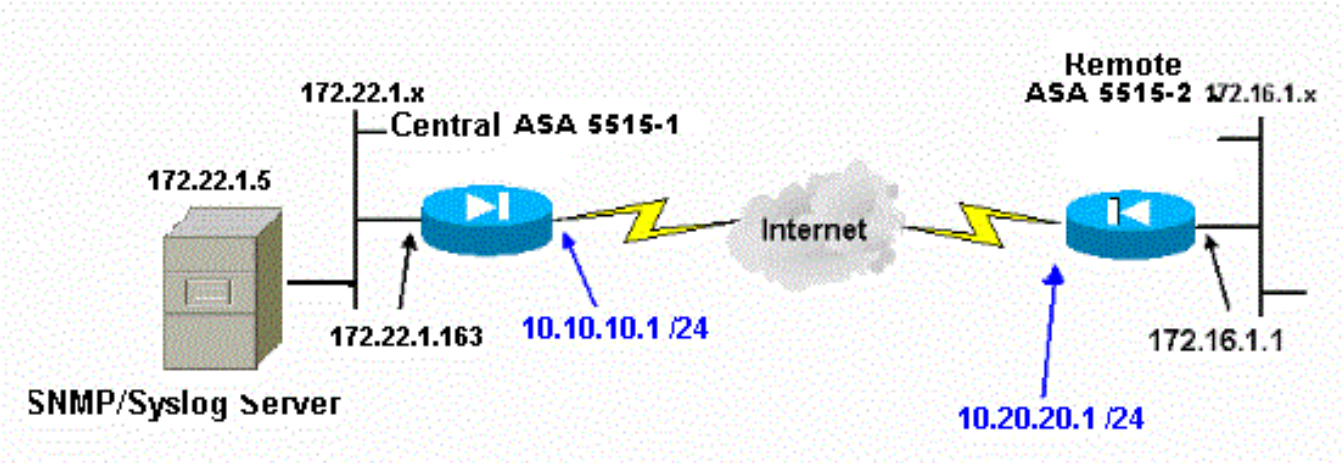


Syslog-Meldungen über ein VPN an einen Syslog-Server senden

Im einfachen Site-to-Site-VPN-Design oder im komplizierteren Hub-and-Spoke-Design kann der Administrator alle entfernten ASA-Firewalls mit dem SNMP- und Syslog-Server an einem zentralen Standort überwachen.

Informationen zur Konfiguration der Site-to-Site-IPsec-VPN-Konfiguration finden Sie unter PIX/ASA 7.x und höher: Konfigurationsbeispiel für den PIX-to-PIX-VPN-Tunnel. Neben der VPN-

Konfiguration müssen Sie das SNMP und den interessanten Datenverkehr für den Syslog-Server sowohl in der Zentrale als auch am lokalen Standort konfigurieren.



Zentrale ASA-Konfiguration

```
!--- This access control list (ACL) defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also includes the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind the ASA 5515.

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 ASA.

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 enable
logging trap 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 community ***** version 2c
snmp-server community *****
```

Remote-ASA-Konfiguration

```
!--- This ACL defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind ASA 5515.
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 ASA 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 community ***** version 2c
snmp-server community *****
```

Weitere Informationen zur Konfiguration von ASA Version 8.4 finden Sie unter Monitoring Cisco Secure ASA Firewall Using SNMP and Syslog Through VPN Tunnel (Cisco Secure ASA Firewall mit SNMP und Syslog durch VPN-Tunnel überwachen).

Erweitertes Syslog

ASA Version 8.4 bietet verschiedene Mechanismen, mit denen Sie Syslog-Meldungen in Gruppen konfigurieren und verwalten können. Zu diesen Mechanismen gehören der Schweregrad einer Nachricht, die Nachrichtenklasse, die Nachrichten-ID oder eine benutzerdefinierte Nachrichtenliste, die Sie erstellen. Mithilfe dieser Mechanismen können Sie einen einzelnen Befehl eingeben, der für kleine oder große Gruppen von Nachrichten gilt. Wenn Sie Syslogs auf diese Weise einrichten, können Sie die Nachrichten aus der angegebenen Nachrichtengruppe erfassen und nicht mehr alle Nachrichten mit demselben Schweregrad.

Nachrichtenliste verwenden

Verwenden Sie die Nachrichtenliste, um nur die interessierten Syslog-Meldungen nach Schweregrad und ID in eine Gruppe aufzunehmen. Ordnen Sie diese Nachrichtenliste dann dem gewünschten Ziel zu.

Gehen Sie wie folgt vor, um eine Nachrichtenliste zu konfigurieren:

1. Geben Sie ***message_list*** in die **Protokollierungsliste ein. | *level severity_level [class message_class]*** Befehl, um eine Nachrichtenliste zu erstellen, die Meldungen mit einem bestimmten Schweregrad oder einer bestimmten Nachrichtenliste enthält.
2. Geben Sie den Befehl **logging list *message_list* message *syslog_id-syslog_id2*** ein, um der soeben erstellten Nachrichtenliste weitere Nachrichten hinzuzufügen.
3. Geben Sie den Befehl **logging *destination message_list*** ein, um das Ziel der erstellten Nachrichtenliste anzugeben.

