ASA 8.2:ASDM을 사용하여 Syslog 구성

목차

소개

이 문서에서는 ASDM(Adaptive Security Device Manager) GUI를 사용하여 Cisco ASA(Adaptive Security Appliance) 8.x에서 syslog를 구성하는 방법에 대해 설명합니다.시스템 로그 메시지는 Cisco ASA가 컨피그레이션의 변경, 네트워크 설정 변경 또는 디바이스 성능 변경 사항을 관리자에게 알리기 위해 생성하는 메시지입니다.관리자는 시스템 로그 메시지를 분석하여 근본 원인 분석을 수행하여 오류를 쉽게 해결할 수 있습니다.

Syslog 메시지는 주로 심각도 수준에 따라 차별화됩니다.

1. 심각도 0 - 긴급 메시지 - 리소스를 사용할 수 없음
2. 심각도 1 - 경고 메시지 - 즉각적인 조치가 필요합니다.
3. 심각도 2 - 중요 메시지 - 중요 조건

4. 심각도 3 - 오류 메시지 - 오류 조건
5. 심각도 4 - 경고 메시지 - 경고 조건
6. 심각도 5 - 알림 메시지 - 정상이지만 중요한 조건
7. 심각도 6 - 정보 메시지 - 정보 메시지만 해당
8. 심각도 7 - 디버깅 메시지 - 디버깅 메시지만 해당**참고:** 가장 높은 심각도 수준은 긴급 수준이며 가장 낮은 심각도 수준은 디버깅입니다.

Cisco ASA에서 생성된 샘플 syslog 메시지는 다음과 같습니다.

- %ASA-6-106012:IP_address에서 IP_address로의 IP 거부, IP 옵션은 16진수입니다.
- %ASA-3-211001:메모리 할당 오류
- %ASA-5-335003:NAC 기본 ACL 적용, ACL:ACL-name - host-address

"%ASA-X-YYYYY:"에 지정된 숫자 값 X는 메시지의 심각도를 나타냅니다.예를 들어 "%ASA-6-106012"는 정보 메시지이며 "%ASA-5-335003"은 오류 메시지입니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 버전 8.2
- Cisco ASDM 버전 6.2

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

표기 규칙

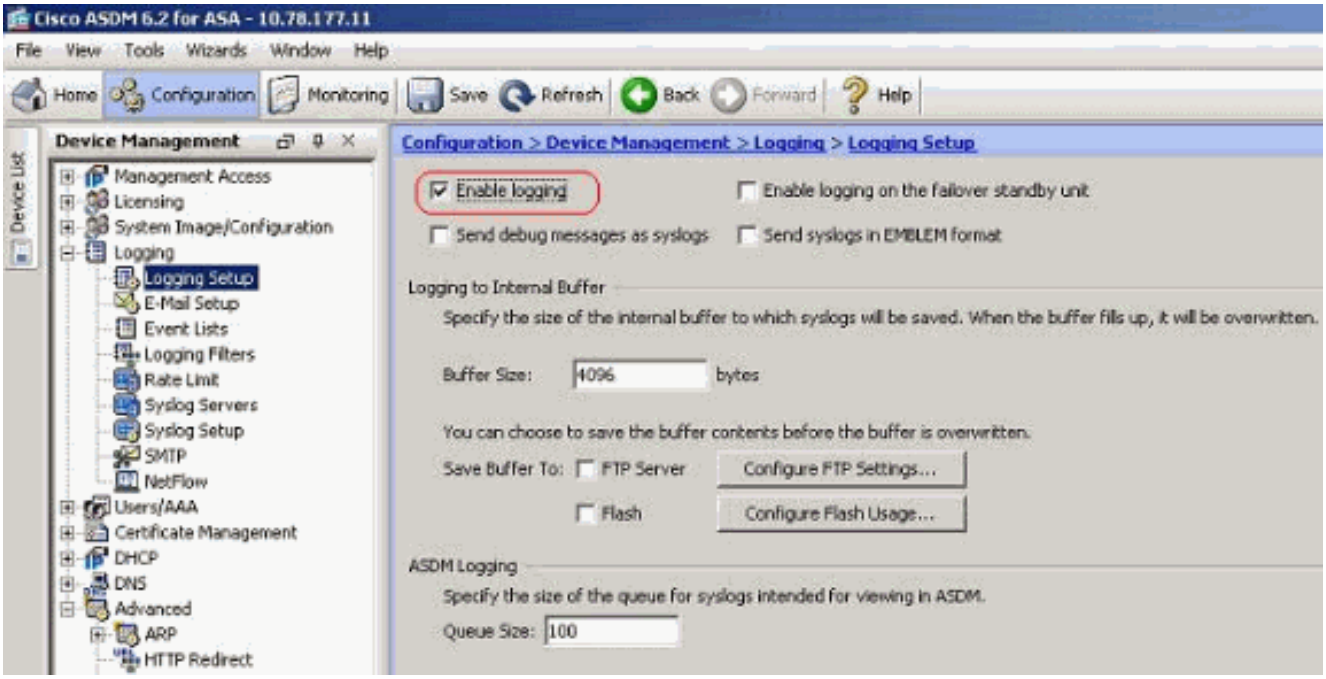
문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

ASDM을 사용하여 기본 Syslog 컨피그레이션

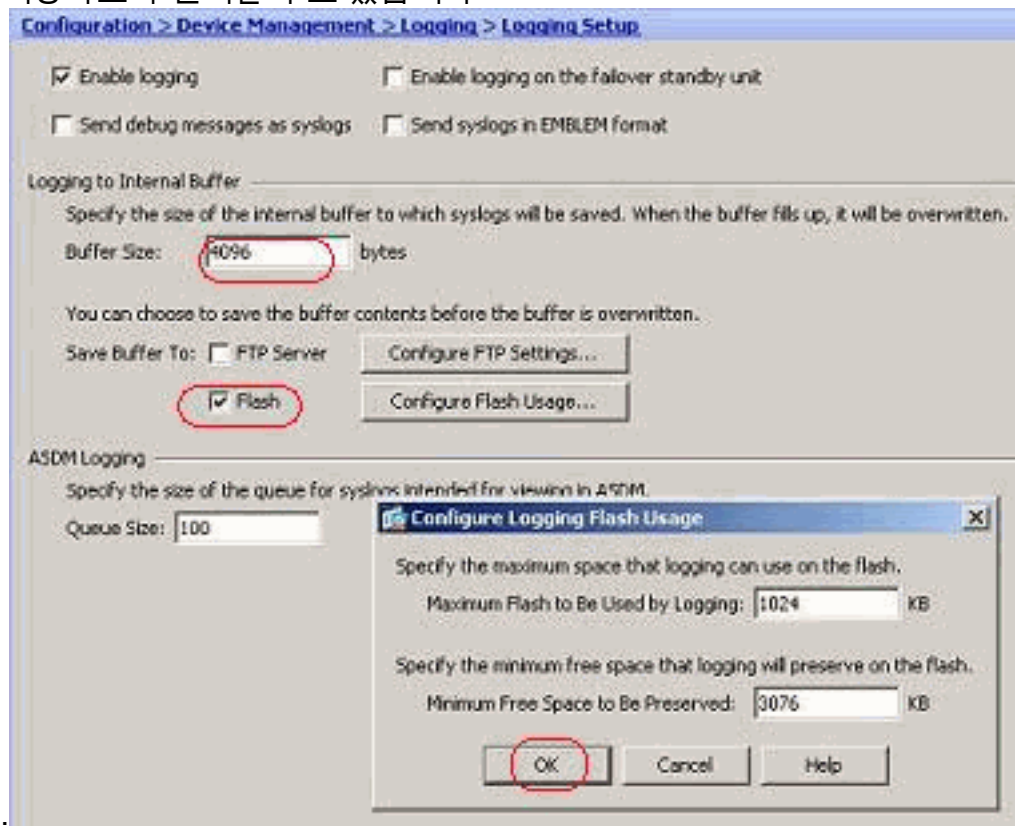
로깅 사용

다음 단계를 완료하십시오.

1. Configuration(*구성*) > *Device Management(디바이스 관리)* > *Logging(로깅)* > *Logging Setup(로깅 설정)*을 선택하고 Enable logging(로깅 활성화) 옵션을 선택합니다
.

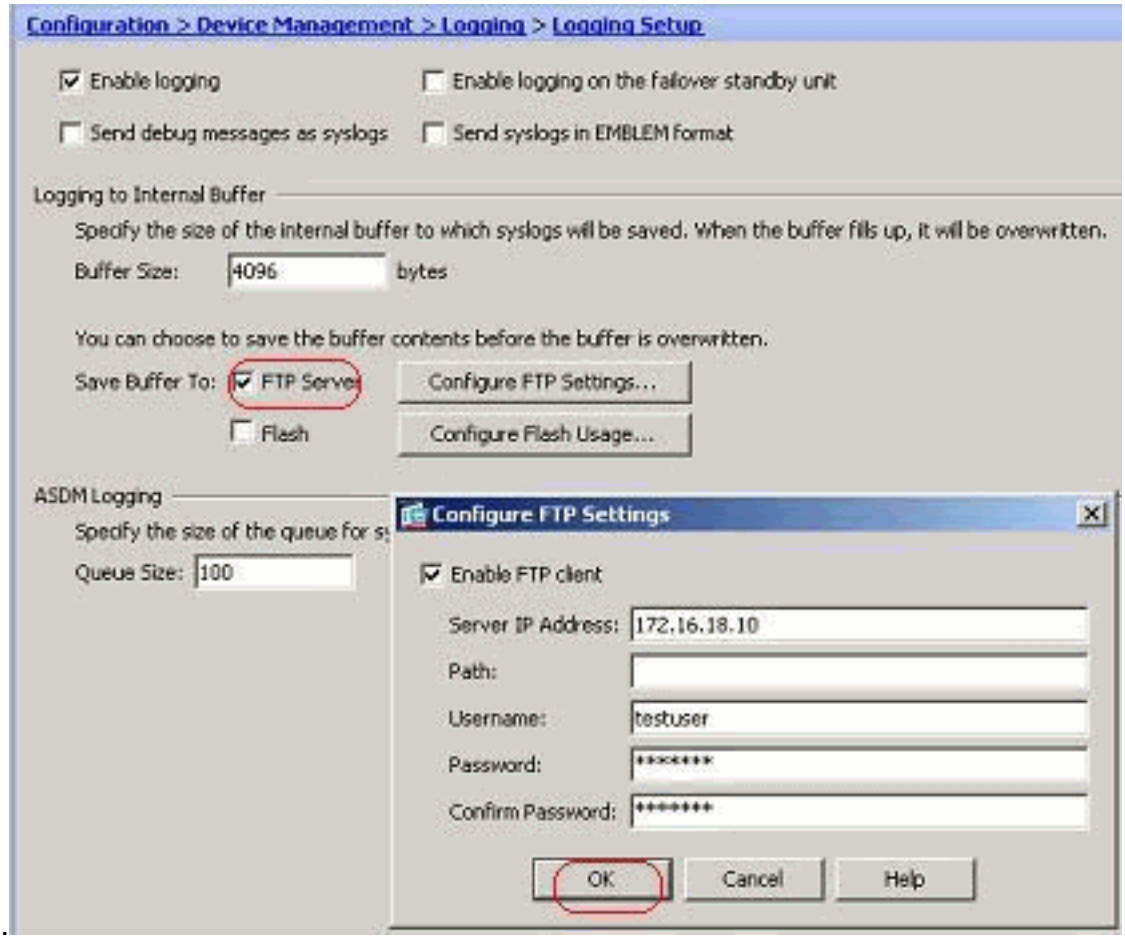


2. 버퍼 크기를 지정하여 syslog 메시지를 내부 버퍼에 로깅할 수 있습니다.*Configure Flash Usage*(플래시 사용량 구성)를 클릭하고 Flash 설정을 정의하여 버퍼 내용을 플래시 메모리에 저장하도록 선택할 수도 있습니다



.

