ASA(Adaptive Security Appliance) Syslog 구성

목차

소개

이 문서에서는 코드 버전 8.4 이상을 실행하는 ASA에서 다양한 로깅 옵션을 구성하는 방법을 보여

주는 샘플 컨피그레이션에 대해 설명합니다.

배경 정보

ASA 버전 8.4에서는 특정 syslog 메시지만 표시되도록 매우 세분화된 필터링 기술을 도입했습니다. 이 문서의 기본 Syslog 섹션에서는 일반적인 syslog 컨피그레이션을 보여줍니다. 이 문서의 고급 Syslog 섹션에는 버전 8.4의 새로운 syslog 기능이 나와 있습니다. 전체 시스템 로그 메시지 가이드는 Cisco Security Appliance 시스템 로그 메시지 가이드를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASA 5515 with ASA Software 버전 8.4
- Cisco ASDM(Adaptive Security Device Manager) 버전 7.1.6

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

참고: ASDM 버전 7.1 이상의 유사한 컨피그레이션 세부사항에 대한 자세한 내용은 ASA 8.2: Configure Syslog using ASDM을 참조하십시오.

기본 시스템 로그

로깅을 활성화하고 로그를 보고 컨피그레이션 설정을 보려면 다음 명령을 입력합니다.

- logging enable - syslog 메시지를 모든 출력 위치로 전송할 수 있습니다.
- no logging enable - 모든 출력 위치에 대한 로깅을 비활성화합니다.
- show logging - syslog 버퍼의 내용과 현재 컨피그레이션과 관련된 정보 및 통계를 나열합니다 .

ASA는 syslog 메시지를 다양한 대상으로 전송할 수 있습니다. syslog 정보를 전송할 위치를 지정하려면 다음 섹션에 명령을 입력합니다.

내부 버퍼에 로깅 정보 보내기

<#root>

logging buffered

 severity_level

ASA 내부 버퍼에 syslog 메시지를 저장할 때 외부 소프트웨어 또는 하드웨어가 필요하지 않습니다. 저장된 syslog 메시지를 보려면 show logging 명령을 입력합니다. 내부 버퍼의 최대 크기는 1MB입니다(logging buffer-size 명령으로 구성 가능). 그 결과, 그것은 매우 빠르게 포장할 수 있습니다. 더 자세한 로깅 수준이 내부 버퍼를 빠르게 채우고 래핑할 수 있으므로 내부 버퍼에 대한 로깅 수준을 선택할 때 이 점에 유의하십시오.

Syslog 서버에 로깅 정보 전송

<#root>

logging host

 interface_name ip_address [tcp[/port] | udp[/port]] [format emblem]

logging trap

 severity_level

logging facility

 number

syslog 메시지를 외부 호스트로 전송하려면 syslog 애플리케이션을 실행하는 서버가 필요합니다. ASA는 기본적으로 UDP 포트 514에서 syslog를 전송하지만, 프로토콜과 포트를 선택할 수 있습니다. TCP가 로깅 프로토콜로 선택된 경우, ASA는 TCP 연결을 통해 syslog를 syslog 서버로 전송합니다. 서버에 액세스할 수 없거나 서버에 대한 TCP 연결을 설정할 수 없는 경우 ASA는 기본적으로 모든 새 연결을 차단합니다. logging permit-hostdown을 활성화하면 이 동작을 비활성화할 수 있습니다. logging permit-hostdown 명령에 대한 자세한 내용은 컨피그레이션 가이드를 참조하십시오.

참고: ASA는 다음 범위의 포트만 허용합니다. 1025-65535 . 다른 포트를 사용하면 다음 오류가 발생합니다.
ciscoasa (config) # logging host tftp 192.168.1.1 udp/516
경고: 인터페이스 Ethernet0/1 보안 레벨은 0입니다.
오류: 포트 '516'이(가) 1025-65535 범위에 있지 않습니다.

로깅 정보를 전자 메일로 보내기

<#root>

logging mail

 severity_level

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

SMTP 서버는 syslog 메시지를 이메일로 전송할 때 필요합니다. ASA에서 지정된 이메일 클라이언트로 이메일을 성공적으로 릴레이하려면 SMTP 서버에 대한 올바른 컨피그레이션이 필요합니다. 이 로깅 수준을 디버그 또는 정보 등 매우 자세한 수준으로 설정하면, 이 로깅 컨피그레이션에서 보낸 각 이메일의 결과로 최대 4개 이상의 추가 로그가 생성되므로 상당한 수의 syslog를 생성할 수 있습니다.

직렬 콘솔에 로깅 정보 보내기

```
<#root>
logging console
 severity_level
```

콘솔 로깅을 사용하면 syslog 메시지가 발생했을 때 ASA 콘솔(tty)에 표시될 수 있습니다. 콘솔 로깅이 구성된 경우 ASA의 모든 로그 생성은 ASA 직렬 콘솔의 속도인 9800bps로 제한됩니다. 이로 인해 syslog가 내부 버퍼를 포함하는 모든 대상으로 삭제될 수 있습니다. 이러한 이유로 자세한 syslog에 대한 콘솔 로깅을 사용하지 마십시오.

텔넷/SSH 세션에 로깅 정보 보내기

```
<#root>
logging monitor
 severity_level
terminal monitor
```

로깅 모니터를 사용하면 텔넷 또는 SSH를 사용하여 ASA 콘솔에 액세스하고 해당 세션에서 명령 터미널 모니터를 실행할 때 syslog 메시지가 표시될 수 있습니다. 세션에 대한 로그 인쇄를 중지하려면 terminal no monitor 명령을 입력합니다.

ASDM에 로그 메시지 표시

<#root>

logging asdm

 severity_level

ASDM에는 syslog 메시지를 저장하는 데 사용할 수 있는 버퍼도 있습니다. ASDM syslog 버퍼의 내용을 표시하려면 show logging asdm 명령을 입력합니다.

SNMP 관리 스테이션에 로그 전송

<#root>

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

사용자는 SNMP와 함께 syslog 메시지를 전송하려면 기존의 기능인 SNMP(Simple Network Management Protocol) 환경이 필요합니다. 출력 대상을 설정 및 관리하는 데 사용할 수 있는 명령에 대한 자세한 내용은 출력 대상 설정 및 관리 명령을 참조하십시오. 심각도 수준별로 나열된 메시지는 심각도 수준별로 나열된 메시지를 참조하십시오.

Syslog에 타임스탬프 추가

이벤트를 정렬하고 정렬하기 위해 syslog에 타임스탬프를 추가할 수 있습니다. 시간을 기준으로 문제를 추적하려면 이 옵션을 사용하는 것이 좋습니다. 타임스탬프를 활성화하려면 logging timestamp 명령을 입력합니다. 다음은 두 가지 syslog 예입니다. 하나는 타임스탬프가 없고 다른 하나는 다음과 같습니다.

```
%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
```

예 1

이 출력은 디버깅 심각도 수준으로 버퍼에 로그인하기 위한 샘플 컨피그레이션을 보여줍니다.

<#root>

```
logging enable
logging buffered debugging
```

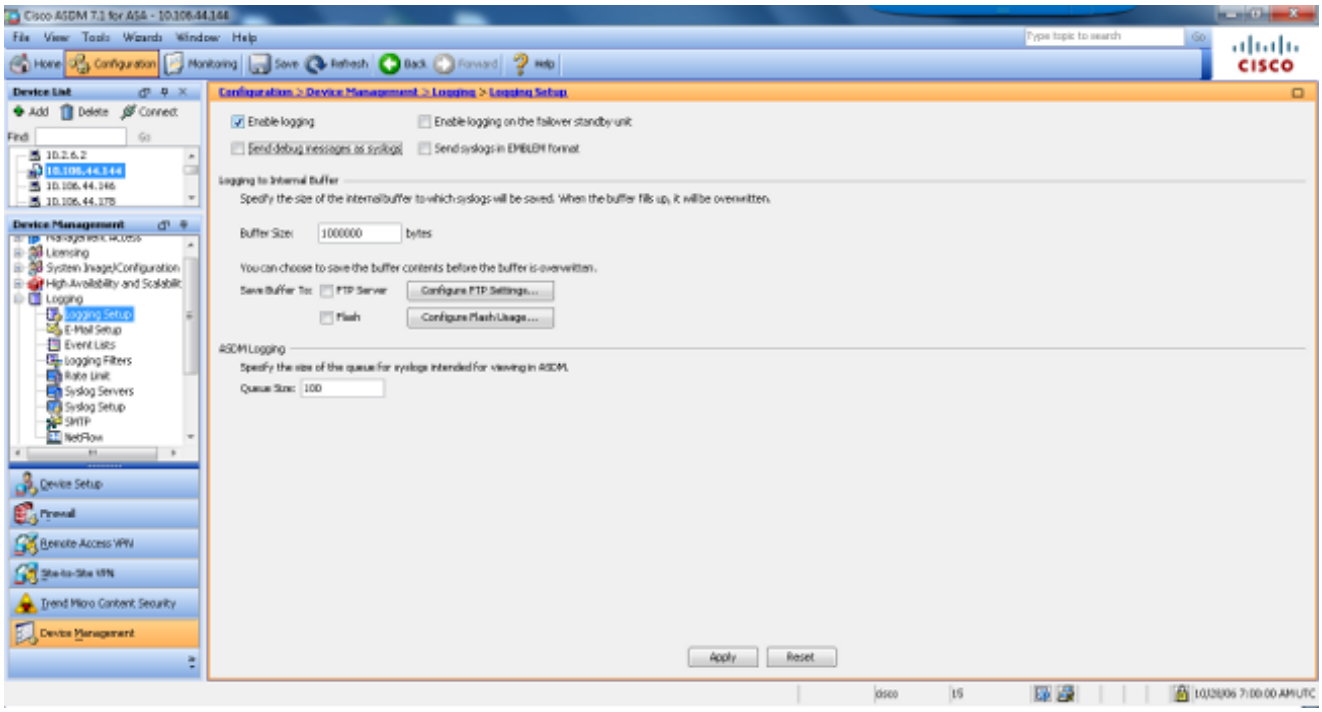
샘플 출력입니다.