Beispiel 2

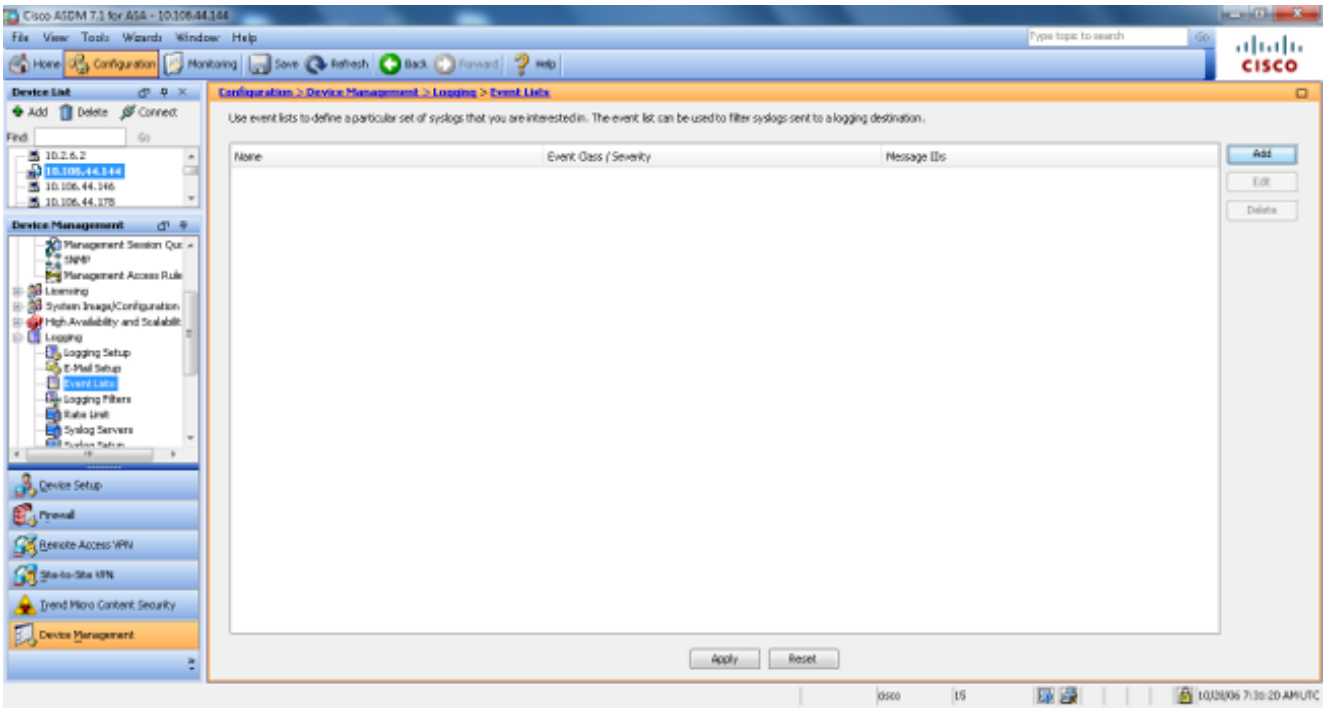
Geben Sie die folgenden Befehle ein, um eine Nachrichtenliste zu erstellen, die alle Meldungen mit dem Schweregrad 2 (kritisch) sowie die Meldungen 611101 bis 611323 enthält, und um sie an die Konsole senden zu lassen:

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

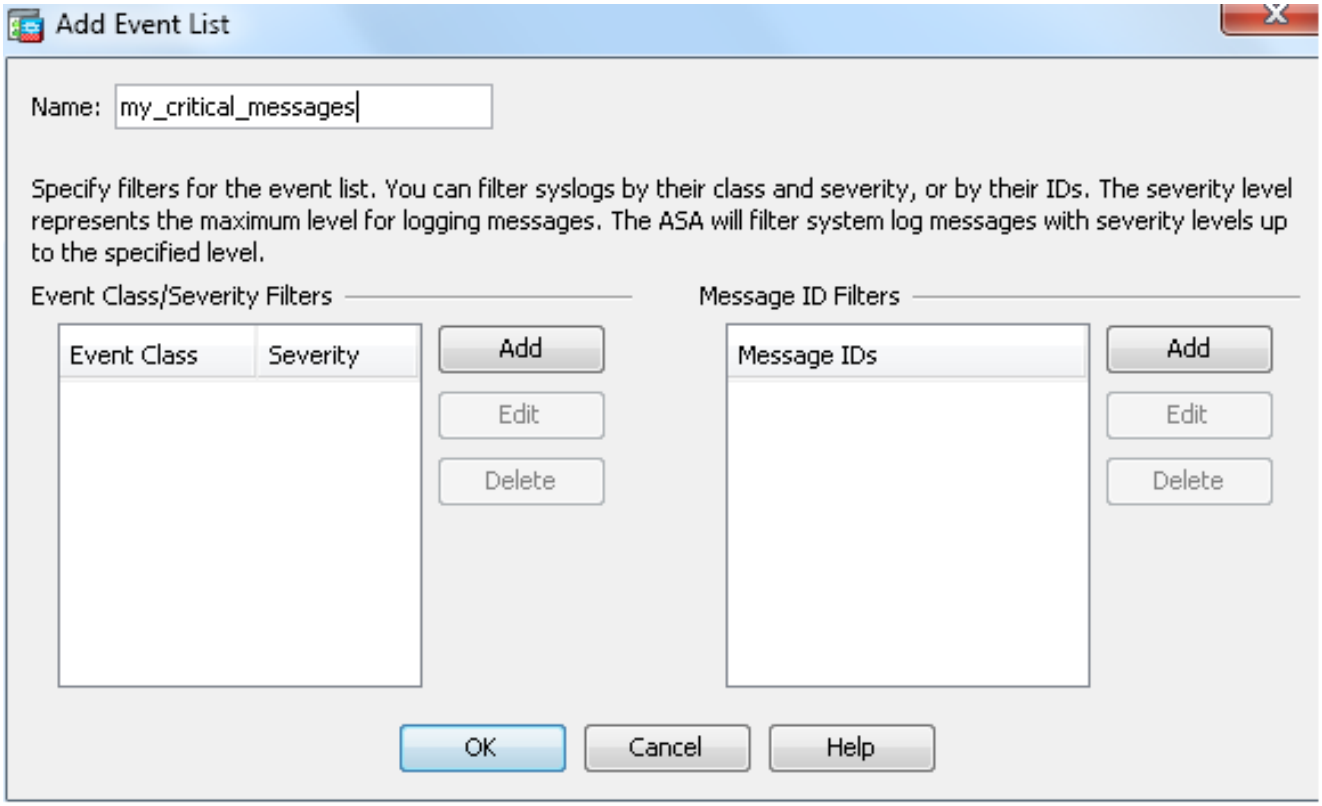
ASDM-Konfiguration

Dieses Verfahren zeigt eine ASDM-Konfiguration für Beispiel 2 unter Verwendung der Nachrichtenliste.