3. 버퍼된 로그 메시지는 덮어쓰기되기 전에 FTP 서버로 전송할 수 있습니다.Configure *FTP Settings(FTP 설정 구성*)를 클릭하고 다음과 같이 FTP 서버 세부사항을 지정합니다

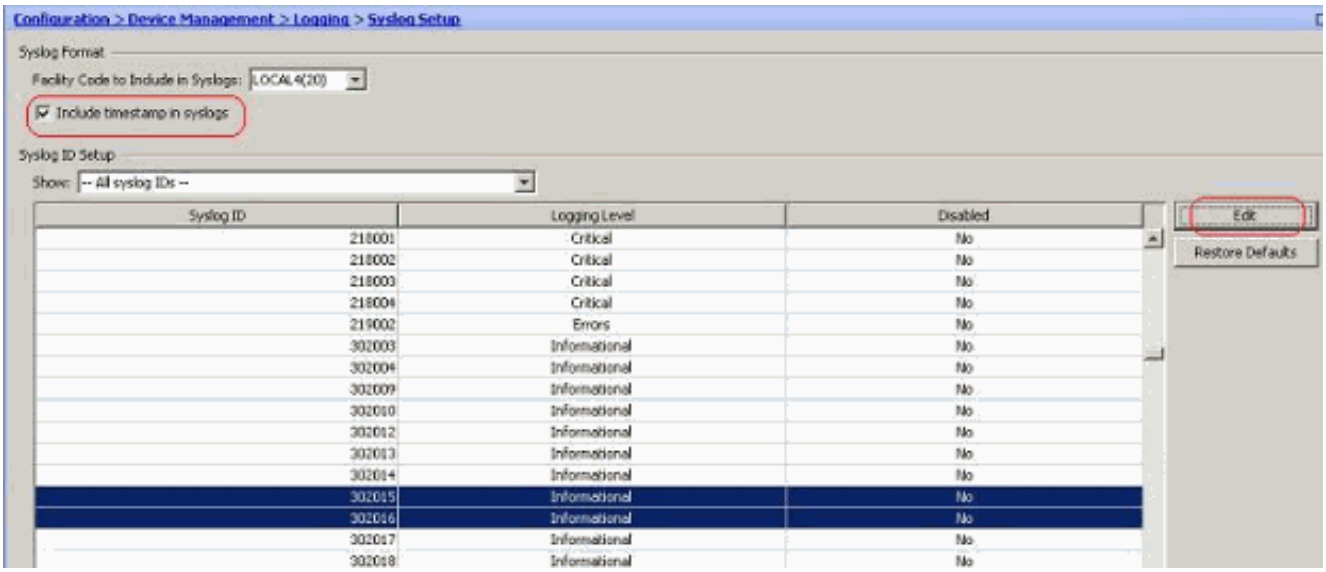


로깅 사용 안 함

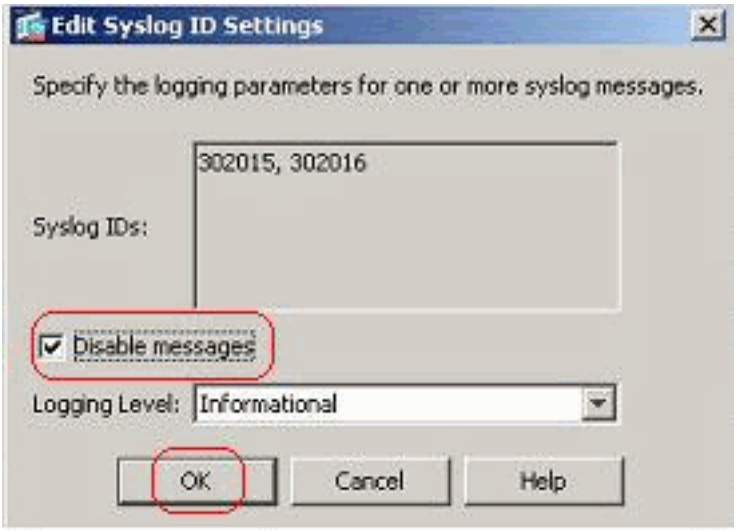
요구 사항에 따라 특정 syslog ID를 비활성화할 수 있습니다.

참고: Include timestamp in syslogs(*syslogs에 타임스탬프 포함*) 옵션의 확인 표시를 선택하면, syslog에 필드로 생성된 날짜와 시간을 추가할 수 있습니다.

1. 비활성화할 syslogs를 선택하고 Edit를 *클릭합니다*



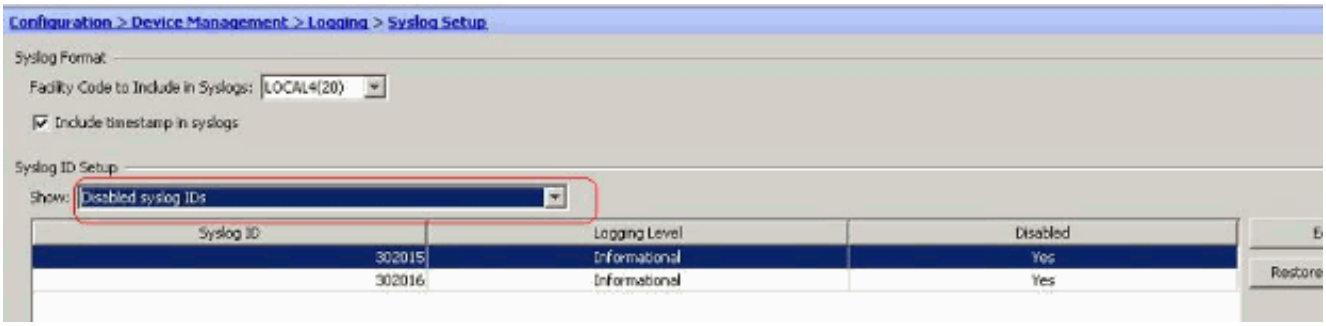
2. Edit Syslog *ID Settings(Syslog ID 설정 수정*) 창에서 Disable messages(*메시지 비활성화*) 옵



션을 선택하고 *OK(확인)*를 클릭합니다.

3. 비활성화된 syslog는 Syslog ID Setup 드롭다운 메뉴에서 Disabled syslog *IDs(비활성화된 syslog ID)*를 선택하여 별도의 탭에서 볼 수 있습니다

.

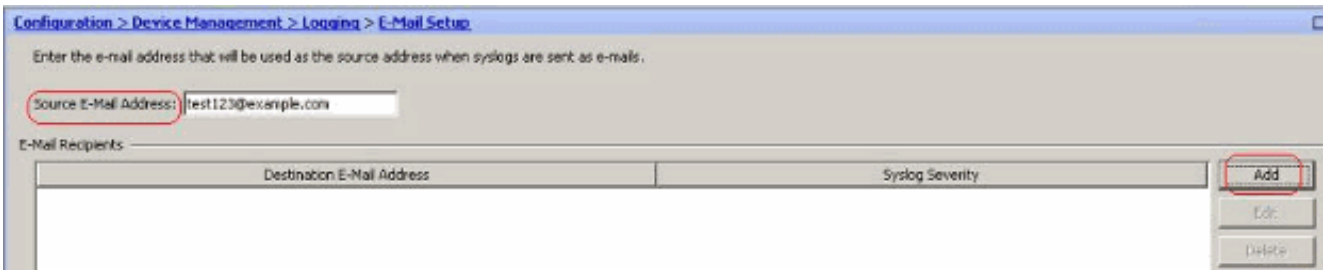


전자 메일에 로깅

ASDM을 사용하여 syslog를 이메일로 전송하려면 다음 단계를 완료합니다.

1. Configuration *> Device Management > Logging > E-Mail Setup을 선택합니다*.Source *E-Mail Address* 필드는 이메일 ID를 syslog의 소스로 할당하는 데 유용합니다.원본 전자 메일 주소를 지정합니다.이제 Add(*추가*)를 클릭하여 전자 메일 수신자를 추가합니다

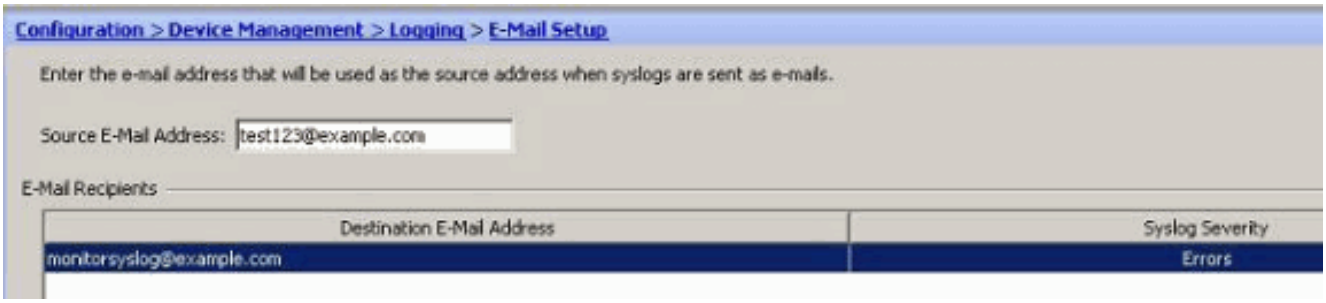
.



2. Destination *E-mail Address(대상 이메일 주소)*를 지정하고 Severity(심각도) *레벨*을 선택합니다.심각도 수준에 따라 다른 이메일 수신자를 정의할 수 있습니다.*확인*을 클릭하여 *전자 메일*

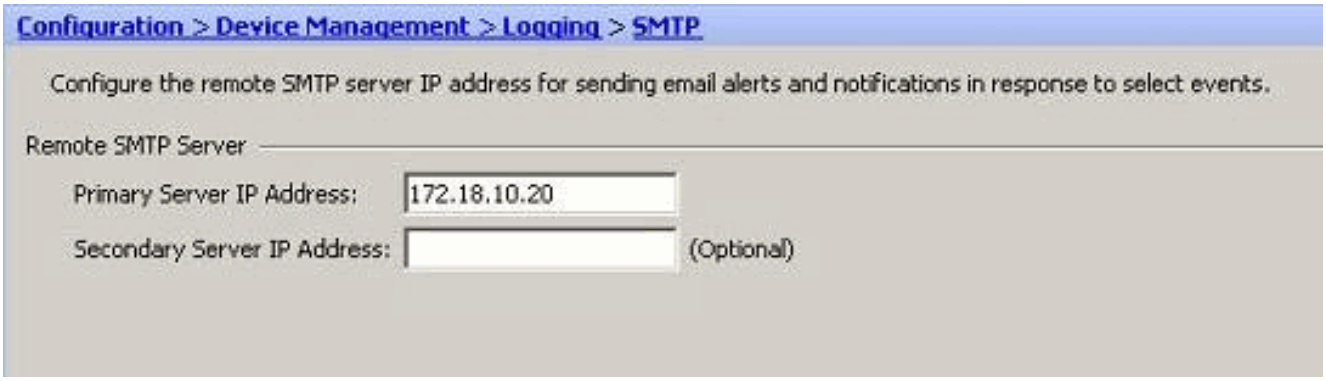
설정 창으로 돌아갑니다. 이렇게 하면 다음 컨피그레이션이 수행됩니다

.