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

ASDM으로 기본 Syslog 구성

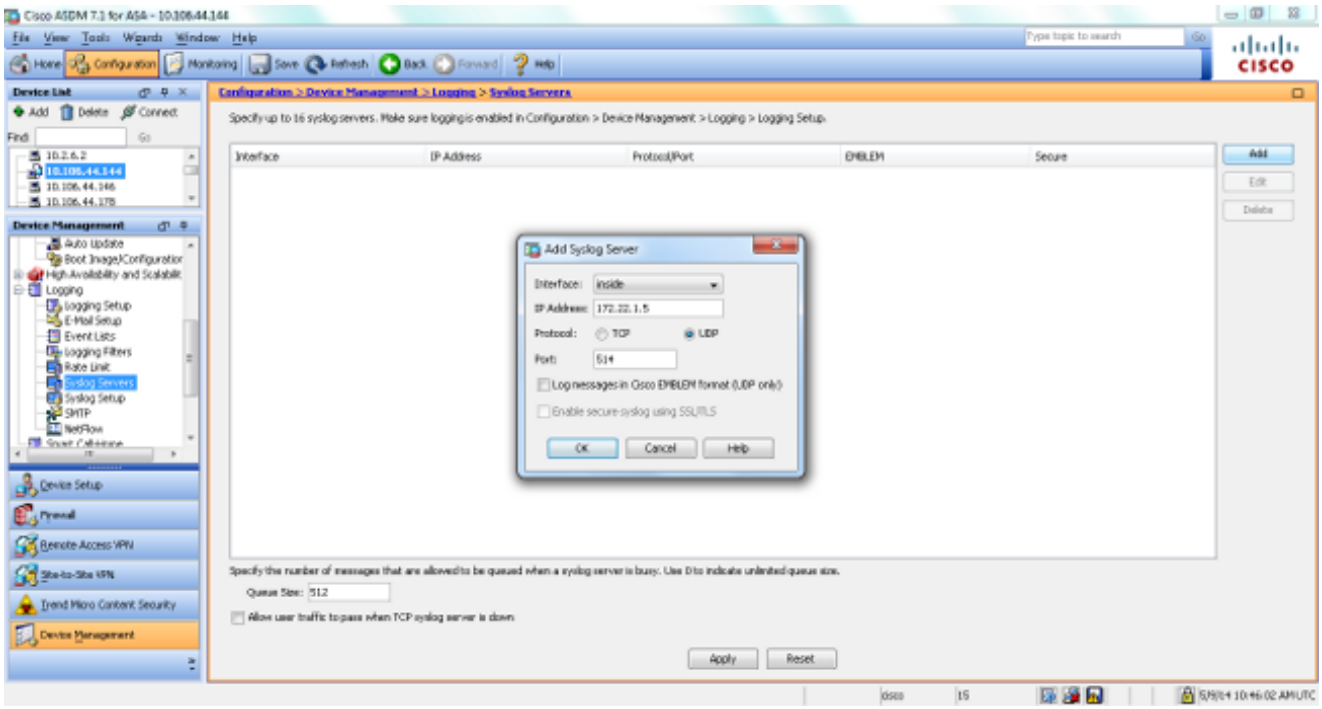
이 절차에서는 사용 가능한 모든 syslog 대상에 대한 ASDM 컨피그레이션을 보여줍니다.

1. ASA에서 로깅을 활성화하려면 먼저 기본 로깅 매개변수를 구성합니다. Configuration > Features > Properties > Logging > Logging Setup을 선택합니다. syslog를 활성화하려면 Enable logging 확인란을 선택합니다.

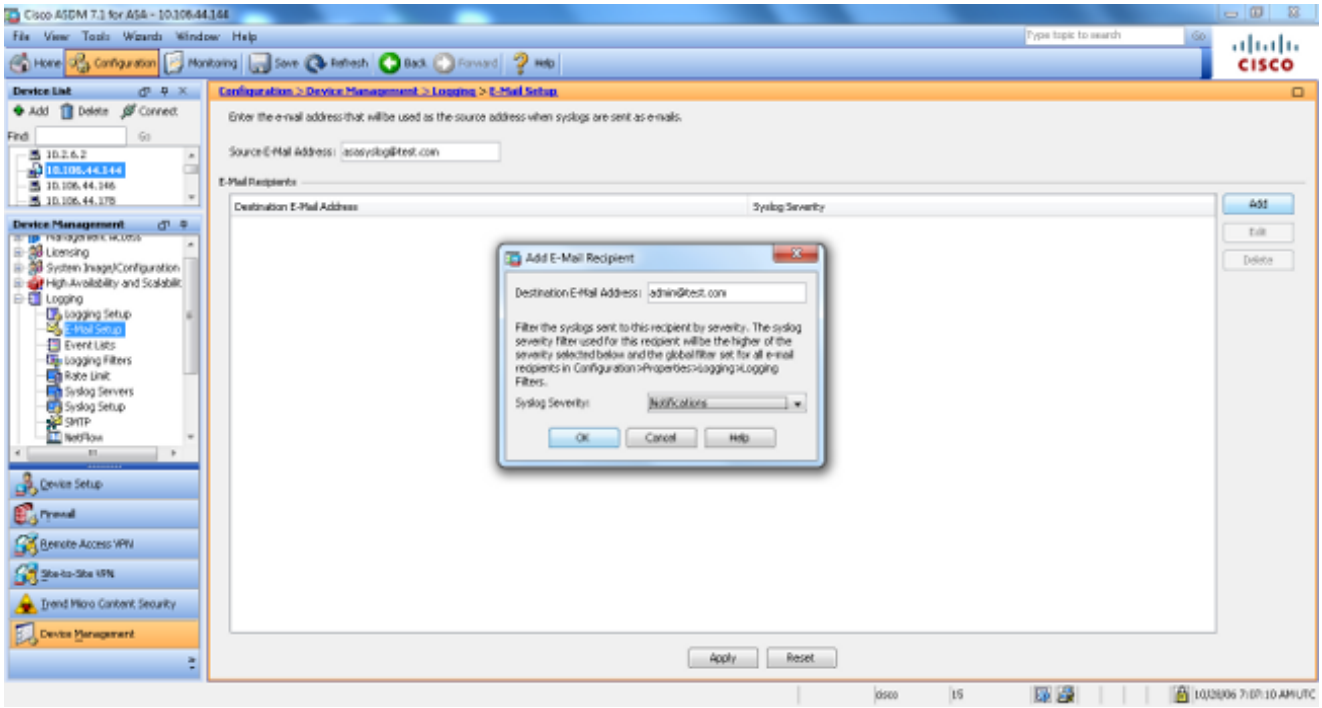


2. 외부 서버를 syslog의 대상으로 구성하려면 Logging(로깅)에서 Syslog Servers(Syslog 서버

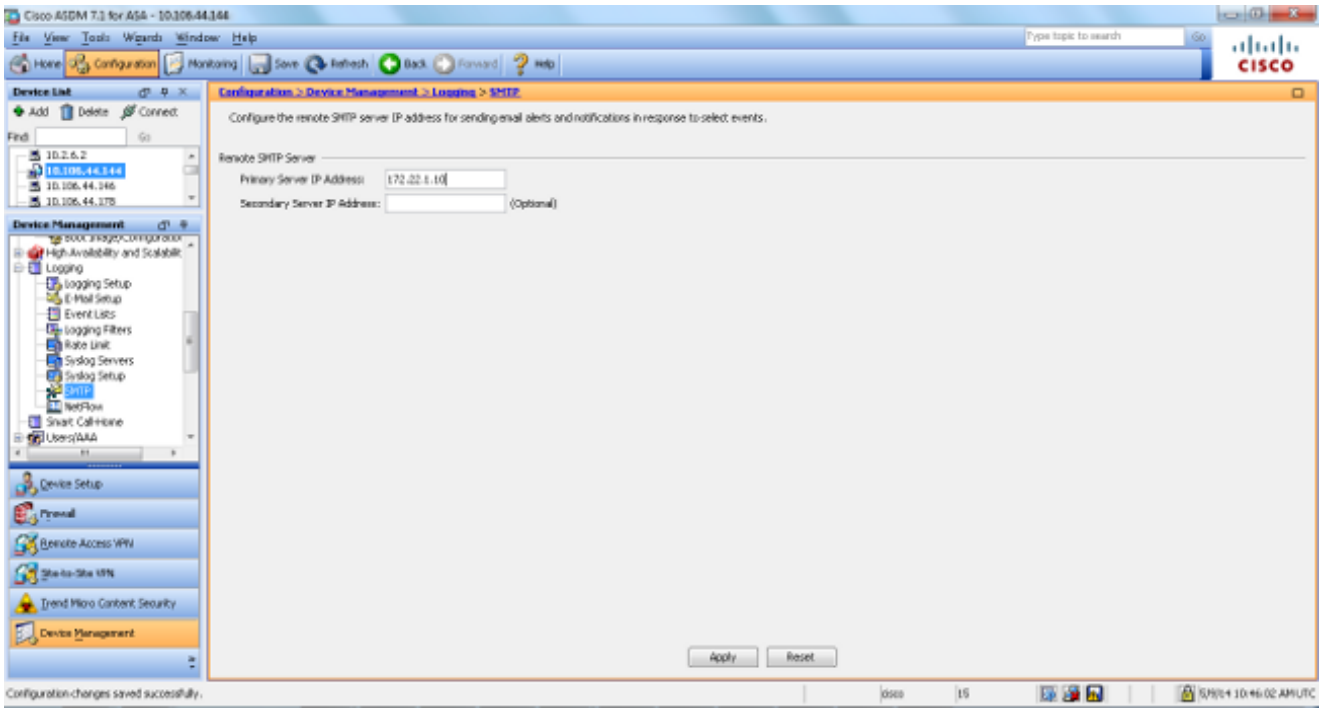
)를 선택하고 Add(추가)를 클릭하여 syslog 서버를 추가합니다. Add Syslog Server(Syslog 서버 추가) 상자에 syslog 서버 세부 정보를 입력하고 완료되면 OK(확인)를 선택합니다.