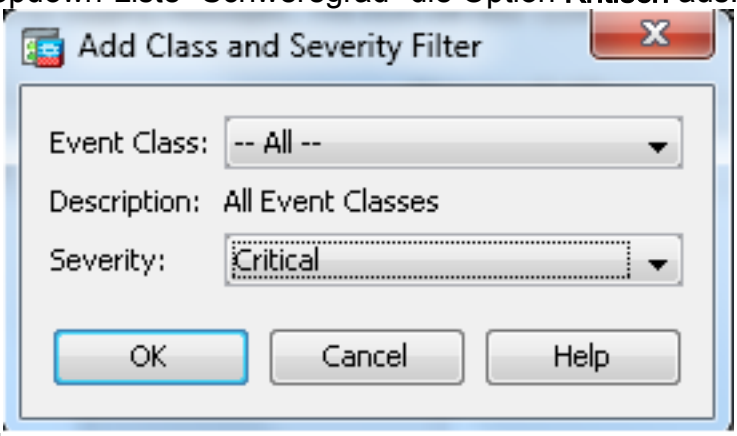
1. Wählen Sie unter Protokollierung die Option **Ereignislisten** aus, und klicken Sie auf **Hinzufügen**, um eine Nachrichtenliste zu erstellen.



2. Geben Sie den Namen der Nachrichtenliste in das Feld Name ein. In diesem Fall wird **my_critical_messages** verwendet. Klicken Sie unter Ereignisklassen-/Schweregradfilter auf **Hinzufügen**.

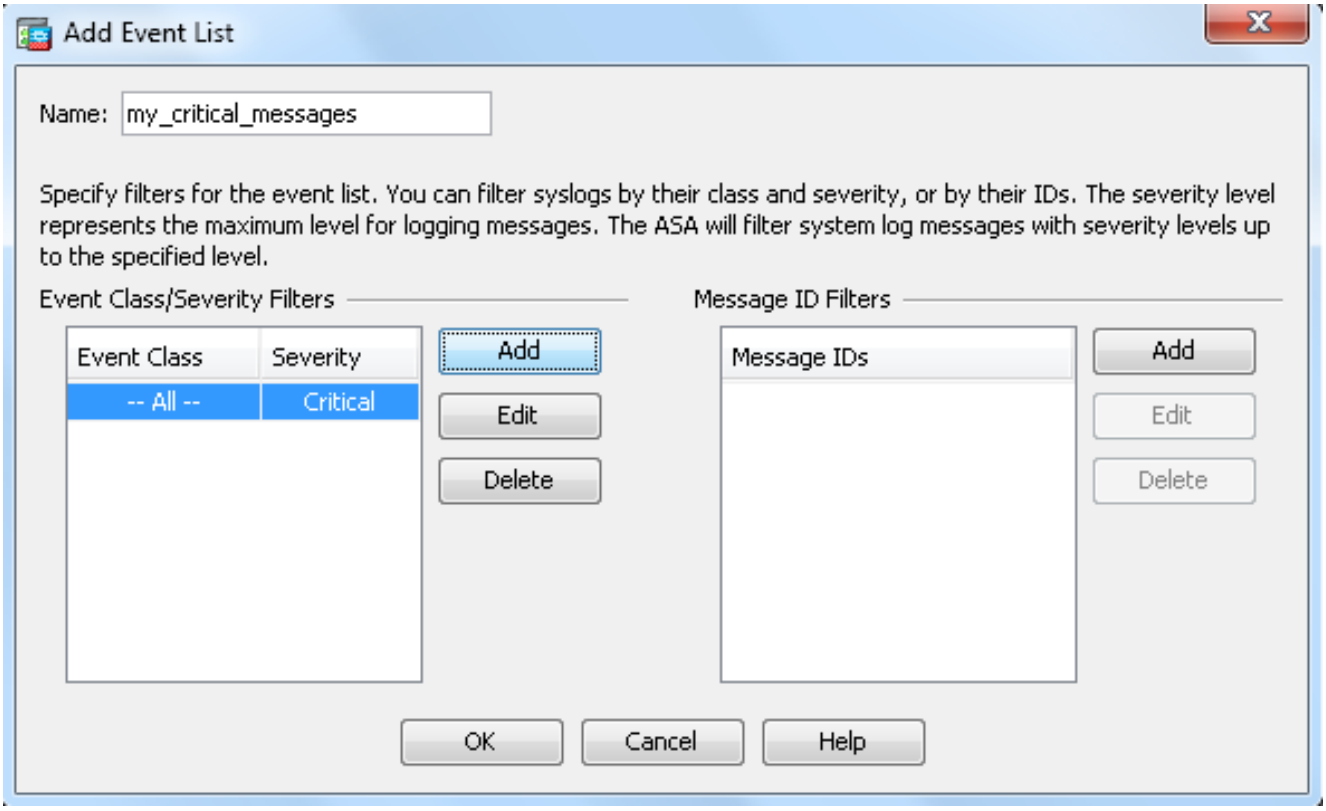


3. Wählen Sie in der Dropdown-Liste Event Class (Ereignisklasse) die Option **All (Alle)** aus. Wählen Sie in der Dropdown-Liste "Schweregrad" die Option **Kritisch** aus. Klicken Sie