3. Configuration > *Device Setup* > *Logging* > *SMTP를 선택하고* SMTP 서버를 지정합니다

.

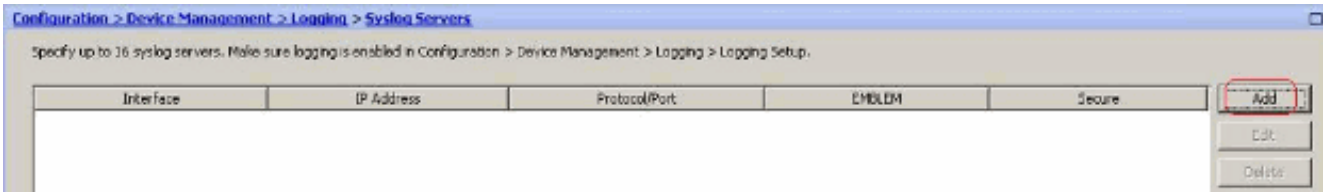


Syslog 서버에 로깅

모든 syslog 메시지를 전용 syslog 서버로 보낼 수 있습니다.ASDM을 사용하여 다음 단계를 수행합니다.

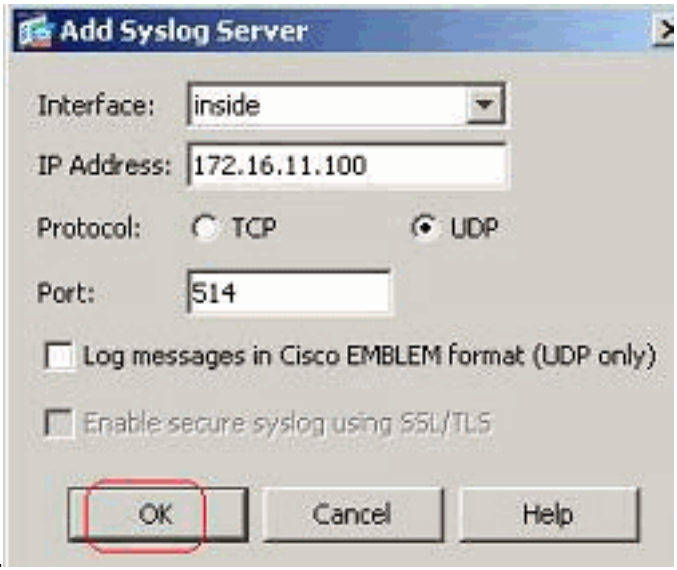
1. Configuration > *Device Management* > *Logging* > *Syslog Servers*를 선택하고 *Add*를 클릭하여 syslog 서버를 추가합니다

.



Add *Syslog Server* 창이 나타납니다.

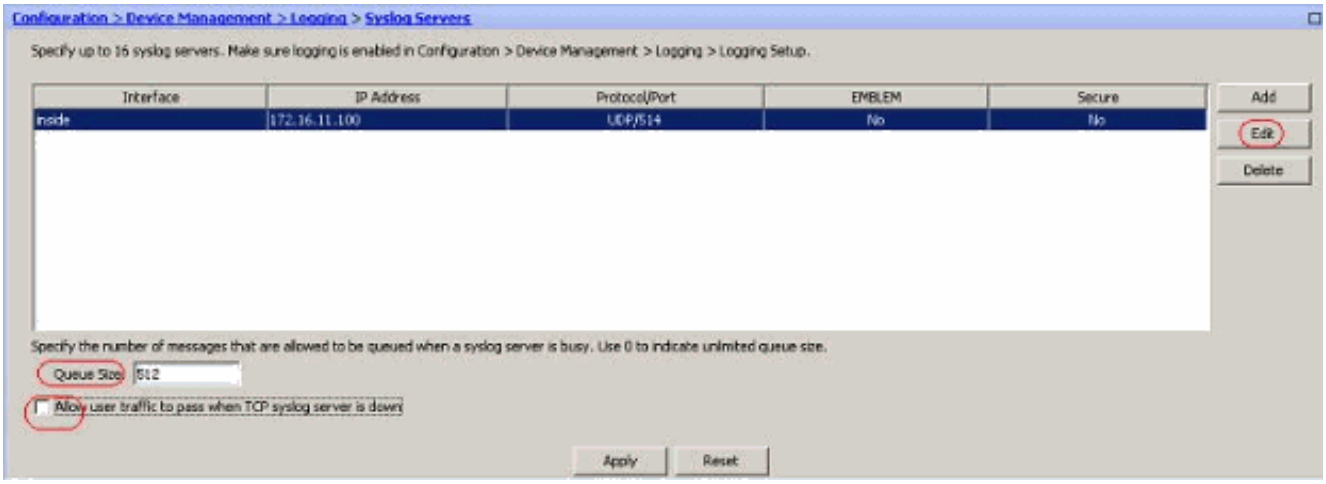
2. 서버가 연결된 인터페이스를 IP 주소와 함께 지정합니다.네트워크 설정에 따라 *Protocol* 및 *Port* 세부사항을 지정합니다.그런 다음 *확인*을 클릭합니다.**참고:** Cisco ASA에서 syslog 서버



에 연결할 수 있는지 확인합니다.

3. 구성된 syslog 서버가 여기에 표시된 것처럼 표시됩니다.이 서버를 선택한 다음 [편집]을 클릭하면 수정할 수 *있습니다*

.



참고: *Allow user traffic to pass when TCP syslog server is down 옵션을 선택합니다*.그렇지 않으면 ASA를 통해 새 사용자 세션이 거부됩니다.이는 ASA와 syslog 서버 간의 전송 프로토콜이 TCP인 경우에만 적용됩니다.기본적으로 Cisco ASA는 syslog 서버가 다운된 경우 어떤 이유로든 새 네트워크 액세스 세션을 거부합니다.syslog 서버로 전송할 syslog 메시지의 유형을 정의하려면 Logging Filter 섹션을 참조하십시오.

ASDM을 사용하여 고급 Syslog 컨피그레이션

이벤트 목록 작업

이벤트 목록을 사용하면 대상에 전송할 syslog 메시지 그룹이 포함된 사용자 지정 목록을 생성할 수 있습니다.이벤트 목록은 다음과 같은 세 가지 방법으로 생성할 수 있습니다.

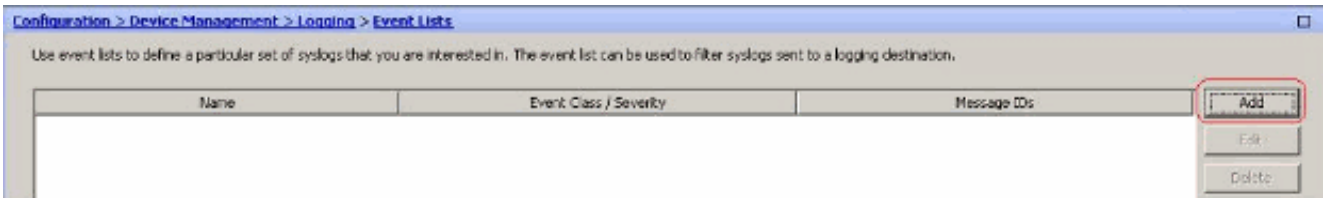
- 메시지 ID 또는 메시지 ID 범위
- 메시지 심각도
- 메시지 클래스

메시지 ID 또는 메시지 ID 범위

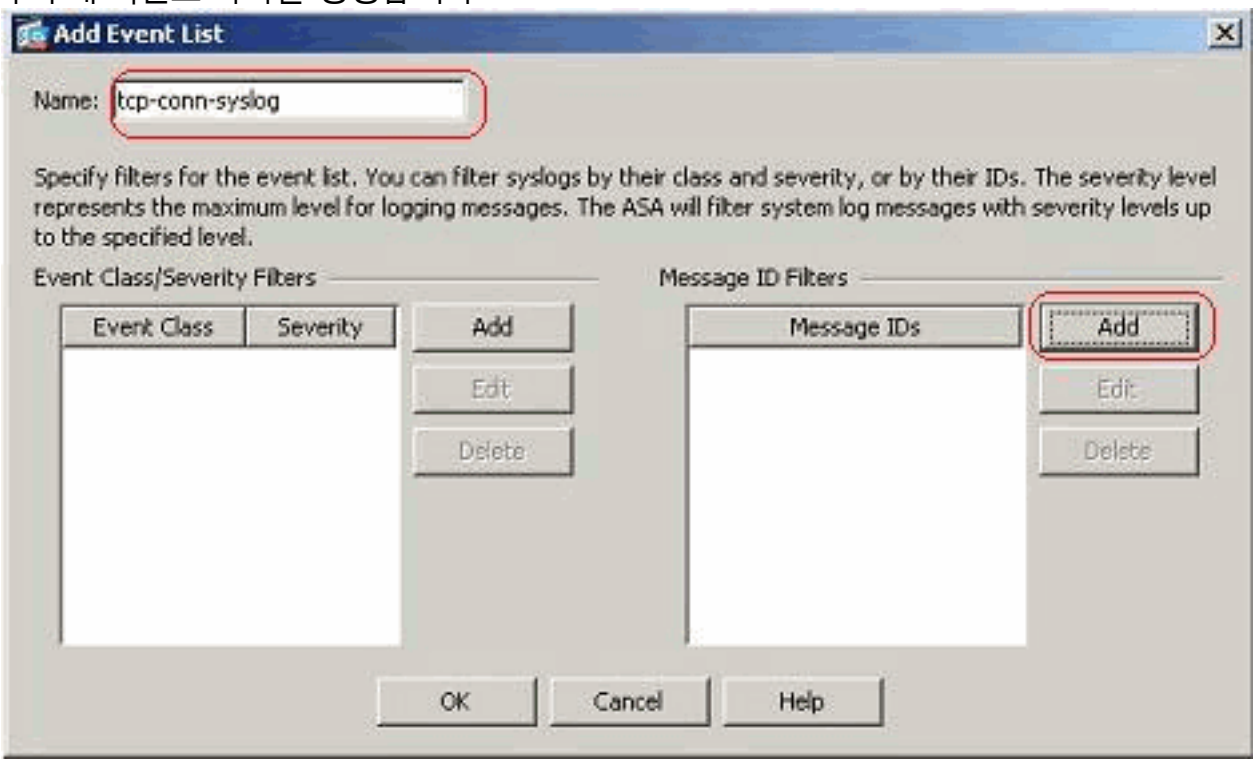
다음 단계를 수행합니다.