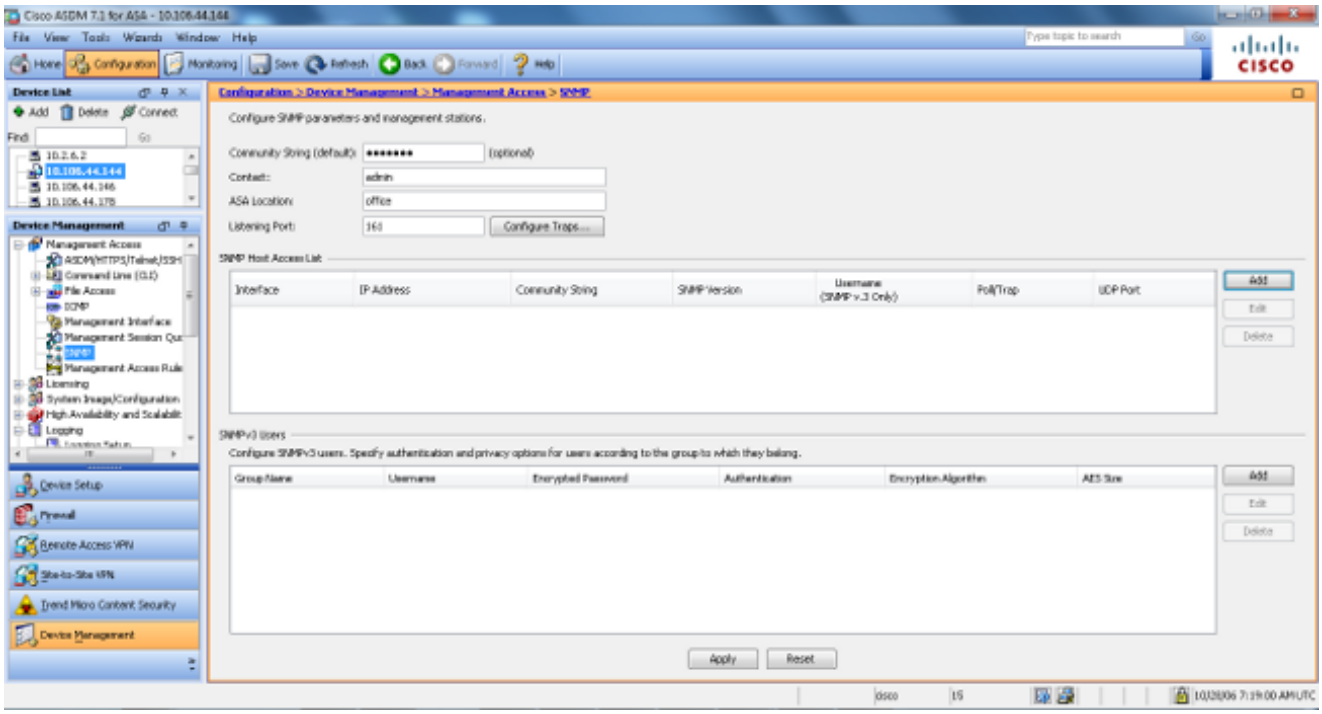
3. syslog 메시지를 특정 수신자에게 이메일로 보내려면 Logging(로깅)에서 E-Mail Setup(이메일 설정)을 선택합니다. 전자 메일 수신자의 대상 전자 메일 주소와 메시지 심각도 수준을 구성하려면 Source E-Mail Address(소스 전자 메일 주소) 상자에서 소스 전자 메일 주소를 지정하고 Add(추가)를 선택합니다. 완료되면 OK(확인)를 클릭합니다.



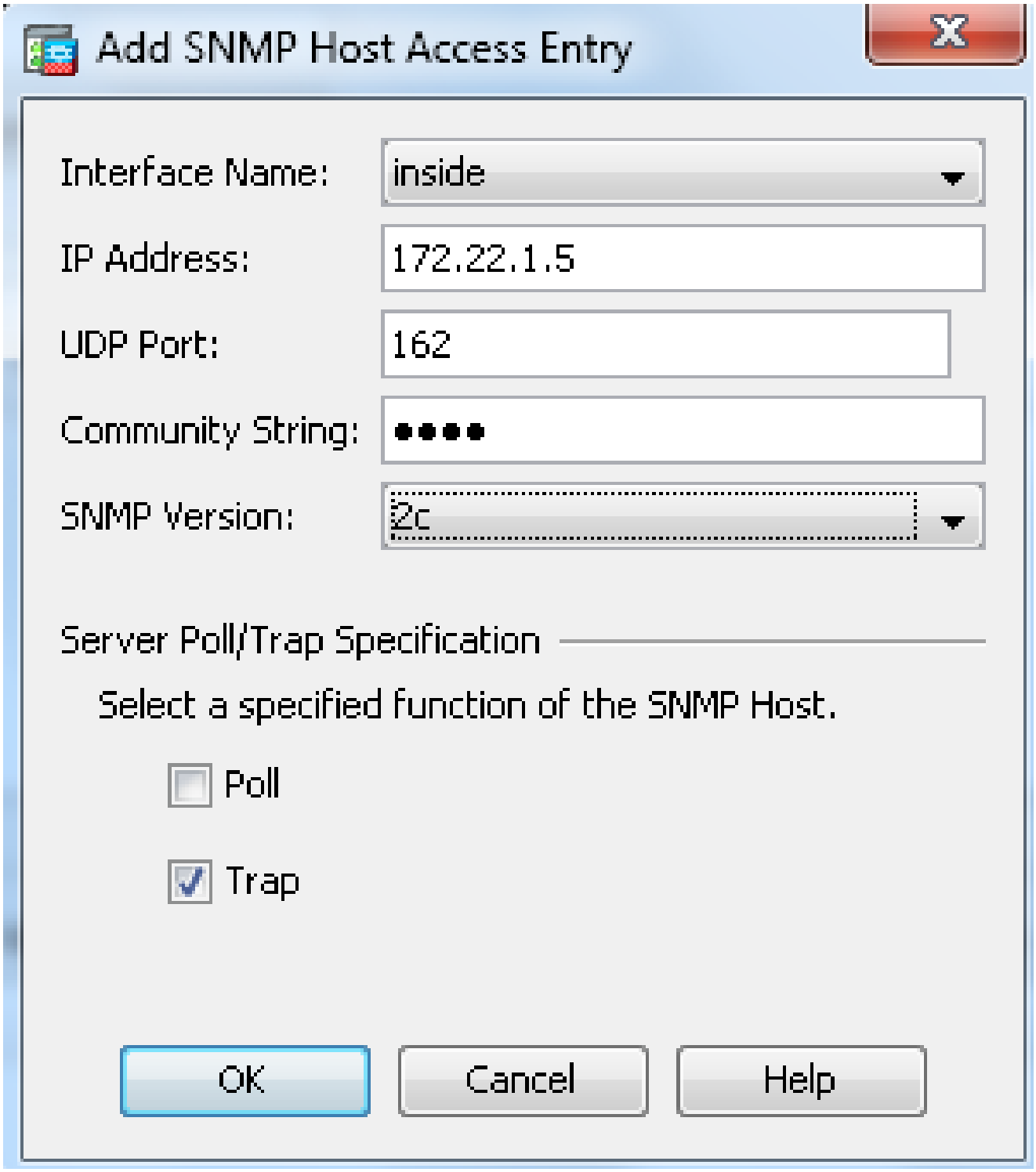
4. Device Administration, Logging을 선택하고 SMTP를 선택한 다음 Primary Server IP Address를 입력하여 SMTP 서버 IP 주소를 지정합니다.



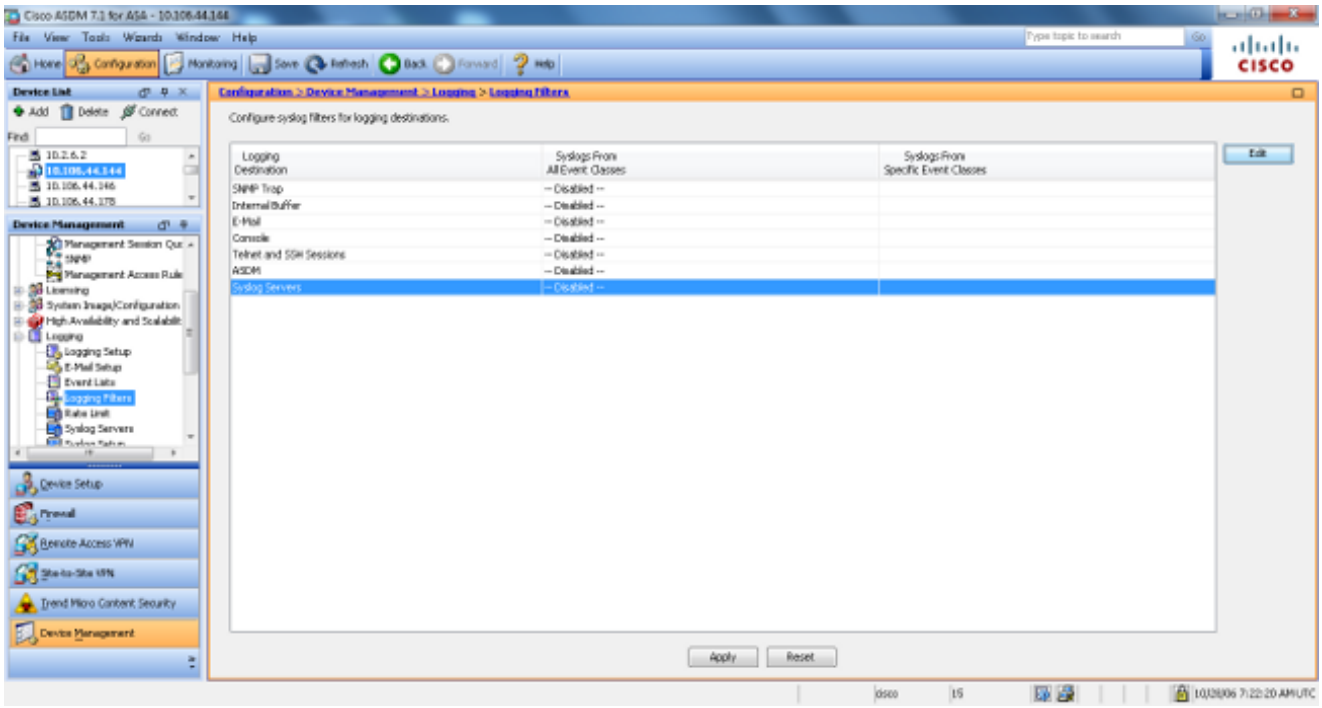
5. syslog를 SNMP 트랩으로 전송하려면 먼저 SNMP 서버를 정의해야 합니다. SNMP 관리 스테이션의 주소와 특정 속성을 지정하려면 Management Access 메뉴에서 SNMP를 선택합니다.