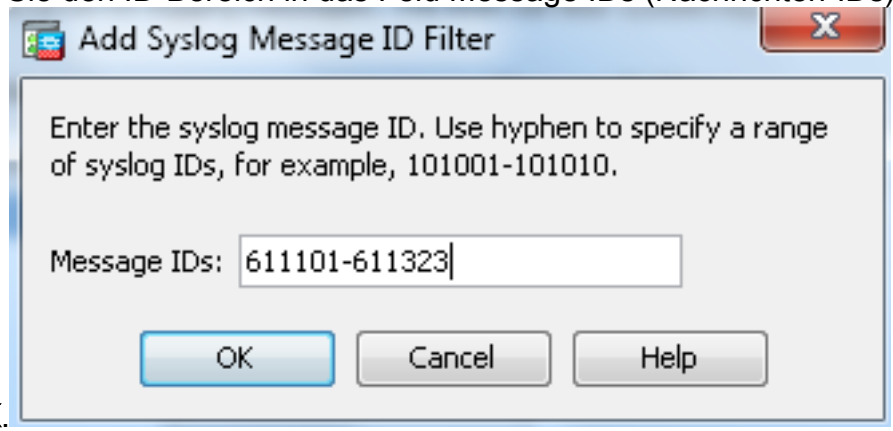


abschließend auf **OK**.

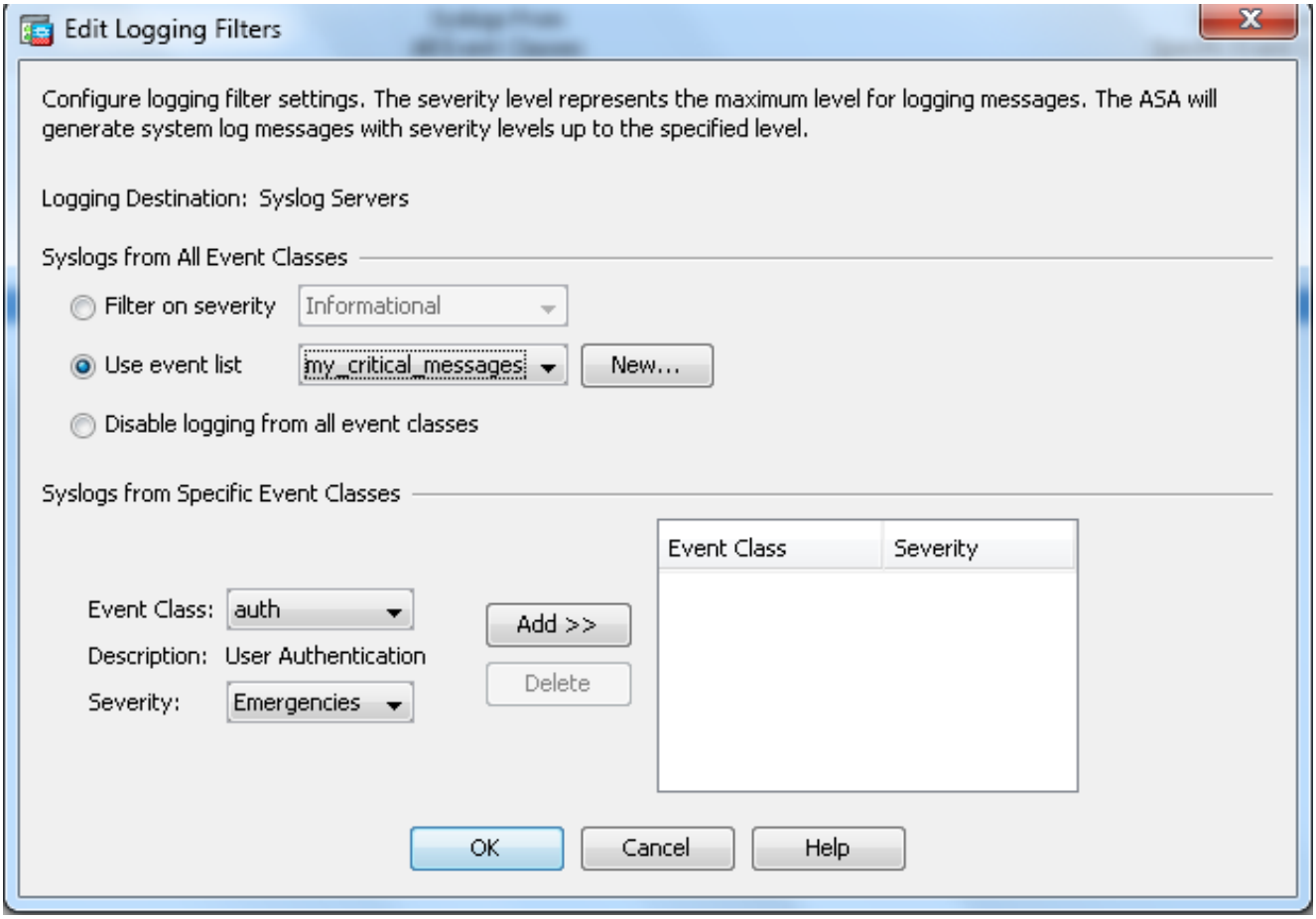
4. Klicken Sie unter "Message ID Filters" (Nachrichten-ID-Filter) auf **Add** (Hinzufügen), wenn weitere Nachrichten erforderlich sind. In diesem Fall müssen Sie Nachrichten mit der ID 611101-611323
eingeben.