1. Configuration > *Device Management* > *Logging* > *Event Lists*를 선택하고 *Add*를 클릭하여 새 이벤트 목록을 생성합니다

.

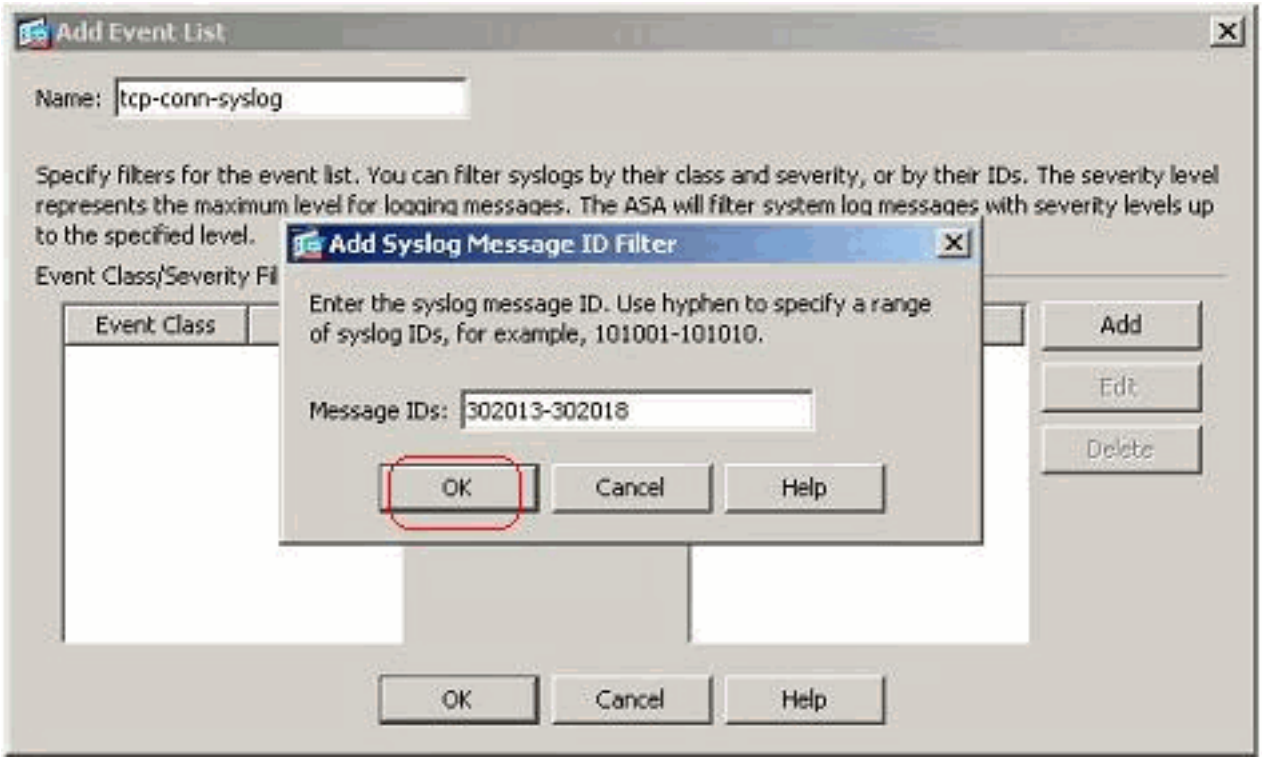


2. *이름* 필드에 이름을 지정합니다.Message *ID Filters*(*메시지 ID 필터*) 창에서 Add(추가)를 클릭하여 새 이벤트 목록을 생성합니다



.

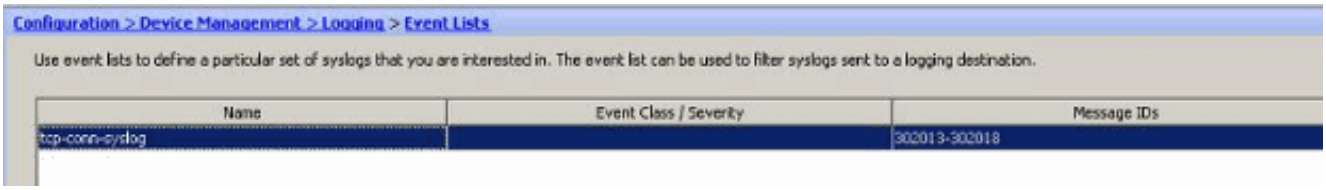
3. syslog 메시지 ID의 범위를 지정합니다.예를 들어 TCP syslog 메시지가 나타납니다.OK(*확인*)를 클릭하여 완료합니다



.

4. *OK*를 다시 클릭하여 *Event Lists* 창으로 돌아갑니다

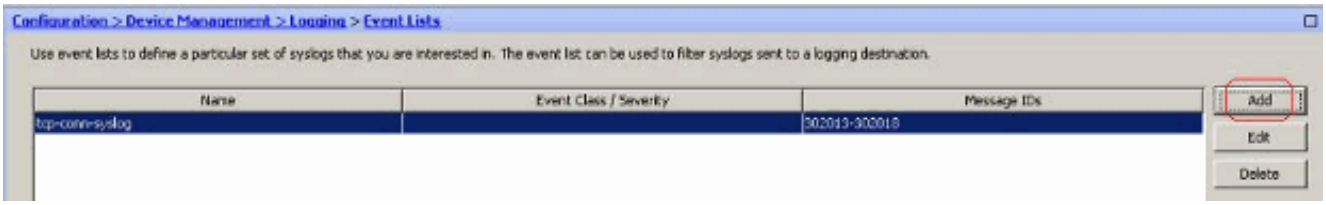
.



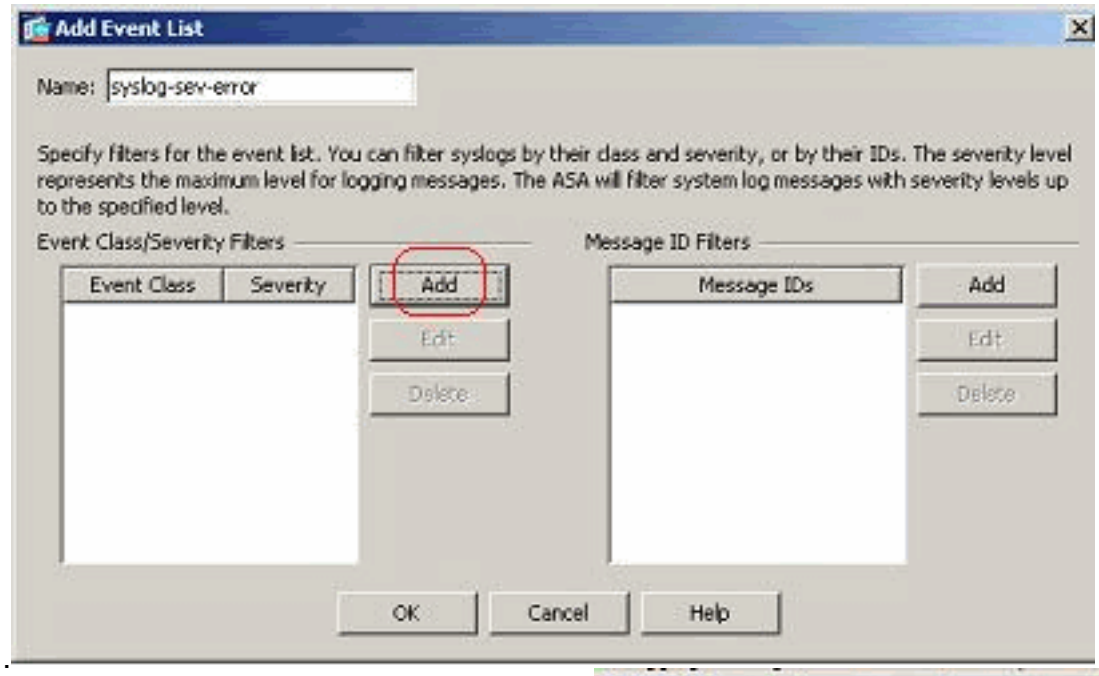
메시지 심각도

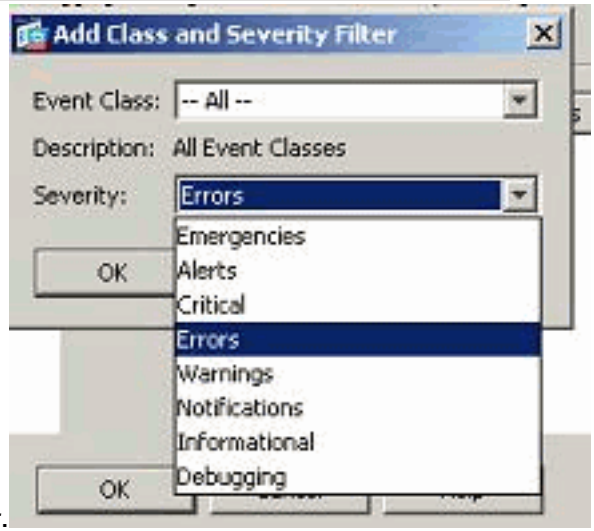
1. 이벤트 목록은 메시지 심각도에 따라 정의할 수도 있습니다.Add(*추가*)를 클릭하여 별도의 이벤트 목록을 생성합니다

.