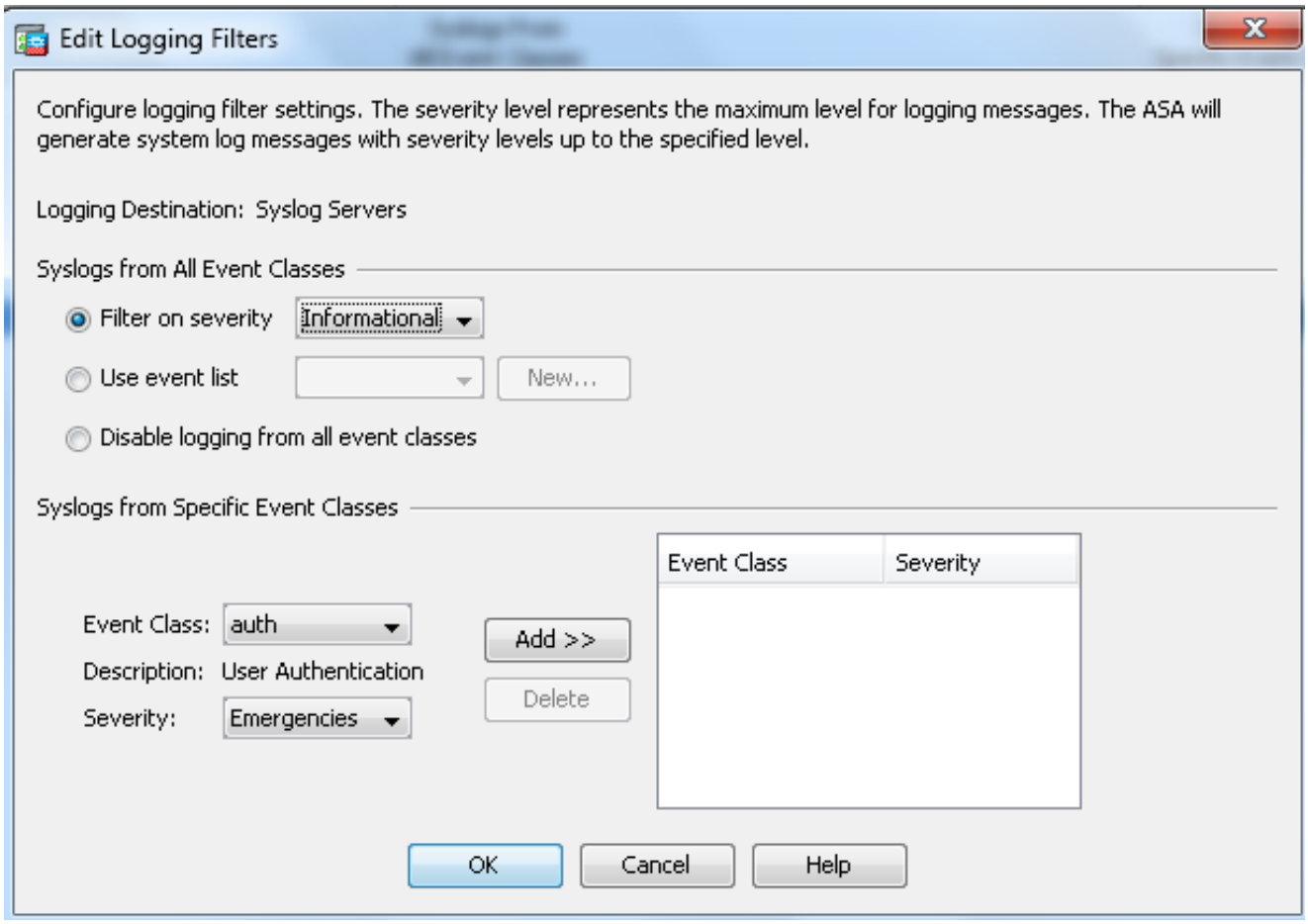
6. SNMP 관리 스테이션을 추가하려면 Add(추가)를 선택합니다. SNMP 호스트 세부 정보를 입력하고 OK(확인)를 클릭합니다.



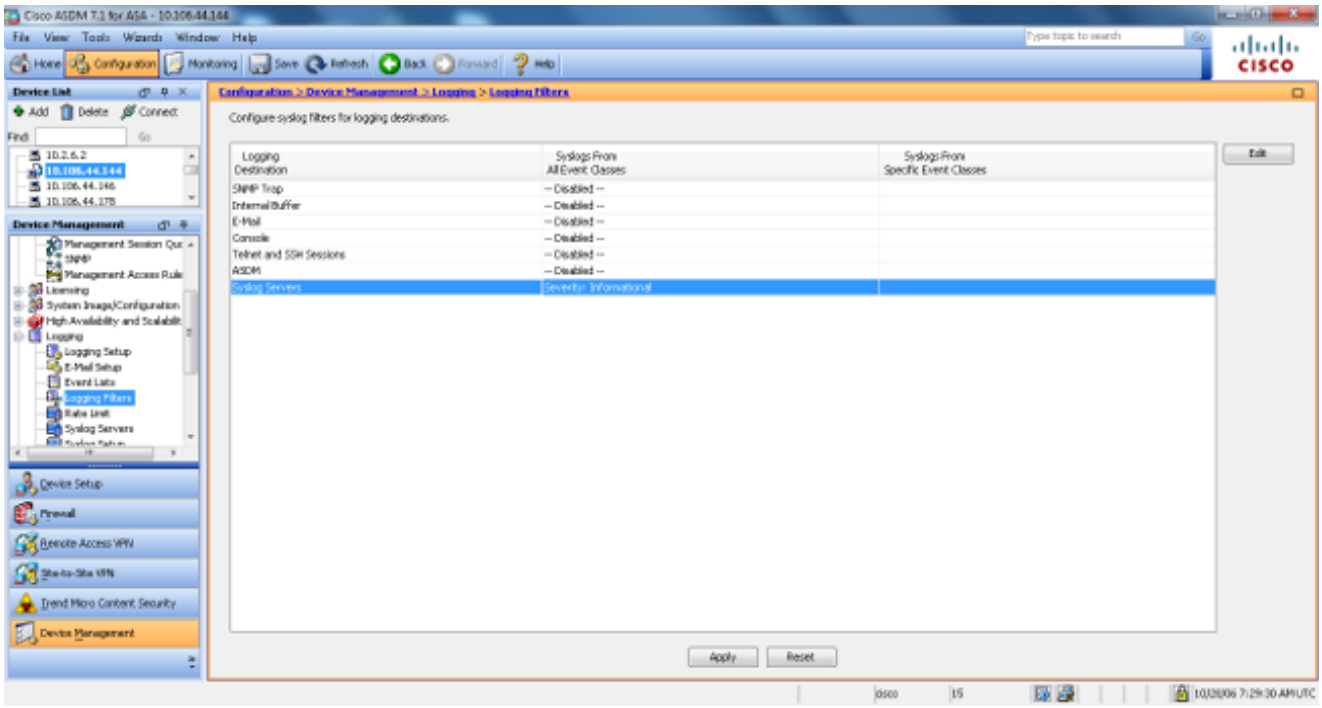
7. 앞서 언급한 대상으로 로그를 보낼 수 있게 하려면 로깅 섹션에서 로깅 필터를 선택합니다. 그러면 각각의 가능한 로깅 대상 및 해당 대상으로 전송된 로그의 현재 레벨이 표시됩니다. 원하는 Logging Destination(로깅 대상)을 선택하고 Edit(편집)를 클릭합니다. 이 예에서는 'Syslog 서버' 대상이 수정됩니다.



8. Filter on severity 드롭다운 목록에서 적절한 심각도(이 경우 Informational)를 선택합니다. 완료되면 OK(확인)를 클릭합니다.



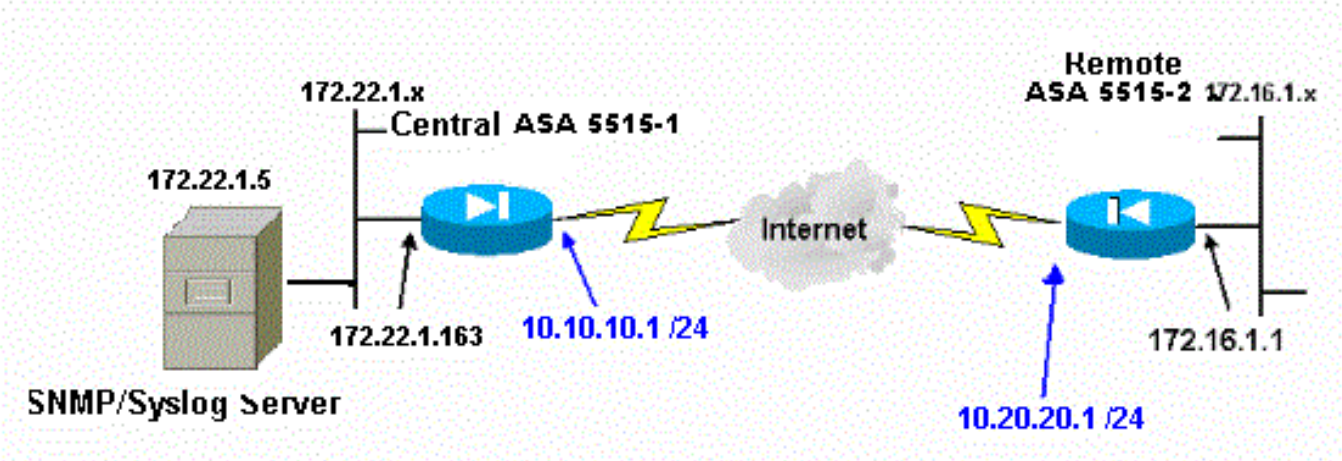
9. Logging Filters 창으로 돌아간 후 Apply를 클릭합니다.



VPN을 통해 Syslog 메시지를 Syslog 서버로 전송

관리자는 간단한 Site-to-Site VPN 설계 또는 좀 더 복잡한 Hub-and-Spoke 설계에서 중앙 사이트에 있는 SNMP 서버 및 syslog 서버를 사용하여 모든 원격 ASA 방화벽을 모니터링할 수 있습니다.

Site-to-Site IPsec VPN 컨피그레이션을 구성하려면 PIX/ASA 7.x 이상: PIX-to-PIX VPN 터널 컨피그레이션 예를 참조하십시오. VPN 컨피그레이션 외에도 중앙 사이트와 로컬 사이트 모두에서 syslog 서버에 대한 SNMP 및 관심 트래픽을 구성해야 합니다.



중앙 ASA 컨피그레이션

<#root>

```
!--- 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 *****
```

원격 ASA 컨피그레이션

<#root>

```
!--- 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 *****
```

ASA 버전 8.4 구성 방법에 대한 자세한 내용은 SNMP 및 Syslog Through VPN 터널을 사용하여 Cisco Secure ASA 방화벽 모니터링을 참조하십시오

고급 시스템 로그

ASA 버전 8.4에서는 그룹의 syslog 메시지를 구성하고 관리할 수 있는 몇 가지 메커니즘을 제공합니다. 이러한 메커니즘에는 메시지 심각도 레벨, 메시지 클래스, 메시지 ID 또는 사용자가 생성하는 사용자 지정 메시지 목록이 포함됩니다. 이러한 메커니즘을 사용하면 작은 또는 큰 메시지 그룹에 적용되는 단일 명령을 입력할 수 있습니다. 이 방법으로 syslogs를 설정 할 때, 지정 된 메시지 그룹에서 메시지를 캡처 할 수 있으며 더 이상 동일 한 심각도의 모든 메시지.

메시지 목록 사용

심각도 및 ID별로 관심 있는 syslog 메시지만 그룹에 포함하려면 메시지 목록을 사용하고 이 메시지 목록을 원하는 대상과 연결합니다.

메시지 목록을 구성하려면 다음 단계를 완료하십시오.