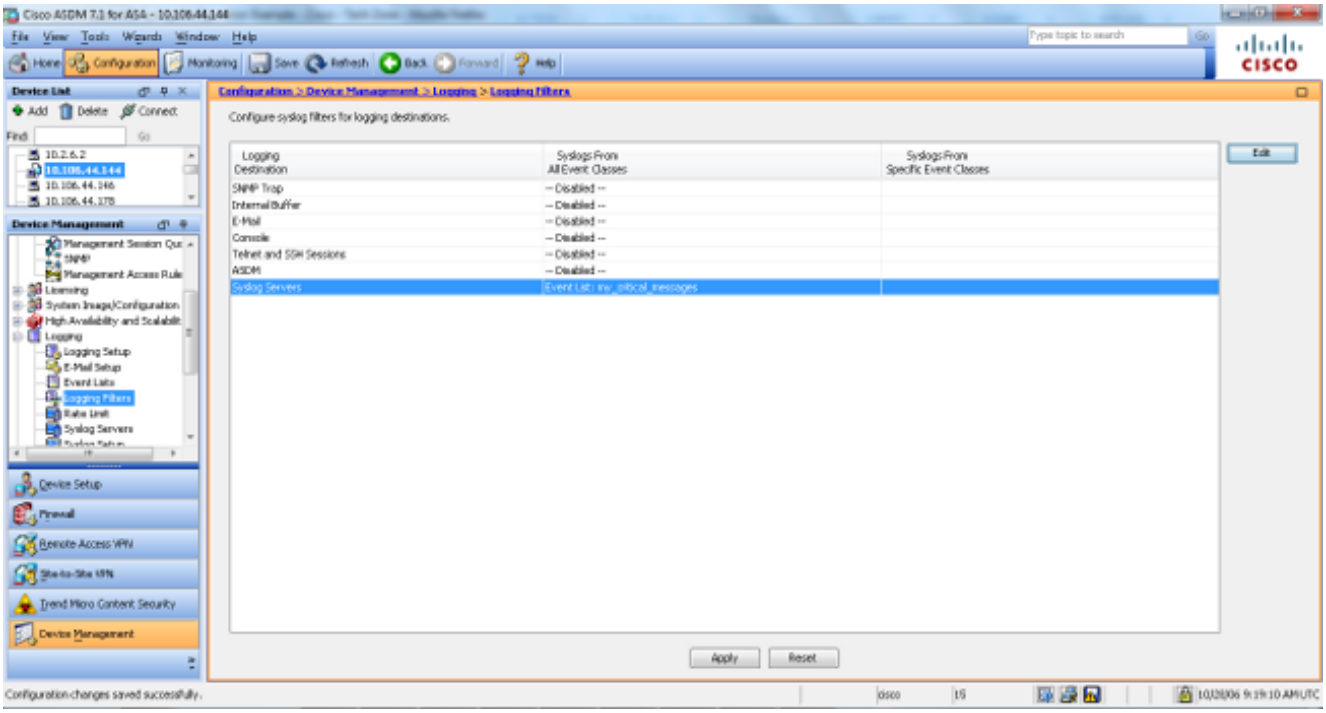
5. Geben Sie den ID-Bereich in das Feld Message IDs (Nachrichten-IDs) ein, und klicken Sie auf **OK**.



6. Wechseln Sie zurück zum Menü **Protokollierungsfilter**, und wählen Sie **Konsole** als Ziel aus.
7. Wählen Sie **my_critical_messages** aus der Dropdown-Liste **Use event list** (Ereignisliste verwenden) aus. Klicken Sie abschließend auf **OK**.



8. Klicken Sie auf **Apply**, nachdem Sie zum Fenster Protokollierungsfilter zurückgekehrt sind.



Damit sind die ASDM-Konfigurationen mit einer Nachrichtenliste gemäß Beispiel 2 abgeschlossen.

Verwenden der Message-Klasse

Verwenden Sie die Nachrichtenklasse, um alle einer Klasse zugeordneten Nachrichten an den angegebenen Ausgabespeicherort zu senden. Wenn Sie einen Schwellenwert für den Schweregrad angeben, können Sie die Anzahl der Nachrichten begrenzen, die an den Ausgabespeicherort gesendet werden.

```
logging class message_class destination | severity_level
```