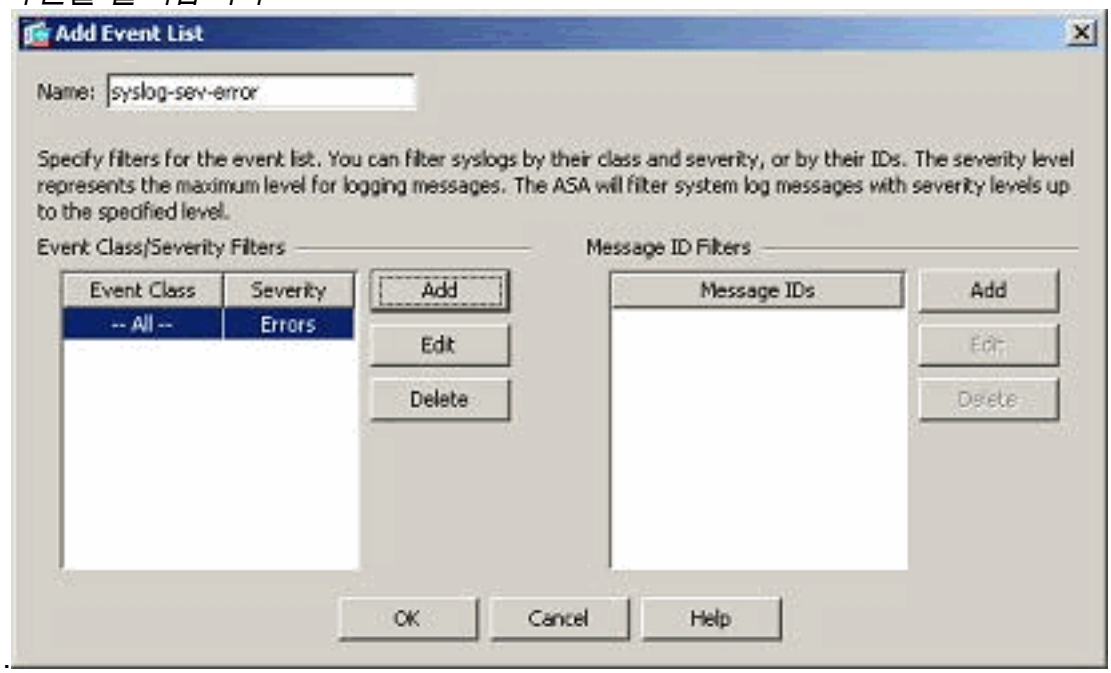


2. 이름을 지정하고 Add를 *클릭합니다*





3. 심각도 레벨을 *Errors*(오류)로 *선택합니다*.
4. *확인을 클릭합니다*



메시지 클래스

이벤트 목록은 메시지 클래스를 기반으로 구성됩니다.메시지 클래스는 보안 어플라이언스 기능과

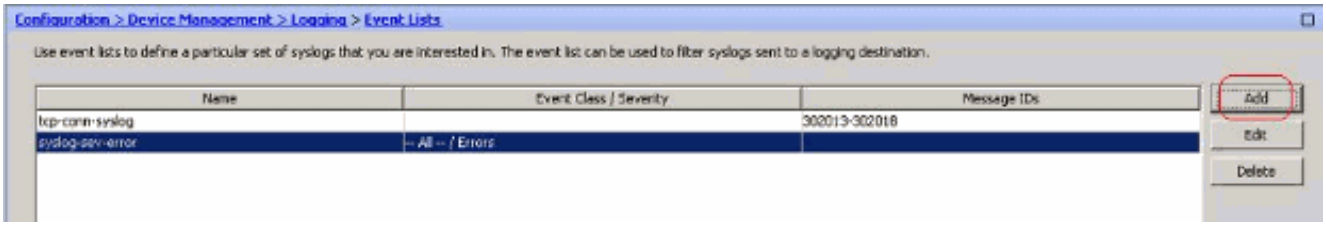
관련된 syslog 메시지 그룹으로서, 각 메시지에 대해 개별적으로 클래스를 지정하는 대신 전체 메시지 클래스를 지정할 수 있습니다.예를 들어 인증 클래스를 사용하여 사용자 인증과 관련된 모든 syslog 메시지를 선택합니다.사용 가능한 일부 메시지 클래스는 다음과 같습니다.

- All(모두) - 모든 이벤트 클래스
- auth - 사용자 인증
- bridge - 투명한 방화벽
- ca - PKI 인증 기관
- config - 명령 인터페이스
- ha - 장애 조치
- ips - Intrusion Protection 서비스
- ip - IP 스택
- np - 네트워크 프로세서
- ospf - OSPF 라우팅
- rip - RIP 라우팅
- session - 사용자 세션

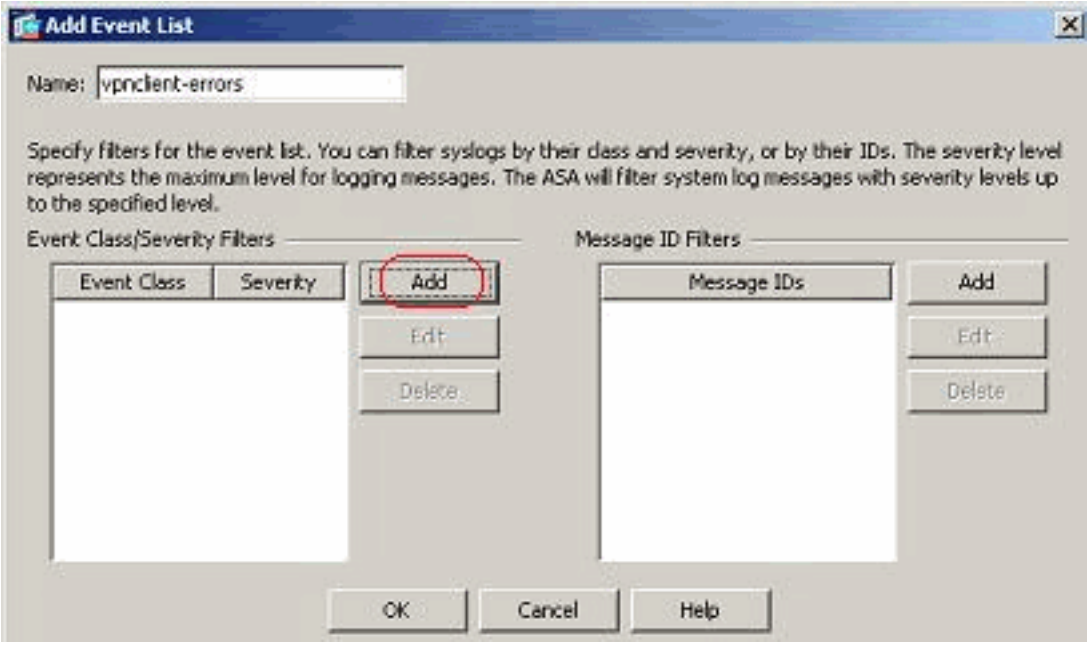
vpnclient-*errors* 메시지 클래스를 기반으로 이벤트 클래스*를* 생성하려면 다음 단계를 수행합니다 .메시지 클래스 vpnc*를* 사용하여 vpnclient와 관련된 모든 syslog 메시지를 분류할 수 있습니다.이 메시지 클래스의 심각도 수준이 "오류"로 선택됩니다.

1. Add를 클릭하여 새 이벤트 목록을 만듭니다

.

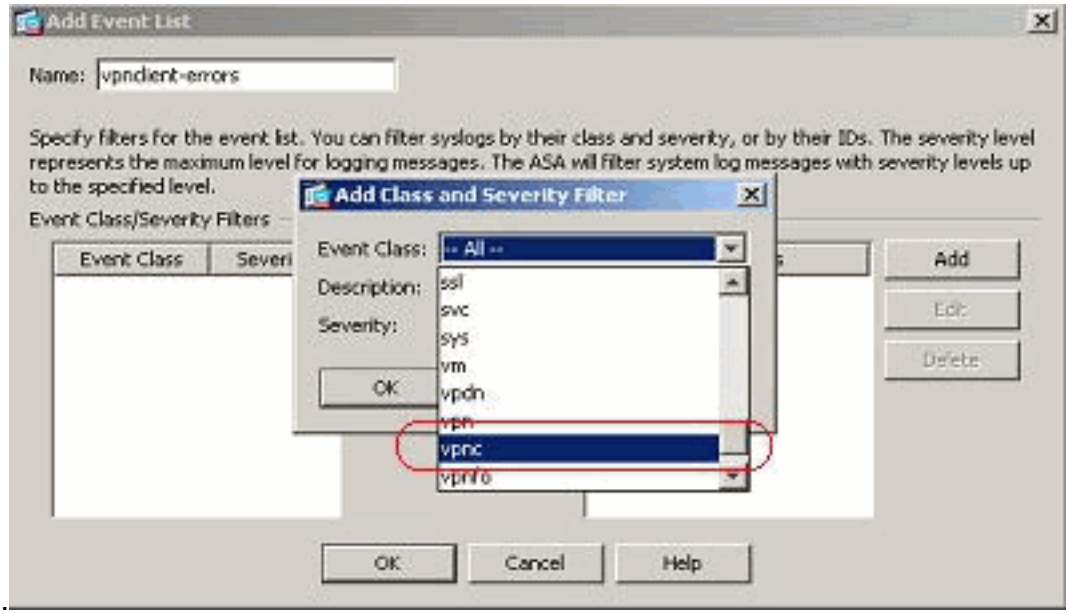


2. 생성하는 메시지 클래스와 관련될 이름을 지정하고 Add를 *클릭합니다*

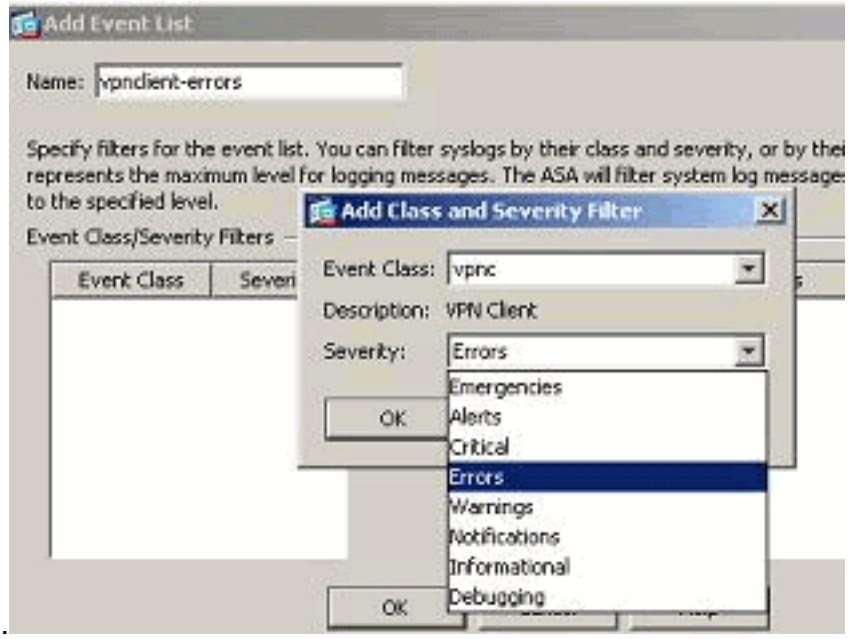


.