1. 로깅 목록 message_list를 입력합니다 | level severity_level [class message_class] 명령을 사용하여 지정된 심각도 수준 또는 메시지 목록을 포함하는 메시지 목록을 생성합니다.
2. 방금 만든 메시지 목록에 추가 메시지를 추가하려면 logging list message _list message syslog_id-syslog_id2 명령을 입력합니다.
3. 생성된 메시지 목록의 대상을 지정하려면 logging destination message_list 명령을 입력합니다.

예 2

메시지 목록을 생성하려면 다음 명령을 입력합니다. 여기에는 611323에 611101 메시지를 추가하는 모든 심각도 2(위험) 메시지가 포함되어 있으며, 콘솔로 전송되도록 할 수 있습니다.

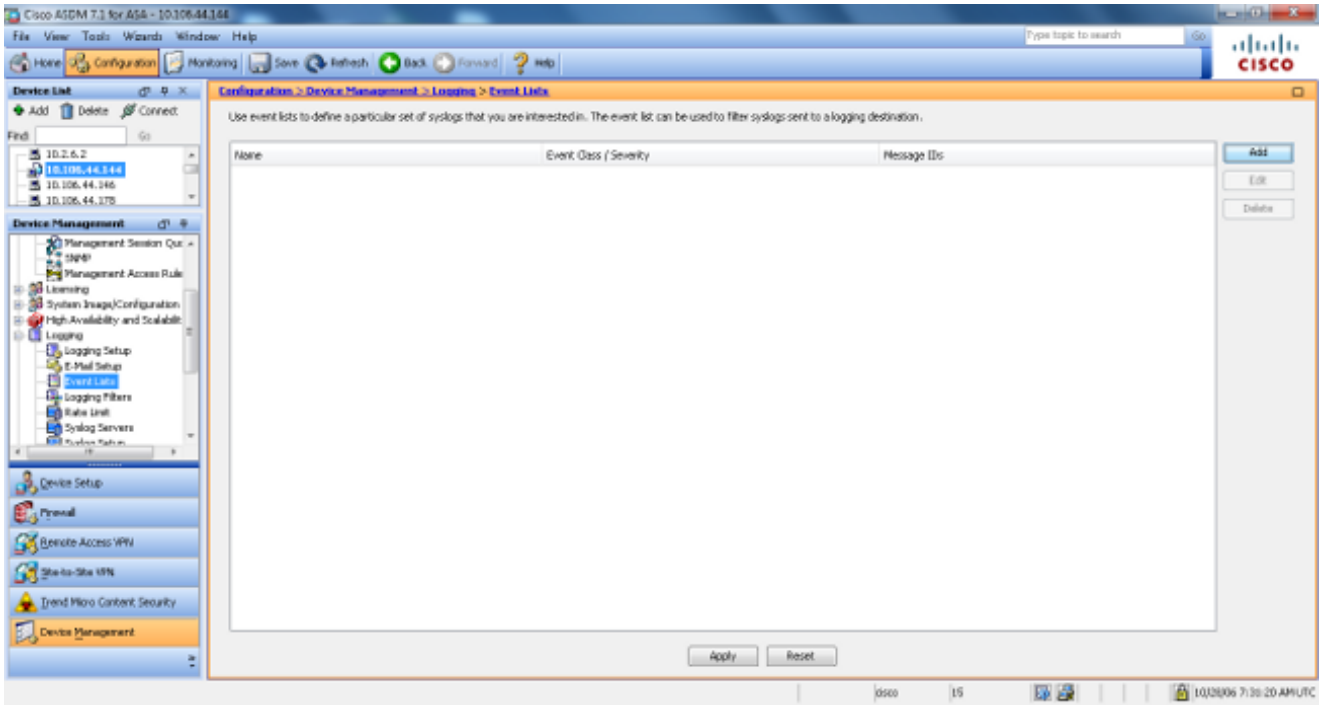
<#root>

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

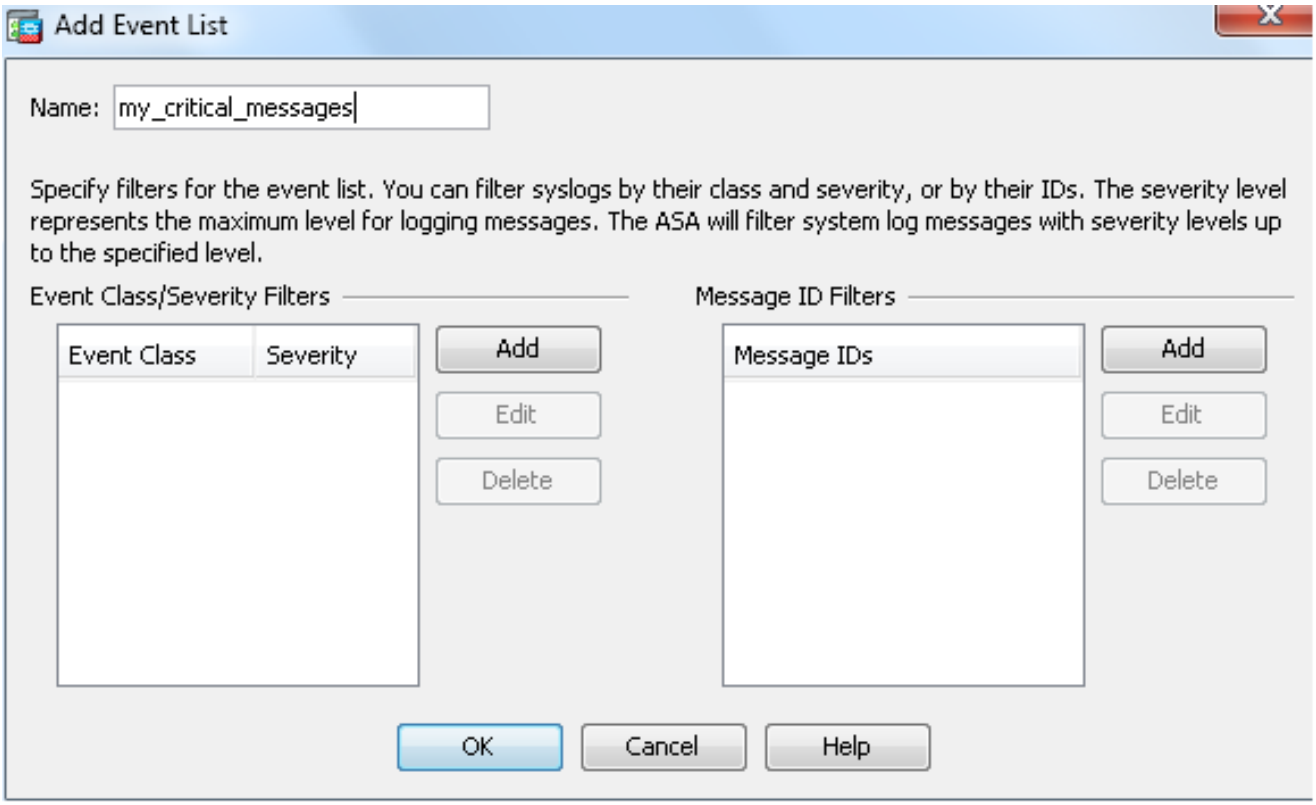
ASDM 컨피그레이션

이 절차에서는 메시지 목록을 사용한 예 2의 ASDM 컨피그레이션을 보여줍니다.

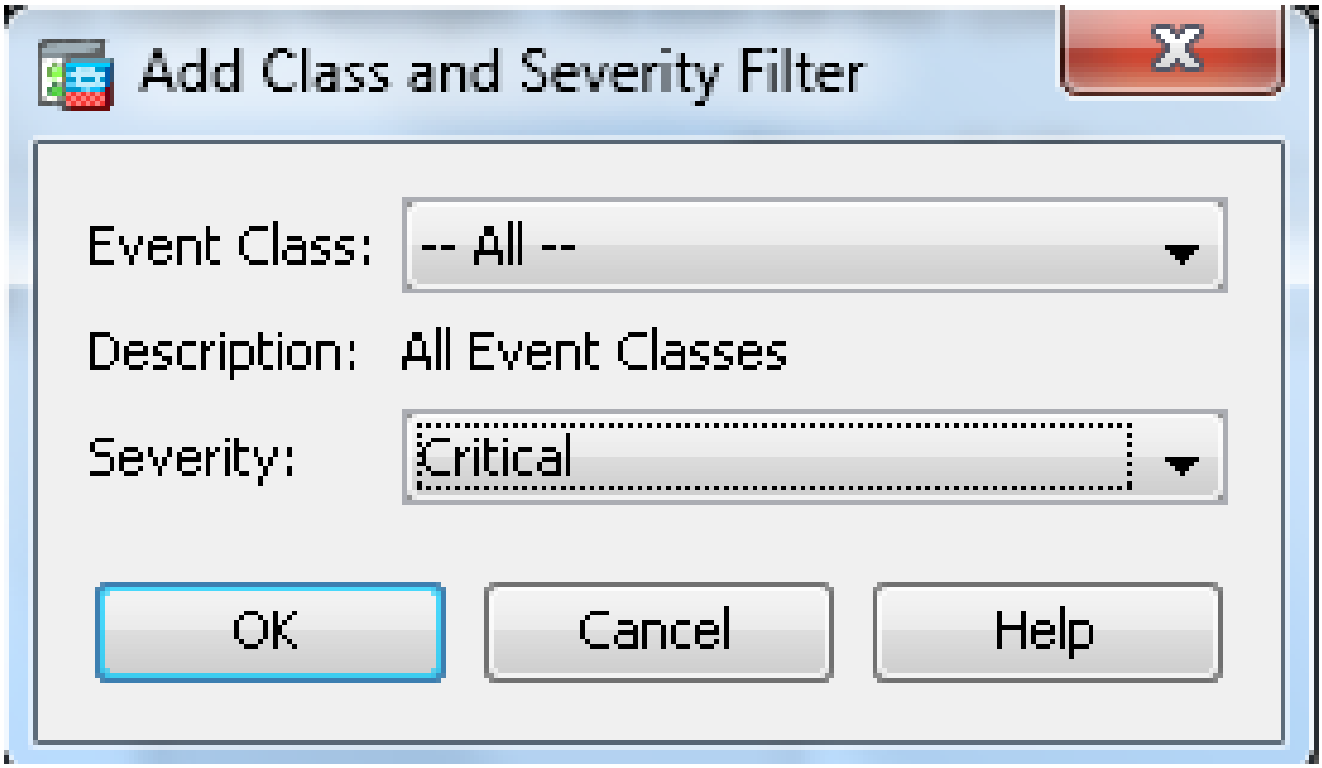
1. 메시지 목록을 만들려면 Logging 아래에서 Event Lists를 선택하고 Add를 클릭합니다.