Beispiel 3

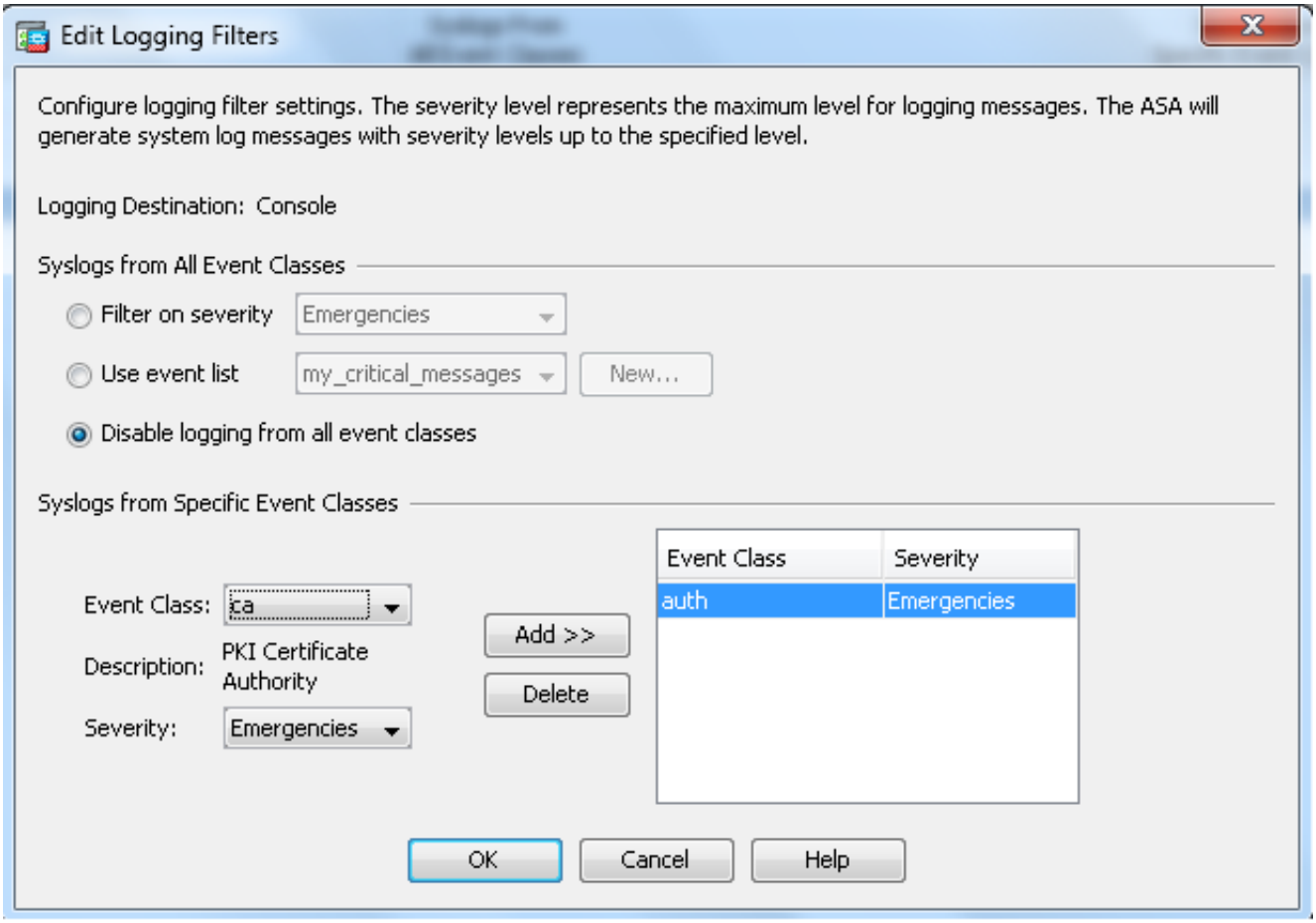
Geben Sie diesen Befehl ein, um alle ca-Klassenmeldungen mit einem Schweregrad von Notfällen oder höher an die Konsole zu senden.

```
logging class ca console emergencies
```

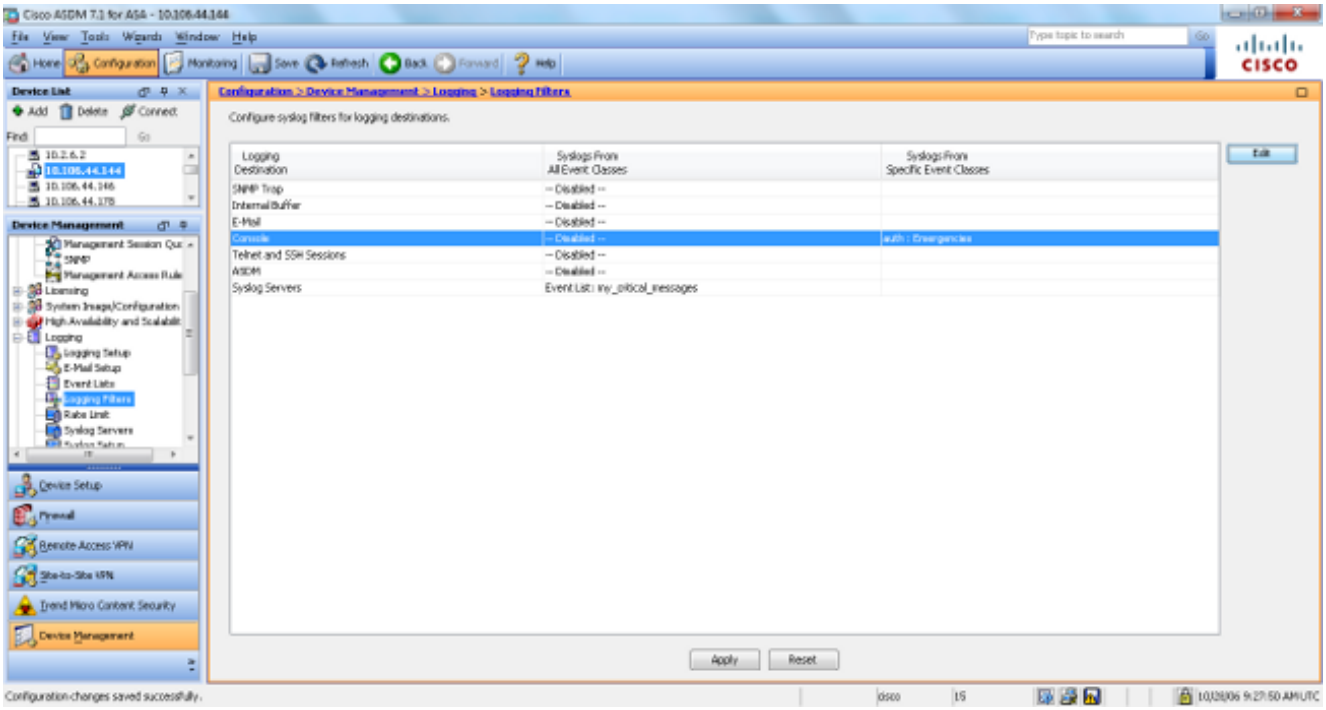
ASDM-Konfiguration

Dieses Verfahren zeigt die ASDM-Konfigurationen für Beispiel 3 unter Verwendung der Nachrichtenliste.