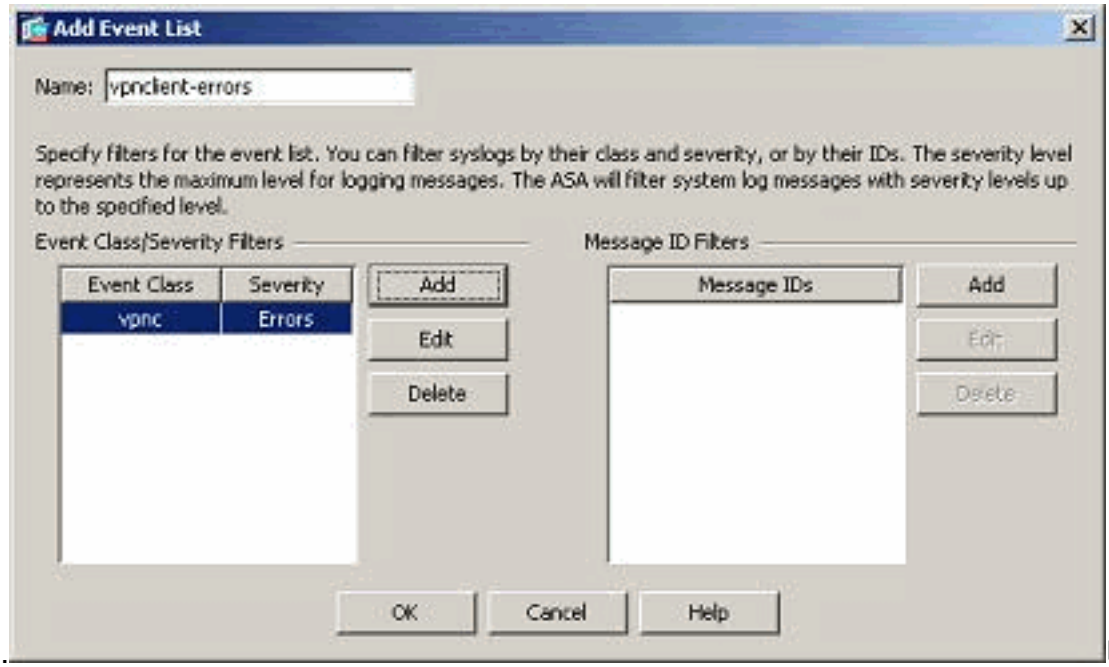
3. 드롭다운 목록에서 vpnc를 선택합니다



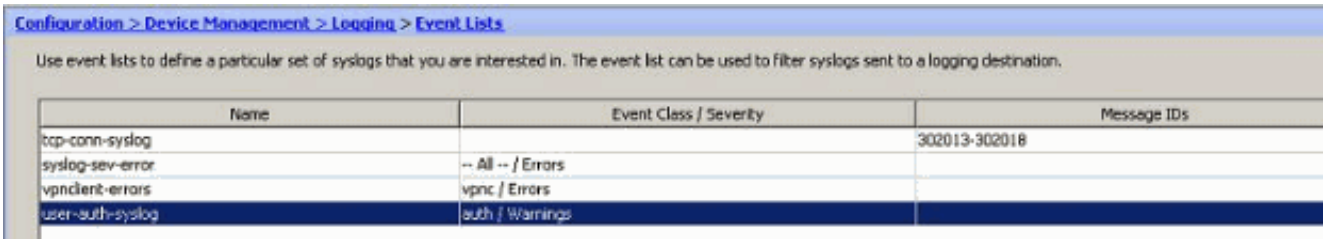
4. 심각도 레벨을 *Errors*(오류)로 *선택합니다*.이 심각도 수준은 이 메시지 클래스에 대해 기록된 메시지에만 적용됩니다.*OK*를 클릭하여 Add Event List 창으로 돌아갑니다



5. 이벤트 클래스/심각도는 여기에 표시됩니다.확인을 클릭하여 "vpnclient-errors" 이벤트 목록 구성을 완료합니다



다음 스크린샷에는 "user-auth-syslog"라는 새 이벤트 목록이 메시지 클래스를 "auth"로, 이 특정 메시지 클래스의 syslogs에 대한 심각도 수준을 "Warnings"로 하여 생성되었음을 보여줍니다. 이를 구성하면 이벤트 목록은 "auth" 메시지 클래스와 관련된 모든 syslog 메시지를 지정하며 심각도 수준은 "Warnings(경고)" 레벨까지**로** 설정됩니다.**참고:** 여기서 "최대" 용어는 중요합니다.심각도 수준을 나타내는 경우, 모든 syslog 메시지는 해당 레벨까지 로깅됩니다.**참고:** 이벤트 목록에는 여러 이벤트 클래스가 포함될 수 있습니다."vpnclient-errors" 이벤트 목록은 **Edit**(수정)를 클릭하고 새 이벤트 클래스 "ssl/error"를 정의하여 수정합니다



로깅 필터 작업

로깅 필터는 syslog 메시지를 지정된 대상으로 전송하는 데 사용됩니다.이러한 syslog 메시지는 "Severity(심각도)" 또는 "Even Lists(짝수 목록)"를 기반으로 할 수 있습니다.

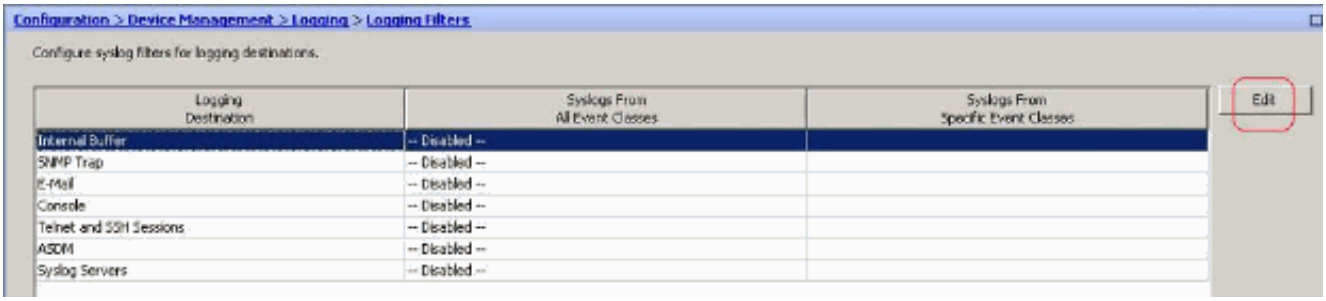
이러한 필터를 적용할 수 있는 대상 유형은 다음과 같습니다.

- 내부 버퍼
- SNMP 트랩
- 이메일
- 콘솔
- 텔넷 세션
- ASDM
- Syslog 서버

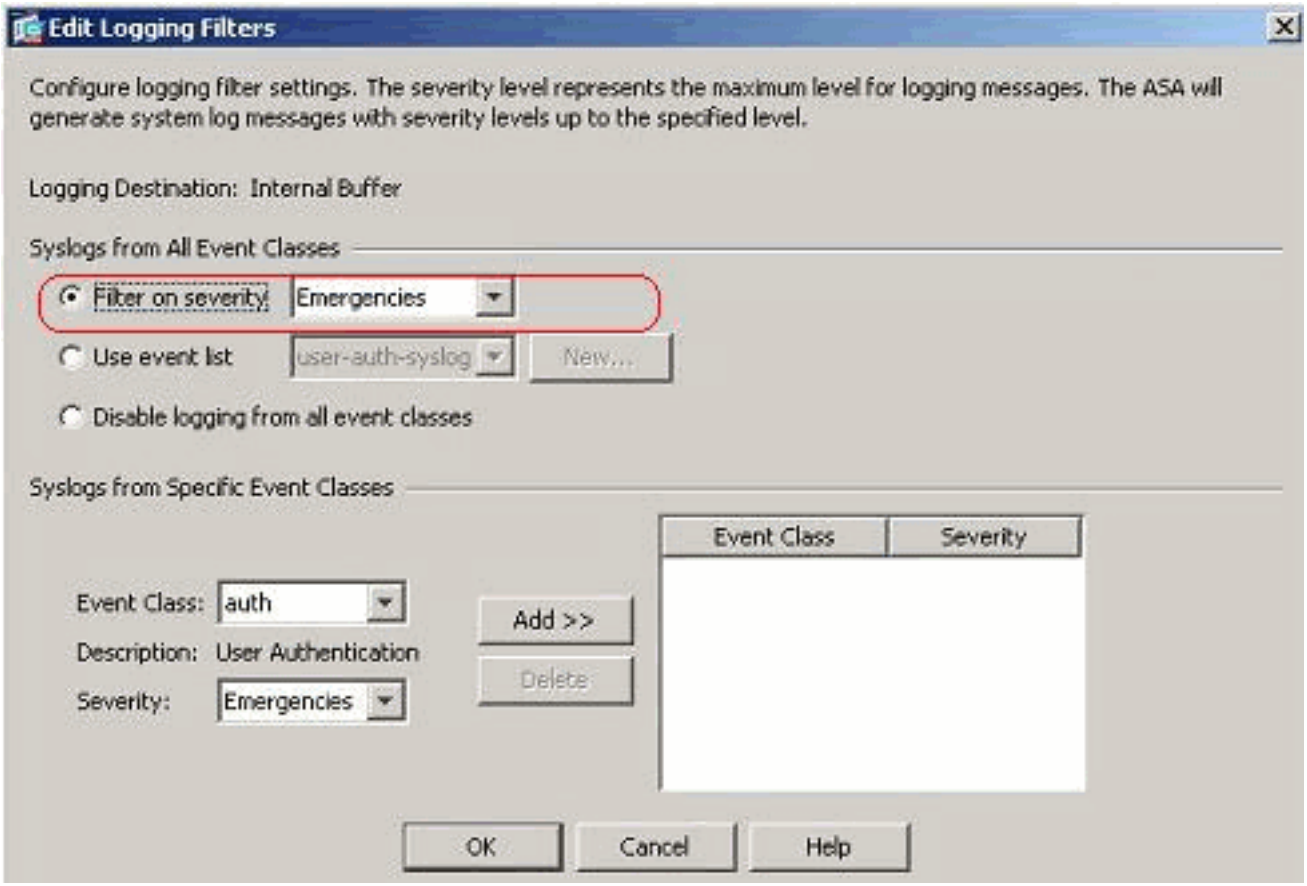
다음 단계를 수행합니다.

1. Configuration **> Device Management > Logging > Logging Filters**를 선택하고 로깅 대상을 선택합니다.그런 다음 **Edit(편집)**를 클릭하여 설정을 수정합니다

.

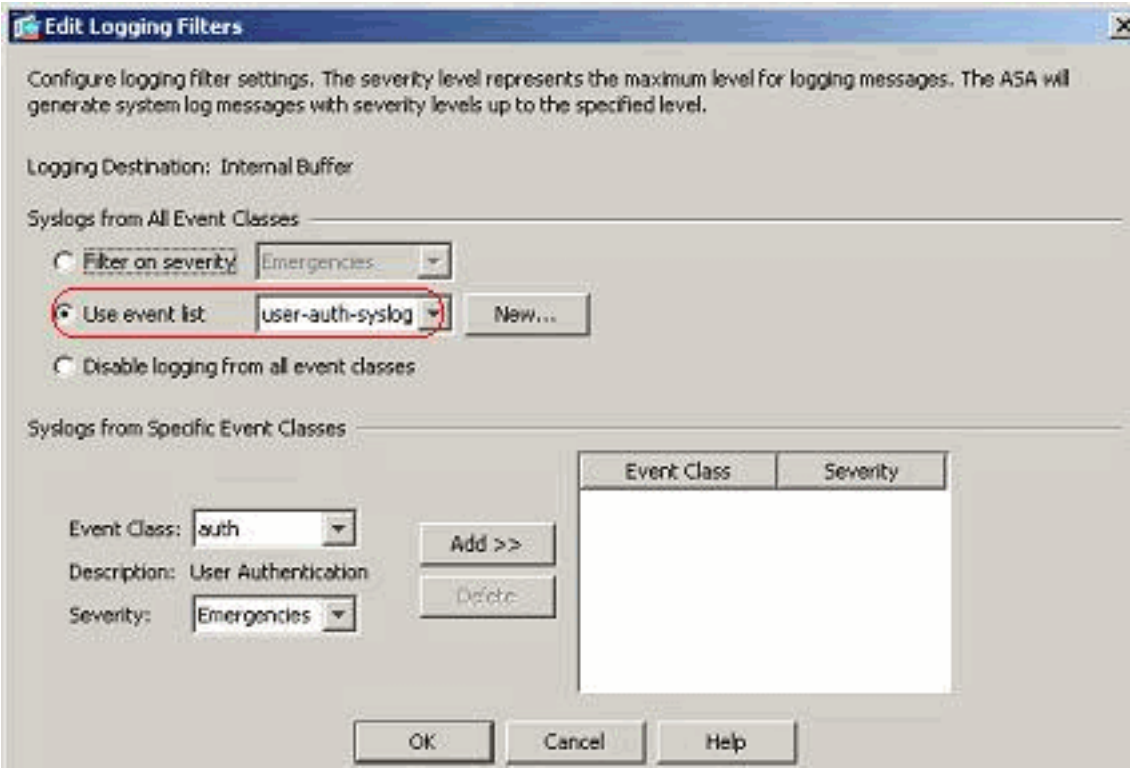


2. 심각도를 기준으로 syslog 메시지를 보낼 수 있습니다.여기서 **Emergencies**는 예제로 표시하도록 선택되었습니다



.