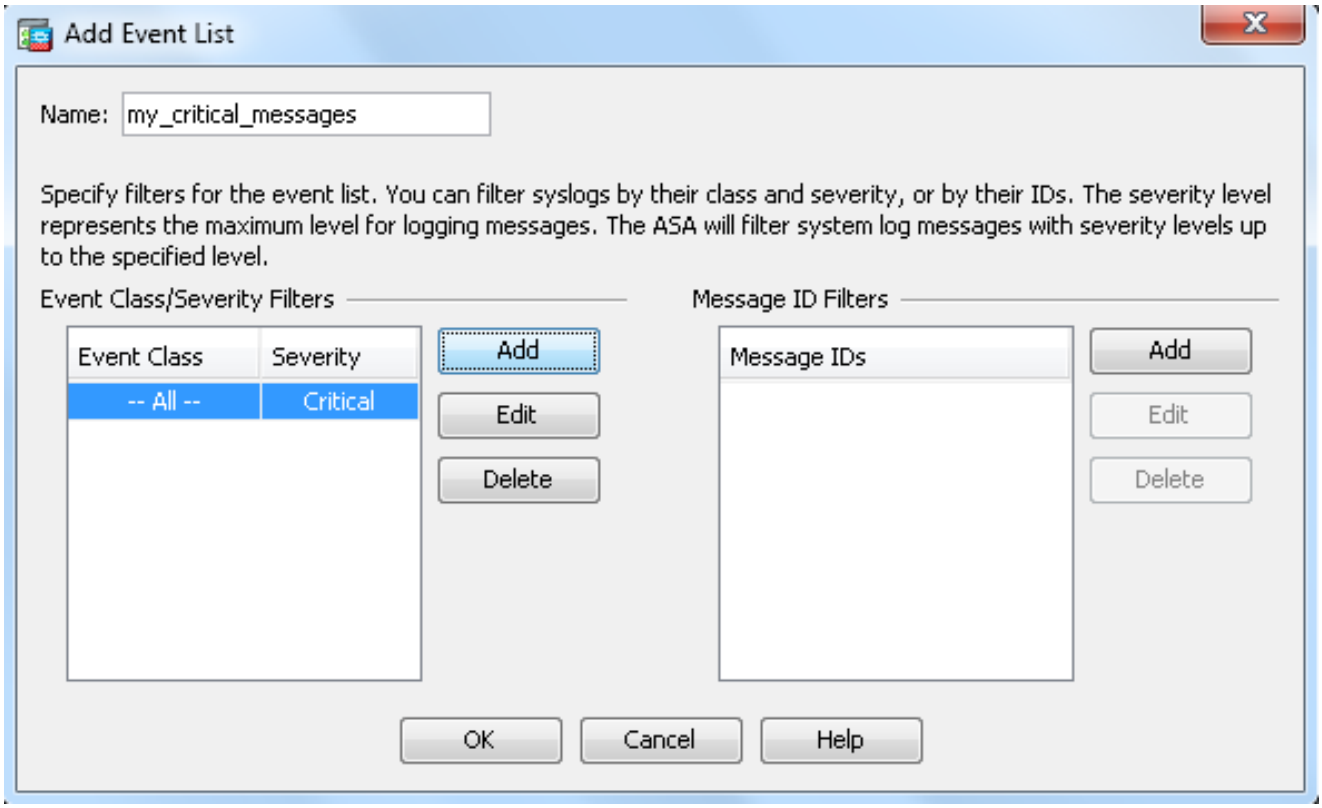
2. Name(이름) 상자에 메시지 목록의 이름을 입력합니다. 이 경우 my_critical_messages가 사용됩니다. Event Class/Severity Filters(이벤트 클래스/심각도 필터)에서 Add(추가)를 클릭합니다.



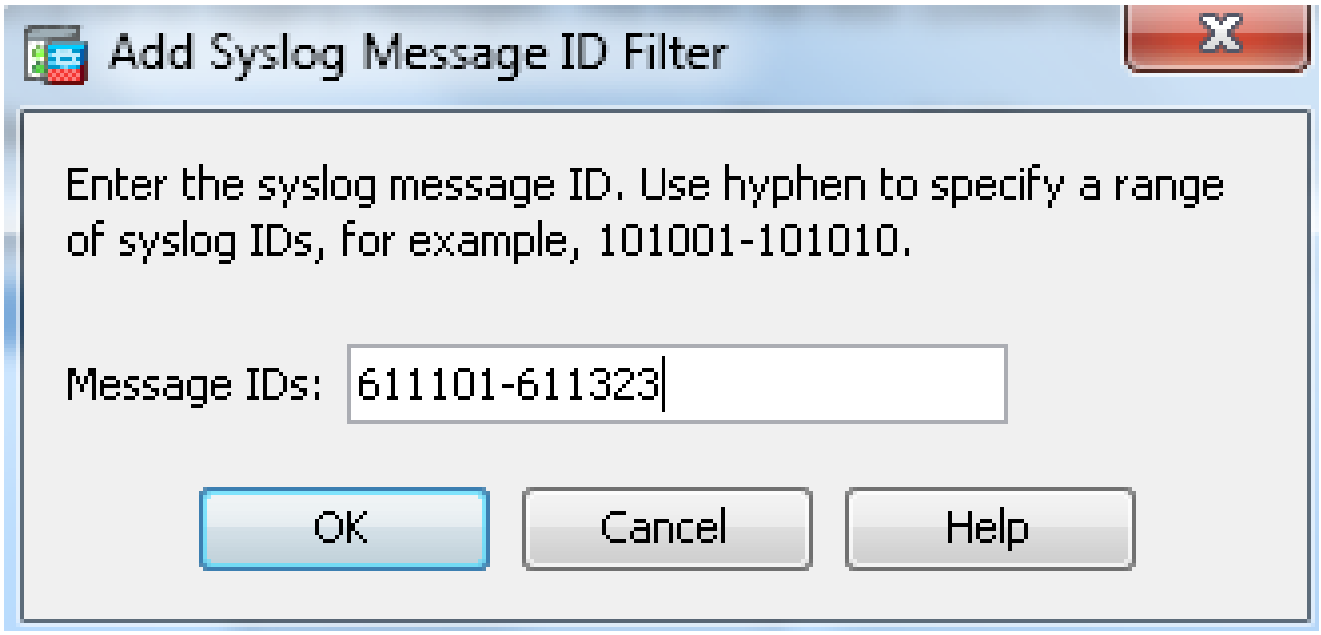
3. Event Class 드롭다운 목록에서 All을 선택합니다. Severity 드롭다운 목록에서 Critical을 선택합니다. 완료되면 OK(확인)를 클릭합니다.



4. 추가 메시지가 필요한 경우 Message ID Filters(메시지 ID 필터) 아래에서 Add(추가)를 클릭합니다. 이 경우 ID가 611101-611323인 메시지를 입력해야 합니다.