1. Wählen Sie das Menü **Protokollierungsfilter** und anschließend **Konsole** als Ziel aus.
2. Klicken Sie auf **Protokollierung für alle Ereignisklassen deaktivieren**.
3. Wählen Sie unter Syslogs from Specific Event Classes (Syslogs aus bestimmten Ereignisklassen) die Ereignisklasse und den Schweregrad aus, die Sie hinzufügen möchten.Bei diesem Verfahren werden **ca**. und **Notfälle** jeweils verwendet.
4. Klicken Sie auf **Hinzufügen**, um dies der Nachrichtenklasse hinzuzufügen, und klicken Sie auf
OK.



5. Klicken Sie auf **Apply**, nachdem Sie zum Fenster Protokollierungsfilter zurückgekehrt sind. Die Konsole erfasst jetzt die ca-Klassenmeldung mit dem Schweregrad Notfälle, wie im Fenster Protokollierungsfilter
angezeigt.



Damit ist die ASDM-Konfiguration für Beispiel 3 abgeschlossen. Eine Liste der Schweregrade für Protokollmeldungen finden Sie unter Nachrichten nach Schweregrad.

Senden von Debug-Protokollmeldungen an einen Syslog-Server

Für eine erweiterte Fehlerbehebung sind feature-/protokollspezifische Debug-Protokolle erforderlich. Diese Protokollmeldungen werden standardmäßig auf dem Terminal (SSH/Telnet) angezeigt. Je nach Art des Debugging und der Anzahl der generierten Debugging-Meldungen kann sich die Verwendung der CLI als schwierig erweisen, wenn Debugging aktiviert ist. Bei Bedarf können Debug-Meldungen an den Syslog-Prozess weitergeleitet und als Syslogs generiert werden. Diese Syslogs können wie jedes andere Syslog an jedes Syslog-Ziel gesendet werden. Um Debug-Meldungen in Syslogs umzuleiten, geben Sie den Befehl **logging debug-trace ein**. Diese Konfiguration sendet die Debug-Ausgabe als Syslogs an einen Syslog-Server.

```
logging trap debugging
logging debug-trace
logging host inside 172.22.1.5
```

Kombinierte Verwendung von Protokollierungsliste und Nachrichtenklassen

Geben Sie den Befehl **logging list** ein, um das Syslog nur für IPsec-VPN-Nachrichten von LAN zu LAN und für Remotezugriff zu erfassen. In diesem Beispiel werden alle Systemprotokollmeldungen der VPN-Klasse (IKE und IPsec) mit Debugging-Ebene oder höher erfasst.

Beispiel

```
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
```

Protokollieren von ACL-Treffern

Fügen Sie jedem gewünschten Zugriffslistenelement (ACE) ein **Protokoll** hinzu, um das Protokoll beim Aufrufen einer Zugriffsliste zu protokollieren. Verwenden Sie diese Syntax:

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

Beispiel

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

ACLs protokollieren standardmäßig jedes abgelehnte Paket. Es ist nicht erforderlich, die Protokolloption hinzuzufügen, um ACLs zu **verweigern**, um Syslogs für abgelehnte Pakete zu generieren. Wenn die **Log**-Option angegeben wird, wird die Syslog-Meldung `106100` für den ACE generiert, auf den sie angewendet wird. Die Syslog-Meldung `106100` wird für jeden passenden "permit"- oder "deny"-ACE-Fluss generiert, der die ASA-Firewall passiert. Der First-Match-Fluss wird zwischengespeichert. Bei nachfolgenden Übereinstimmungen wird die Trefferanzahl erhöht, die im Befehl **show access-list** angezeigt wird. Das standardmäßige Protokollierungsverhalten der Zugriffsliste, bei dem das **log-**Schlüsselwort nicht angegeben wurde, besteht darin, dass bei Ablehnung eines Pakets die Meldung `106023` generiert wird. Wenn ein Paket zulässig ist, wird keine Syslog-Meldung generiert.

Für die generierten Syslog-Meldungen (`106100`) kann eine optionale Syslog-Stufe (0 - 7) angegeben werden. Wenn keine Ebene angegeben ist, ist die Standardebene 6 (informativ) für einen neuen ACE. Wenn der ACE bereits vorhanden ist, bleibt sein aktueller Protokolllevel unverändert. Wenn die Option **log disable** angegeben ist, ist die Zugriffslistenprotokollierung vollständig deaktiviert. Es wird keine Syslog-Meldung mit der Meldung `106023` generiert. Die **Log**-Standardoption stellt das Standardverhalten der Zugriffslistenprotokollierung wieder her.

Führen Sie die folgenden Schritte aus, damit die Syslog-Meldung `106100` in der Konsolenausgabe angezeigt wird:

1. Geben Sie den Befehl **logging enable** ein, um die Übertragung von Systemprotokollmeldungen an alle Ausgabestandorte zu aktivieren. Sie müssen einen Speicherort für die Protokollausgabe festlegen, um alle Protokolle anzeigen zu können.
2. Geben Sie den Befehl **logging message <message_number> level <severity_level> ein**, um den Schweregrad einer bestimmten Systemprotokollmeldung festzulegen.Geben Sie in diesem Fall den Befehl **logging message 106100** ein, um die Meldung `106100` zu aktivieren.
3. Geben Sie **message_list der Protokollierungskonsole ein. | severity_level**-Befehl, damit Systemprotokollmeldungen auf der Konsole der Security Appliance (tty) angezeigt werden, sobald sie auftreten. Legen Sie den `Schweregrad` von 1 auf 7 fest, oder verwenden Sie den Ebenennamen. Sie können auch angeben, welche Nachrichten mit der Variablen `message_list` gesendet werden.
4. Geben Sie den Befehl **show logging message (Protokollnachricht anzeigen)** ein, um eine Liste der von der Standardeinstellung geänderten Systemprotokollnachrichten anzuzeigen. Dabei handelt es sich um Nachrichten, denen ein anderer Schweregrad zugewiesen wurde, und um Nachrichten, die deaktiviert wurden.Dies ist eine Beispielausgabe des Befehls **show logging message**:
   ```
   ASAfirewall#show logging message 106100
   syslog 106100: default-level informational (enabled)
   ASAfirewall# %ASA-7-111009: User 'enable_15' executed cmd: show logging mess 106
   ```

```
100
```

Blockierung der Syslog-Generierung auf Standby-ASA

Ab Version 9.4.1 der ASA-Software können Sie verhindern, dass bestimmte Syslogs auf einem Standby-Gerät generiert werden. Verwenden Sie hierzu command:

```
no logging message syslog-id standby
```

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Wenn Sie eine bestimmte Syslog-Meldung unterdrücken möchten, die an den Syslog-Server gesendet werden soll, müssen Sie den Befehl wie folgt eingeben.