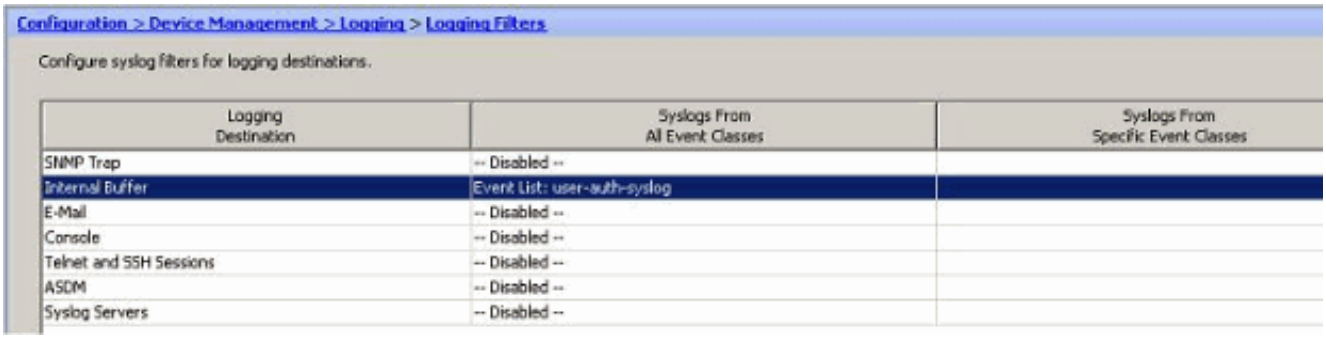
3. 이벤트 목록을 선택하여 특정 대상으로 전송할 메시지 유형을 지정할 수도 있습니다.**확인**을



클릭합니다.

4. 수정을 확인합니다

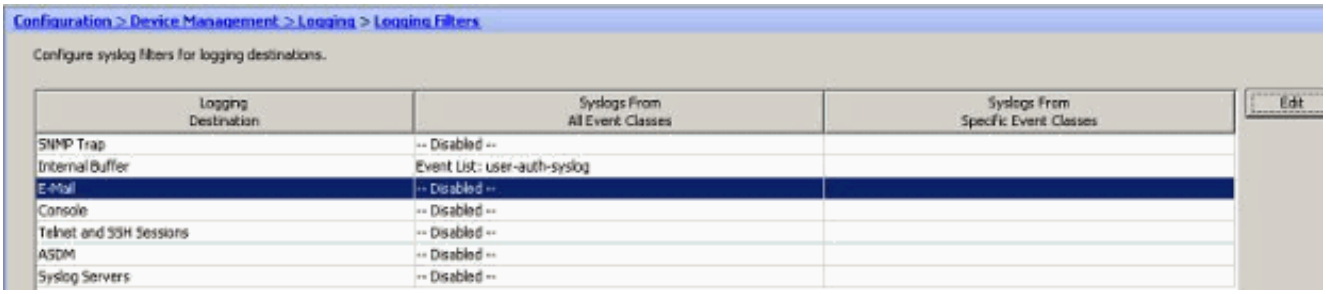
.



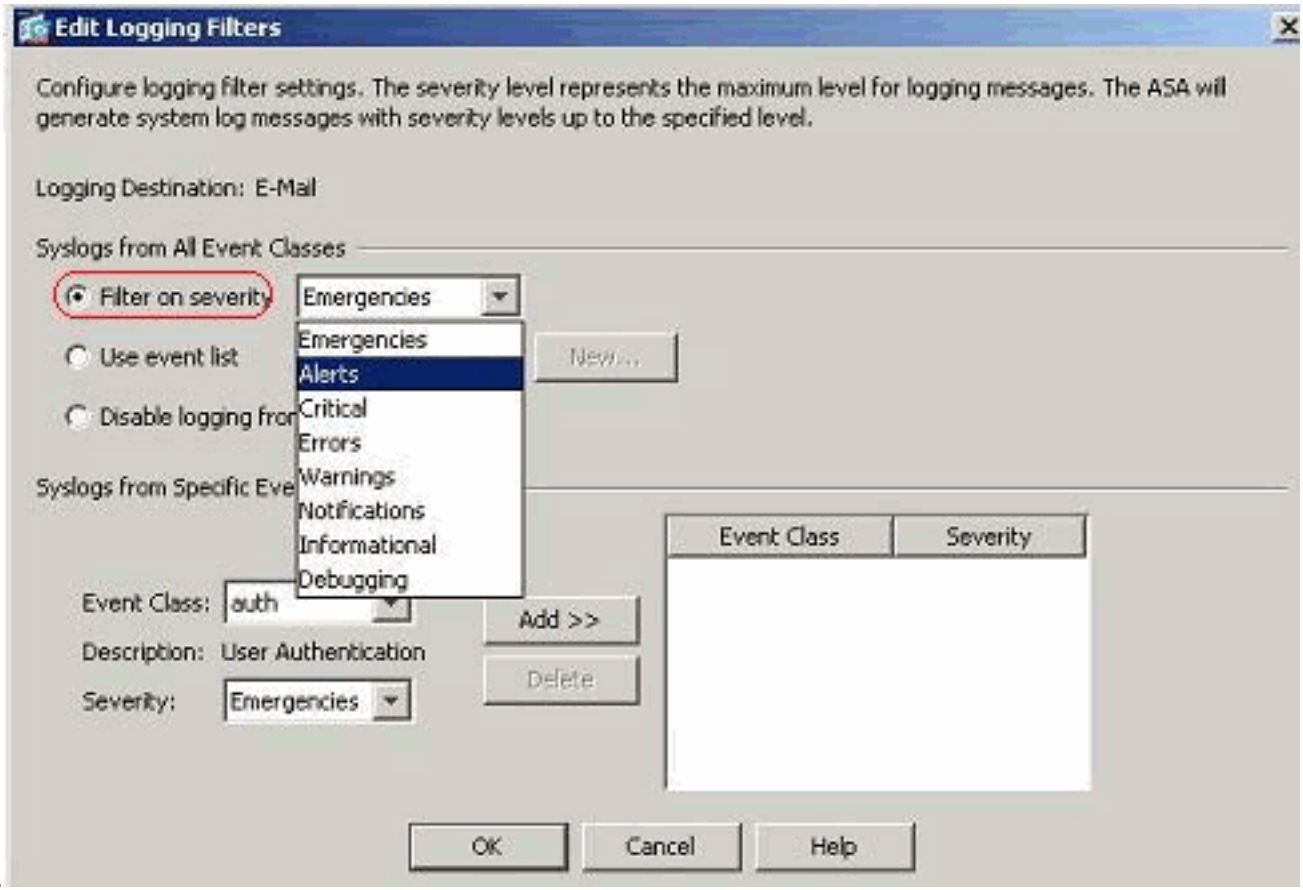
심각도 수준에 따라 메시지 그룹을 이메일 서버로 전송하는 방법에 대한 단계입니다.

1. Logging **Destination** 필드에서 Email을 선택합니다.그런 다음 **편집**을 클릭합니다

.



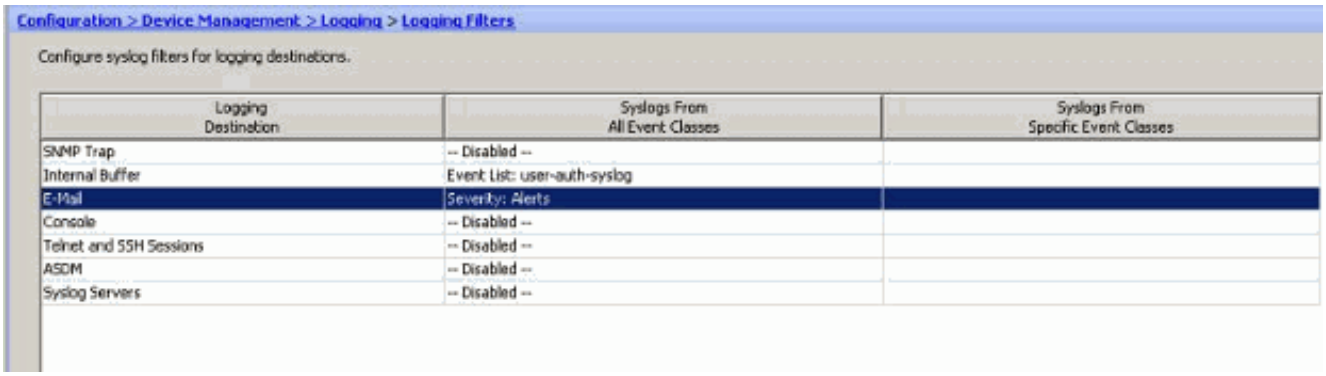
2. Filter **on severity**(심각도 **기준 필터링**) 옵션을 선택하고 필요한 심각도 수준을 선택합니다



.

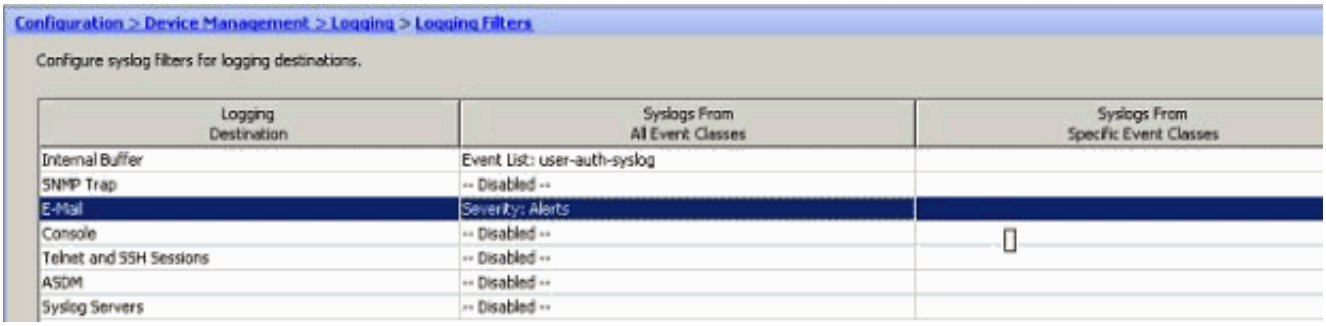
여기서 **Alerts**가 심각도 레벨로 선택되었습니다

.