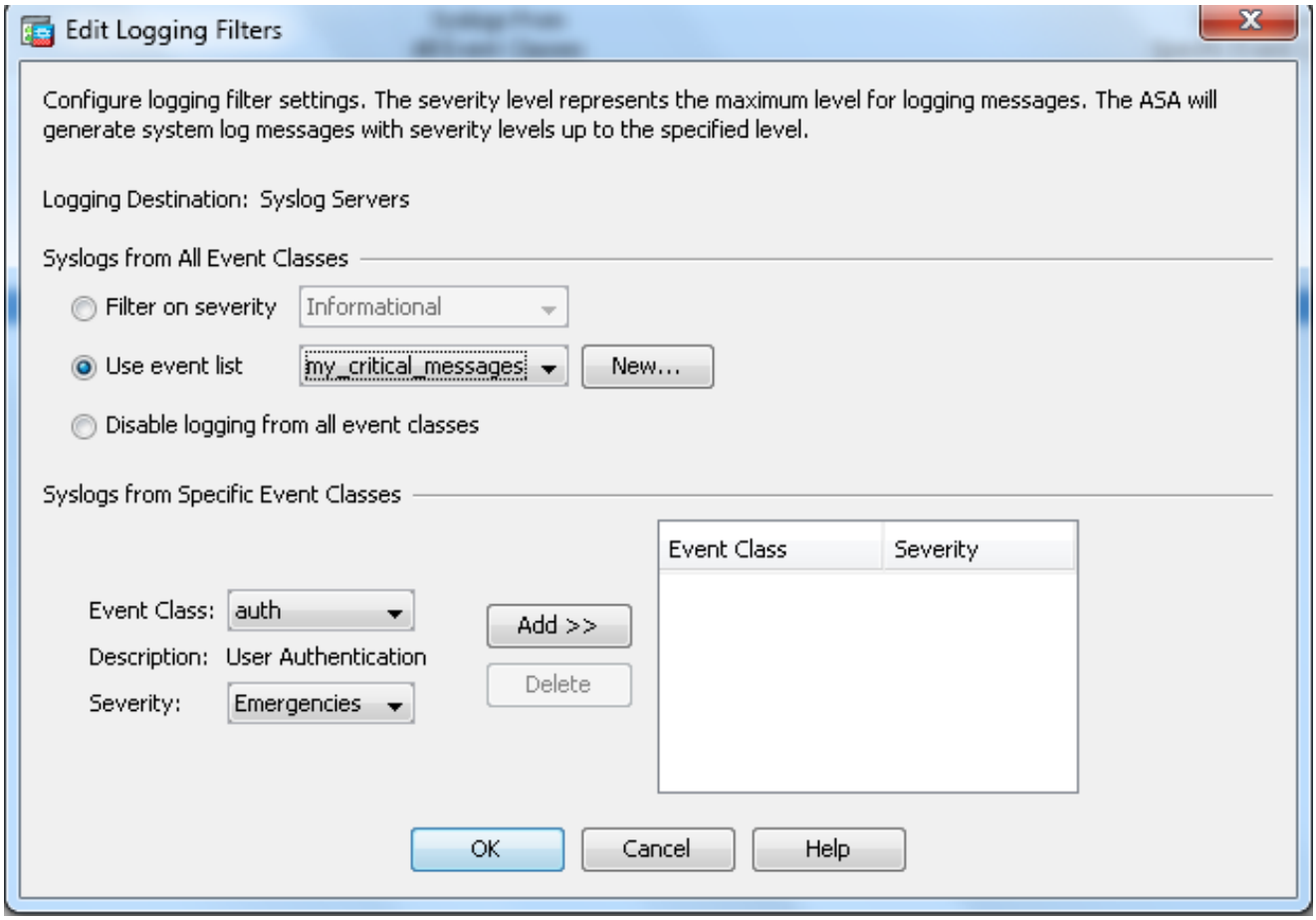


5. Message IDs(메시지 ID) 상자에 ID 범위를 입력하고 OK(확인)를 클릭합니다.

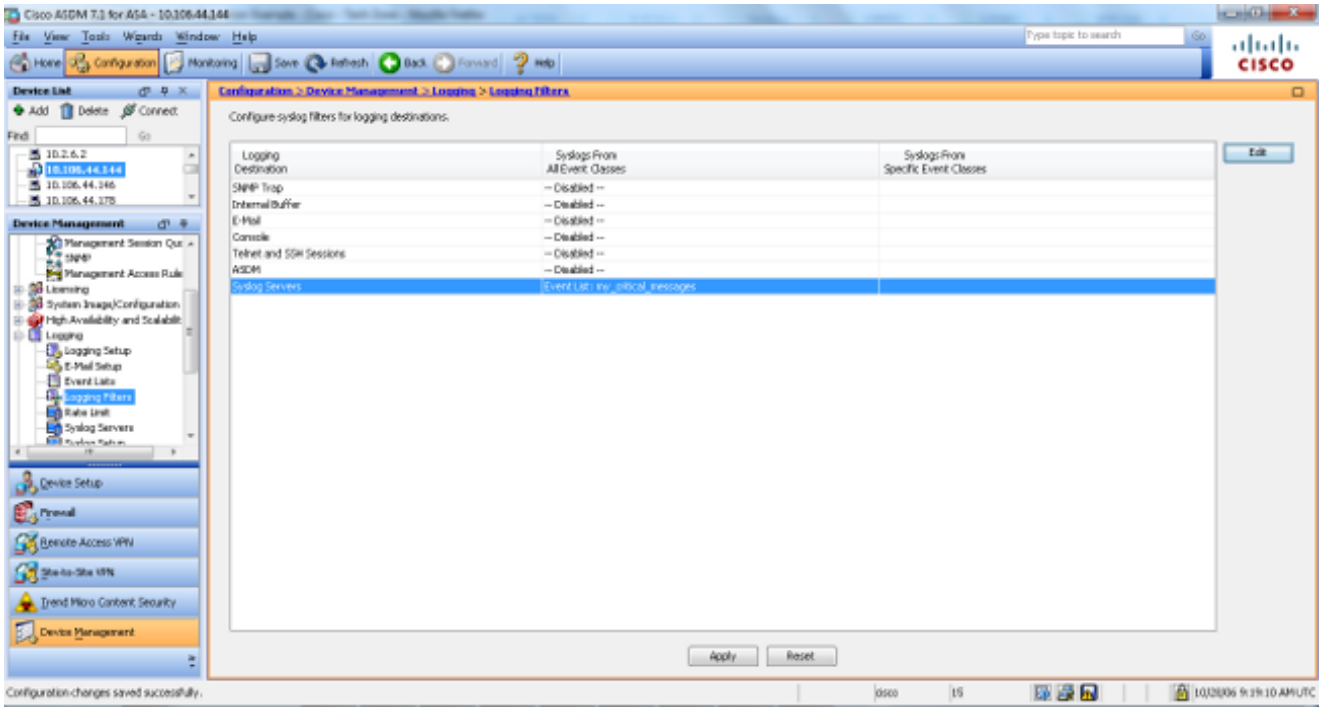


6. Logging Filters(로깅 필터) 메뉴로 돌아가 Console(콘솔)을 대상으로 선택합니다.

7. Use event list 드롭다운 목록에서 my_critical_messages를 선택합니다. 완료되면 OK(확인)를 클릭합니다.



8. Logging Filters 창으로 돌아간 후 Apply를 클릭합니다.



그러면 예 2에 나와 있는 것처럼 메시지 목록을 사용하여 ASDM 컨피그레이션이 완료됩니다.

메시지 클래스 사용

클래스와 연결된 모든 메시지를 지정된 출력 위치로 보내려면 message 클래스를 사용합니다. 심각

도 수준 임계값을 지정할 때 출력 위치로 전송되는 메시지 수를 제한할 수 있습니다.

```
<#root>

logging class

 message_class destination | severity_level
```

예 3

심각도 수준이 긴급 이상인 모든 ca 클래스 메시지를 콘솔로 전송하려면 이 명령을 입력합니다.

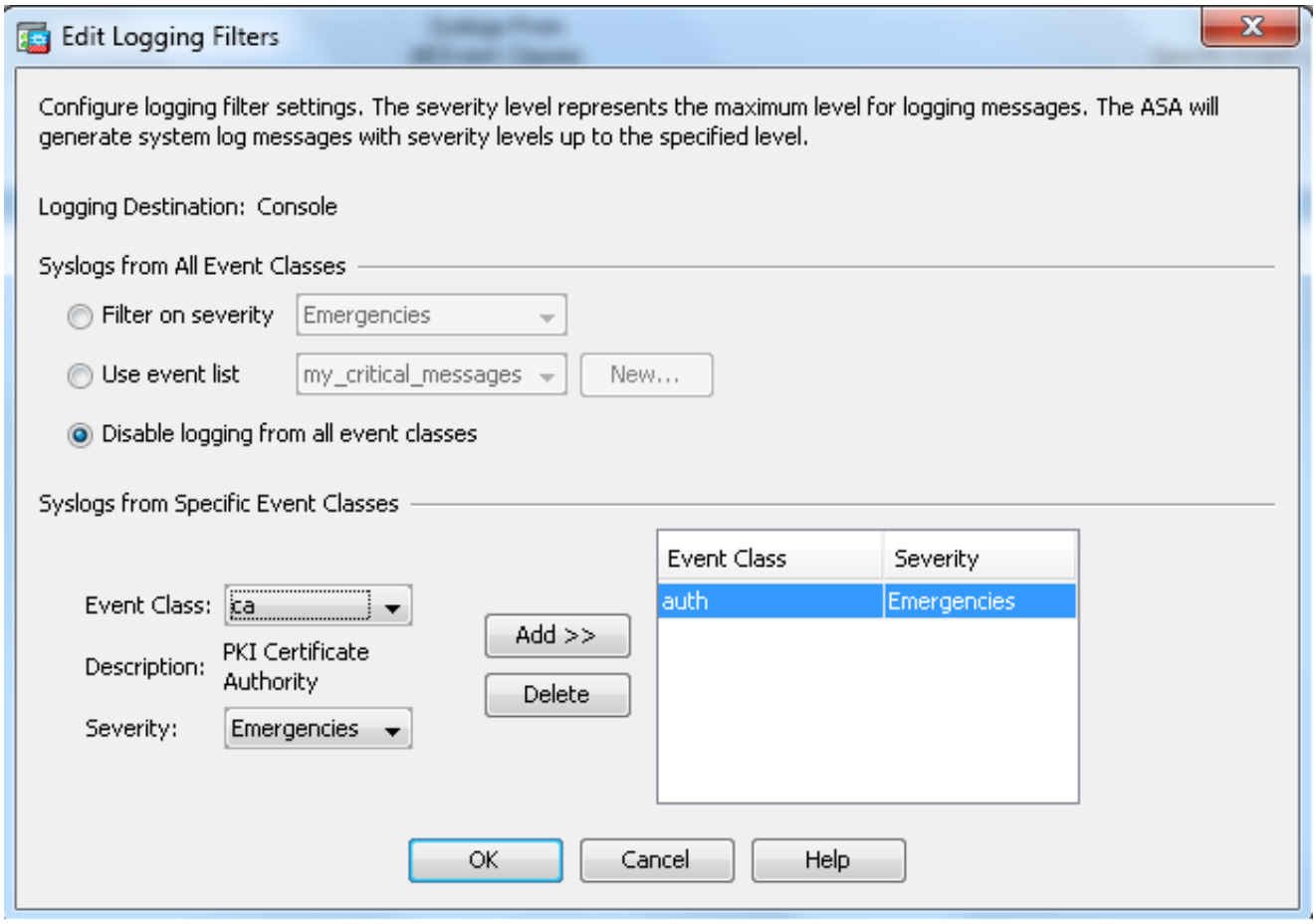
```
<#root>

logging class ca console emergencies
```

ASDM 컨피그레이션

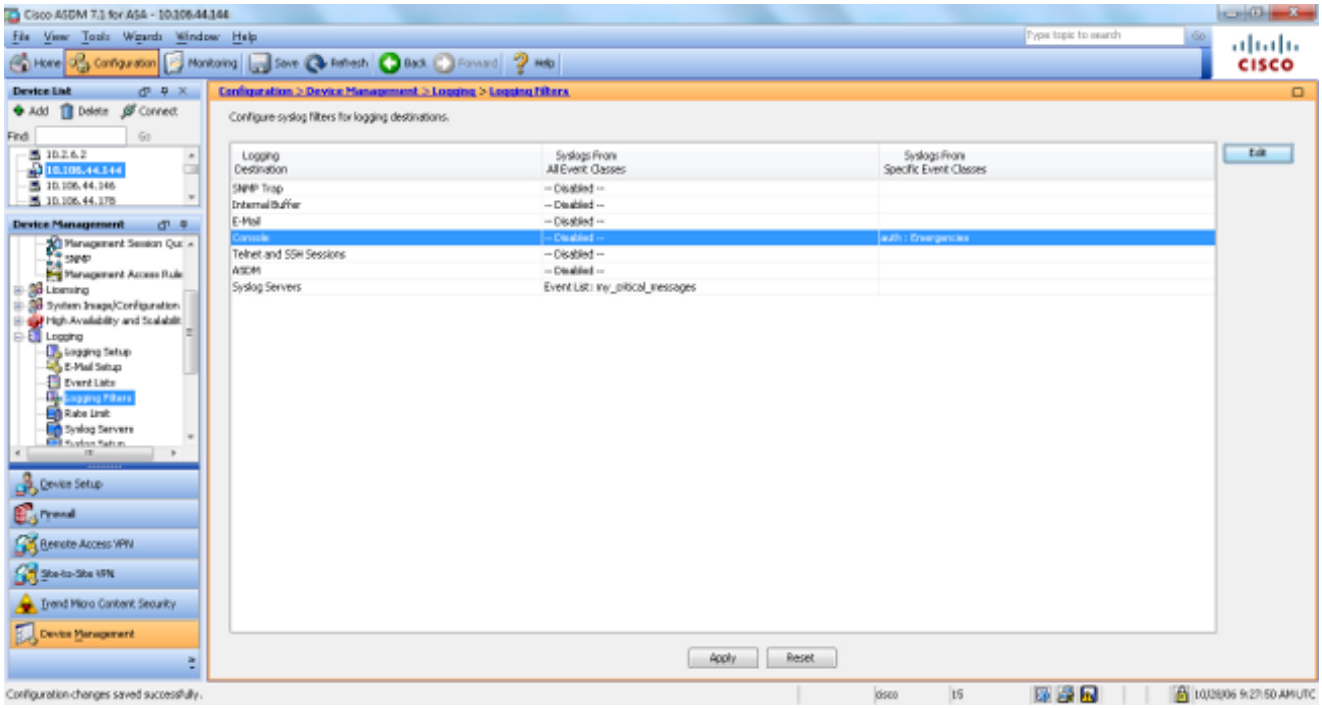
이 절차에서는 메시지 목록을 사용한 예 3의 ASDM 컨피그레이션을 보여줍니다.