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

Weitere Informationen finden Sie im Befehl logging message (Protokollierungsmeldung).

%ASA-3-201008: Deaktivieren neuer Verbindungen

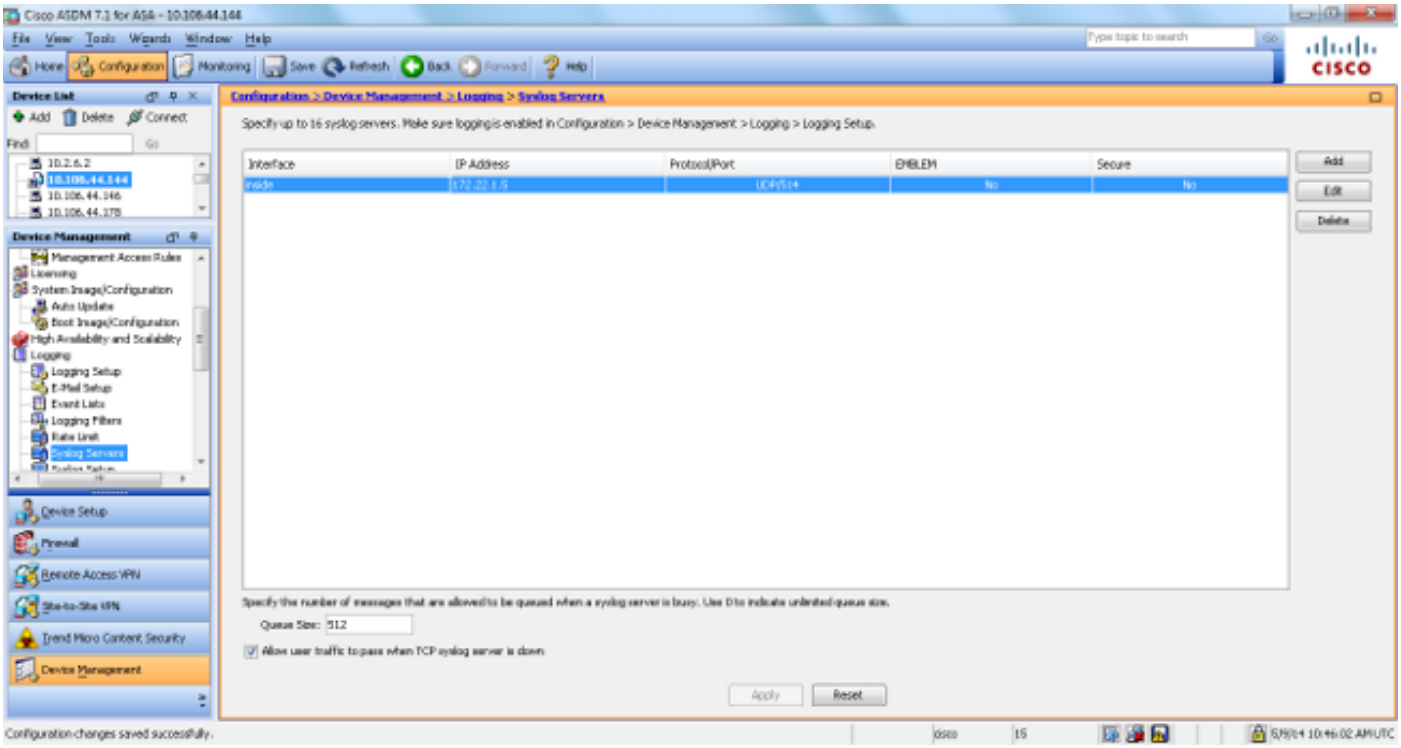
%ASA-3-201008: Keine neuen Verbindungen zulassen. Die Fehlermeldung wird angezeigt, wenn ein ASA keine Verbindung zum Syslog-Server herstellen kann und keine neuen Verbindungen zulässig sind.

Lösung

Diese Meldung wird angezeigt, wenn Sie die TCP-Systemprotokollmeldung aktiviert haben und der Syslog-Server nicht erreichbar ist oder wenn Sie Cisco ASA Syslog Server (PFSS) verwenden und der Datenträger auf dem Windows NT-System voll ist. Gehen Sie wie folgt vor, um diese Fehlermeldung zu beheben:

- Deaktivieren Sie die TCP-Systemprotokollmeldung, wenn diese aktiviert ist.
- Wenn Sie PFSS verwenden, geben Sie Speicherplatz auf dem Windows NT-System frei, auf dem sich PFSS befindet.
- Stellen Sie sicher, dass der Syslog-Server aktiv ist, und Sie können den Host von der Cisco ASA-Konsole aus pingen.
- Starten Sie die Protokollierung von TCP-Systemmeldungen neu, um Datenverkehr zuzulassen.

Wenn der Syslog-Server ausfällt und die TCP-Protokollierung konfiguriert ist, verwenden Sie entweder den Befehl logging permit-hostdown oder wechseln Sie zur UDP-Protokollierung.



Zugehörige Informationen

- Cisco Secure PIX Firewall - Befehlsreferenzen
- Request For Comments (RFCs)
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.