1. Logging Filters(로깅 필터) 메뉴를 선택하고 Console(콘솔)을 대상으로 선택합니다.
2. Disable logging from all event classes(모든 이벤트 클래스에서 로깅 비활성화)를 클릭합니다.
3. Syslogs from Specific Event Classes(특정 이벤트 클래스의 Syslogs)에서 추가할 이벤트 클래스와 심각도를 선택합니다.

   이 절차에서는 각각 ca 및 Emergencies를 사용합니다.
4. 메시지 클래스에 추가하려면 Add를 클릭하고 OK를 클릭합니다.



5. Logging Filters 창으로 돌아간 후 Apply를 클릭합니다. 이제 콘솔은 Logging Filters 창에 표시된 대로 심각도 수준 Emergencies의 ca 클래스 메시지를 수집합니다.



이렇게 하면 예 3에 대한 ASDM 컨피그레이션이 완료됩니다. 로그 메시지 심각도 레벨 목록은 Messages Listed by Severity Level(심각도 레벨별로 나열되는 메시지)을 참조하십시오.

디버그 로그 메시지를 Syslog 서버로 전송

고급 문제 해결을 위해서는 기능/프로토콜별 디버그 로그가 필요합니다. 기본적으로 이러한 로그 메시지는 터미널(SSH/Telnet)에 표시됩니다. 디버그 유형 및 생성된 디버그 메시지의 속도에 따라 디버그가 활성화된 경우 CLI를 사용하는 것이 어려울 수 있습니다. 선택적으로, 디버그 메시지를 syslog 프로세스로 리디렉션하고 syslogs로 생성할 수 있습니다. 이러한 syslog는 다른 syslog와 마찬가지로 어떤 syslog 대상으로도 전송될 수 있습니다. 디버그를 syslog로 전환하려면 logging debug-trace 명령을 입력합니다. 이 컨피그레이션은 디버그 출력을 syslog 서버로 전송합니다.

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

로깅 목록 및 메시지 클래스 함께 사용

LAN-to-LAN 및 원격 액세스 IPsec VPN 메시지에만 syslog를 캡처하려면 logging list 명령을 입력합니다. 이 예에서는 디버깅 레벨 이상의 모든 VPN(IKE 및 IPsec) 클래스 시스템 로그 메시지를 캡처합니다.

예

<#root>

```
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
```

로그 ACL 적중

액세스 목록이 적중할 때 기록하기 위해 원하는 각 ACE(access list element)에 로그를 추가합니다.

다음 구문을 사용합니다.

<#root>

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

예

<#root>

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

ACL은 기본적으로 거부된 모든 패킷을 기록합니다. 거부된 패킷에 대해 syslog를 생성하기 위해 거부 ACL에 대한 log 옵션을 추가할 필요가 없습니다. log 옵션을 지정하면 적용되는 ACE에 대해 syslog 메시지 106100이 생성됩니다. Syslog 메시지 106100은 ASA 방화벽을 통과하는 모든 일치하는 허용 또는 거부 ACE 흐름에 대해 생성됩니다. 첫 번째 일치 흐름이 캐시됩니다. 이후의 일치 항목은 show access-list 명령에 표시되는 히트 수를 증가시킵니다. 기본 액세스 목록 로깅 동작인 log 키워드는 패킷이 거부되면 메시지 106023이 생성되고, 패킷이 허용되면 syslog 메시지가 생성되지 않는다는 것입니다.

생성된 syslog 메시지(106100)에 대해 선택적인 syslog 레벨(0 - 7)을 지정할 수 있습니다. 레벨을 지정하지 않으면 새 ACE의 기본 레벨은 6(정보)입니다. ACE가 이미 존재하는 경우 현재 로그 레벨은 변경되지 않습니다. log disable 옵션을 지정하면 액세스 목록 로깅이 완전히 비활성화됩니다. 메시지 106023을 포함하는 syslog 메시지가 생성되지 않습니다. log default 옵션은 기본 액세스 목록 로깅 동작을 복원합니다.

syslog 메시지 106100이 콘솔 출력에서 볼 수 있도록 하려면 다음 단계를 완료합니다.

1. 모든 출력 위치에 시스템 로그 메시지 전송을 활성화하려면 logging enable 명령을 입력합니다. 로그를 보려면 로깅 출력 위치를 설정해야 합니다.
2. 특정 시스템 로그 메시지의 심각도 수준을 설정하려면 logging message <message_number> level <severity_level> 명령을 입력합니다.

   이 경우 메시지 106100을 활성화하려면 logging message 106100 명령을 입력합니다.
3. 로깅 콘솔 message_list를 입력합니다 | severity_level 명령을 사용하여 시스템 로그 메시지가 발생할 때 tty(Security Appliance 콘솔)에 표시되도록 할 수 있습니다. severity_level을 1~7로 설정하거나 레벨 이름을 사용합니다. 또한 message_list 변수를 사용하여 어떤 메시지를 보낼지 지정할 수 있습니다.
4. 다른 심각도 수준이 할당된 메시지 및 비활성화된 메시지인 기본 설정에서 수정된 시스템 로그 메시지 메시지 목록을 표시하려면 show logging message 명령을 입력합니다.

다음은 show logging message 명령의 샘플 출력입니다.

```
<#root>

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
```

스탠바이 ASA에서 syslog 생성 차단

ASA 소프트웨어 릴리스 9.4.1 이후부터 시작하여 스탠바이 유닛에서 특정 syslog가 생성되는 것을 차단하고 이를 사용할 수 있습니다 명령을 사용합니다:

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

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

특정 syslog 메시지가 syslog 서버로 전송되도록 억제하려면 표시된 대로 명령을 입력해야 합니다.

```
<#root>

hostname(config)#

no logging message

 <syslog_id>
```

자세한 내용은 logging message 명령을 참조하십시오.

%ASA-3-201008: 새 연결 허용 안 함

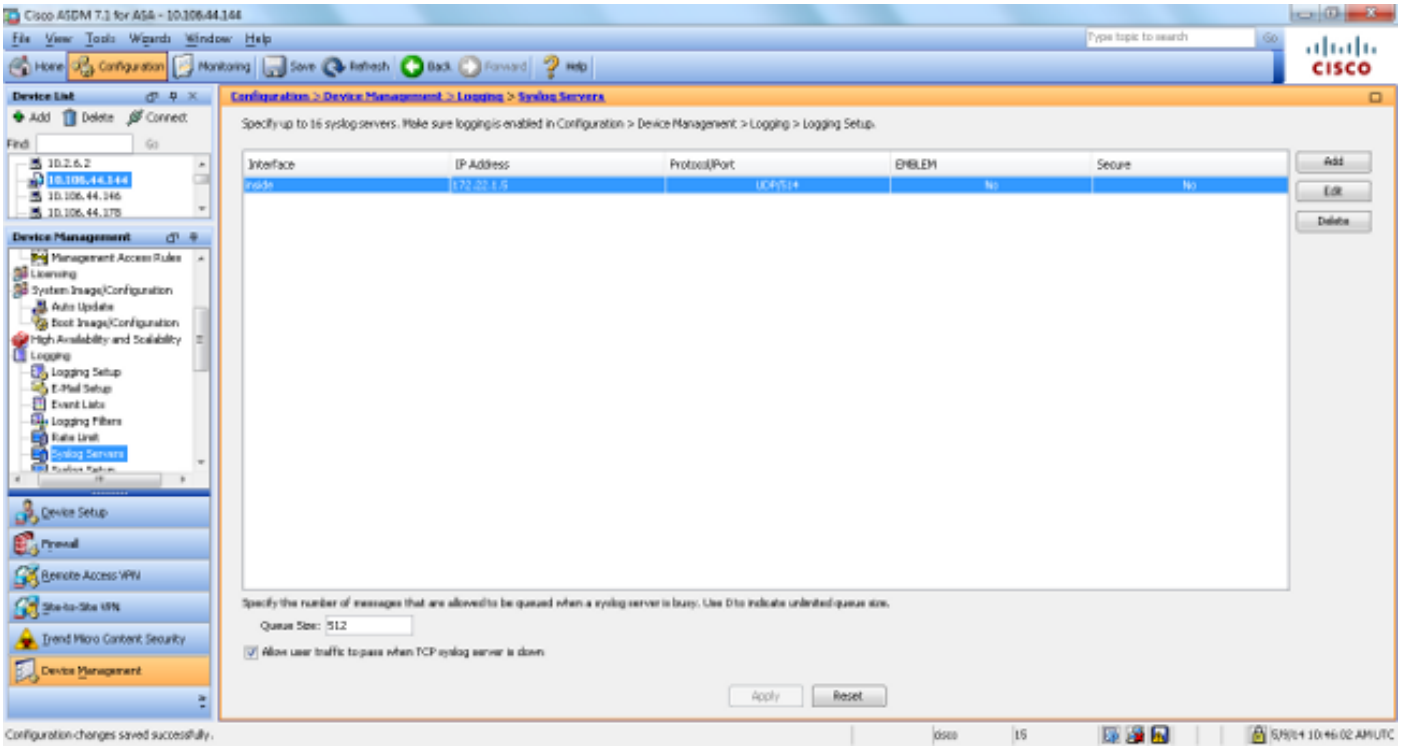
%ASA-3-201008: 새 연결을 허용하지 않습니다. ASA가 syslog 서버에 연결할 수 없고 새 연결이 허용되지 않는 경우 오류 메시지가 표시됩니다.

솔루션

이 메시지는 TCP 시스템 로그 메시징을 활성화한 상태에서 syslog 서버에 연결할 수 없거나 Cisco ASA PFSS(Syslog Server)를 사용하는 경우 및 Windows NT 시스템의 디스크가 꽉 찬 경우에 나타납니다. 이 오류 메시지를 해결하려면 다음 단계를 완료하십시오.

- TCP 시스템 로그 메시징이 활성화된 경우 비활성화합니다.
- PFSS를 사용하는 경우 PFSS가 있는 Windows NT 시스템에서 공간을 확보합니다.
- syslog 서버가 작동 중인지 확인하고 Cisco ASA 콘솔에서 호스트를 ping할 수 있습니다.
- 트래픽을 허용하려면 TCP 시스템 메시지 로깅을 다시 시작합니다.

syslog 서버가 다운되고 TCP 로깅이 구성된 경우 logging permit-hostdown 명령을 사용하거나 UDP 로깅으로 전환합니다.



관련 정보

- Cisco Secure PIX Firewall 명령 참조
- RFC(설명 요청)
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.