모든 Alert syslog 메시지가 구성된 e-메일로 전송됨을 확인할 수 있습니다

.



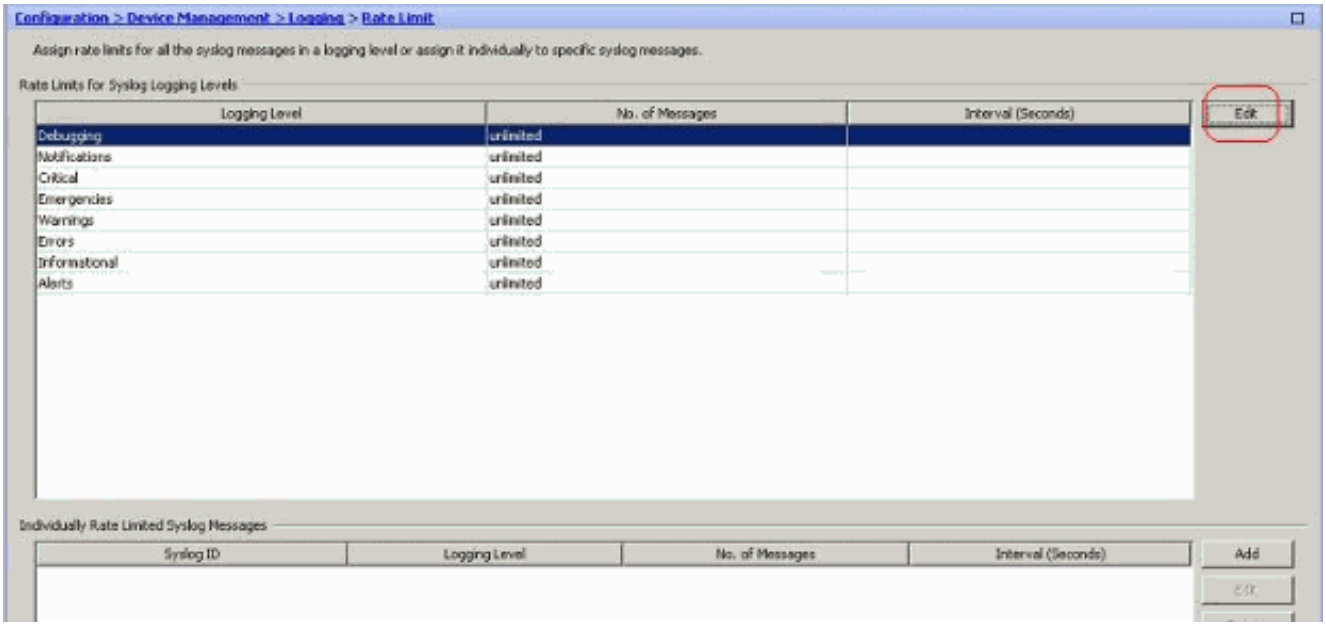
속도 제한

지정된 기간 동안 Cisco ASA가 대상에 전송하는 syslog 메시지의 수를 지정합니다.일반적으로 심각도 레벨에 대해 정의됩니다.

1. Configuration **> Device Management > Logging > Rate Limit**을 선택하고 필요한 심각도 수준

을 선택합니다.그런 다음 **편집**을 클릭합니다

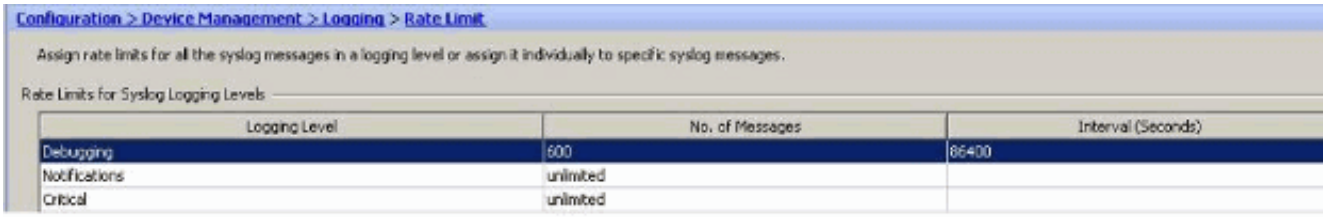
.



2. 시간 간격과 함께 보낼 메시지 수를 지정합니다.**확인**을 **클릭합니다**

참고: 이 수치는 예시로 제공됩니다 .이는 네트워크 환경의 유형에 따라 다릅니다.수정된 값은 다음과 같습니다

.

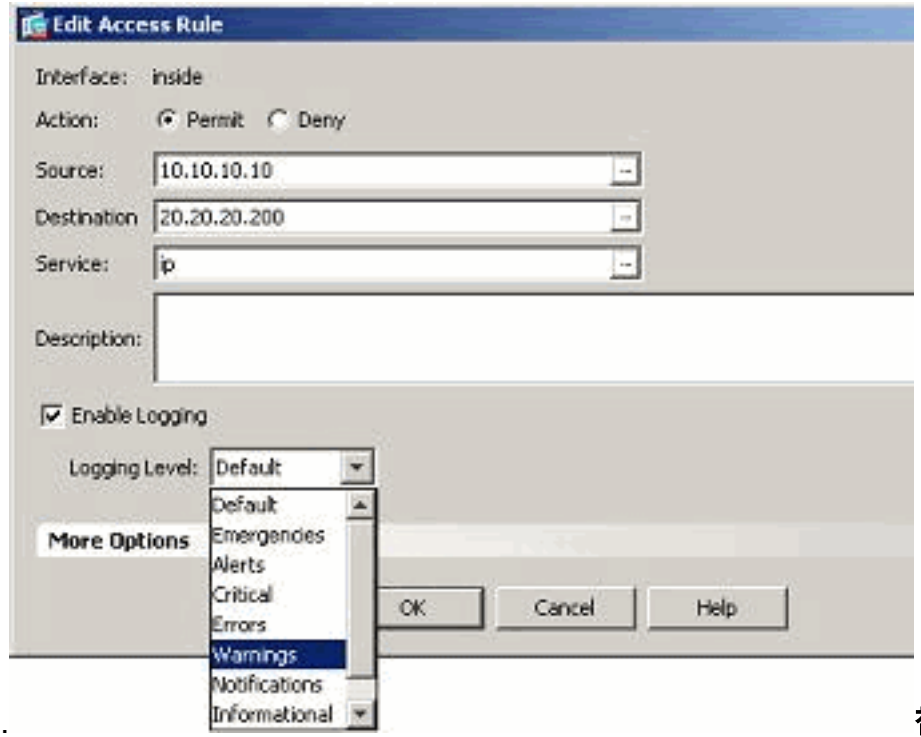


액세스 규칙의 적중 기록

ASDM을 사용하여 액세스 규칙 적중을 로깅할 수 있습니다.기본 로깅 동작은 거부된 모든 패킷에 대해 syslog 메시지를 보내는 것입니다.허용된 패킷에 대한 syslog 메시지가 없으며 로깅되지 않습니다.그러나 액세스 규칙에 대한 사용자 지정 로깅 심각도 수준을 정의하여 이 액세스 규칙에 일치하는 패킷의 수를 추적할 수 있습니다.

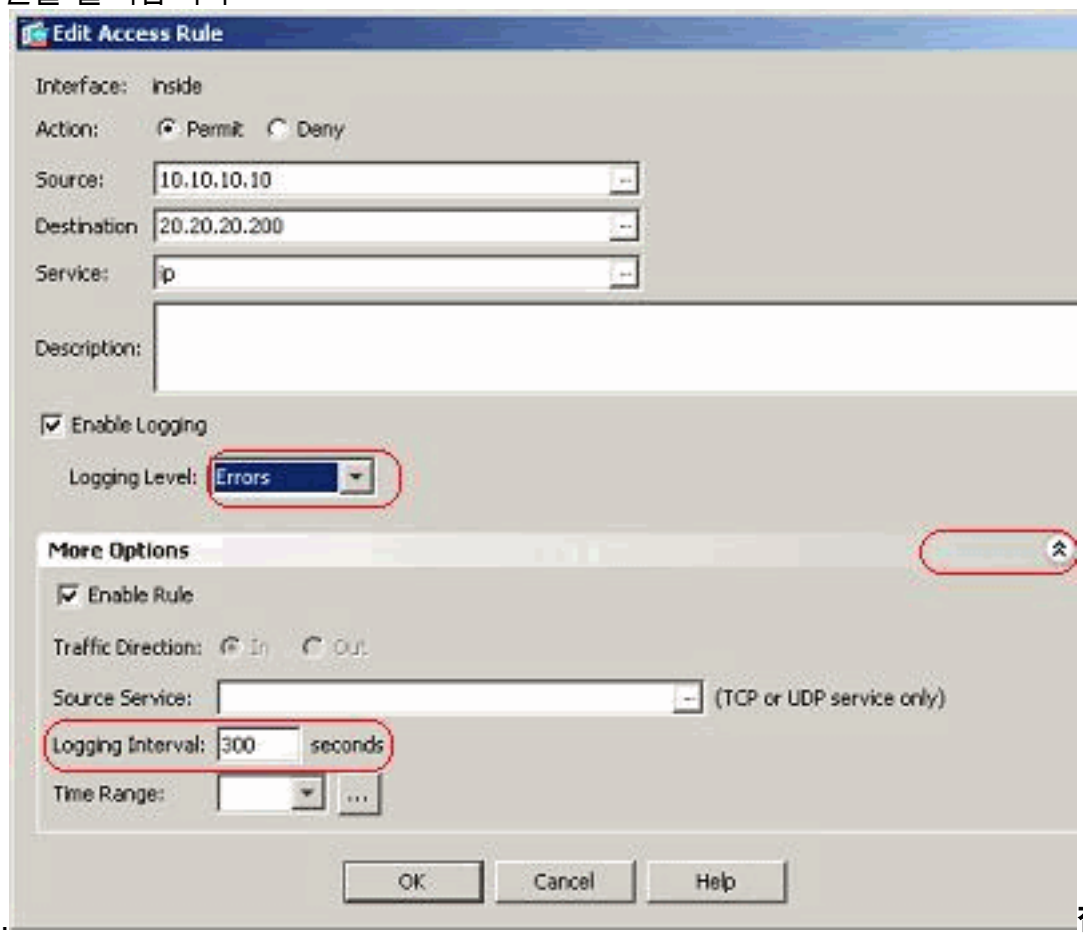
다음 단계를 수행합니다.

1. 필요한 액세스 규칙을 선택하고 Edit를 *클릭합니다*.Edit *the Access Rule* 창이 나타납니다



. **참고:** 이 이미지에서 Logging Level(로깅 *레벨*) 필드의 Default(기본) 옵션은 Cisco ASA의 기본 로깅 동작을 나타냅니다.이에 대한 자세한 내용은 Logging Access List Activity 섹션을 참조하십시오.

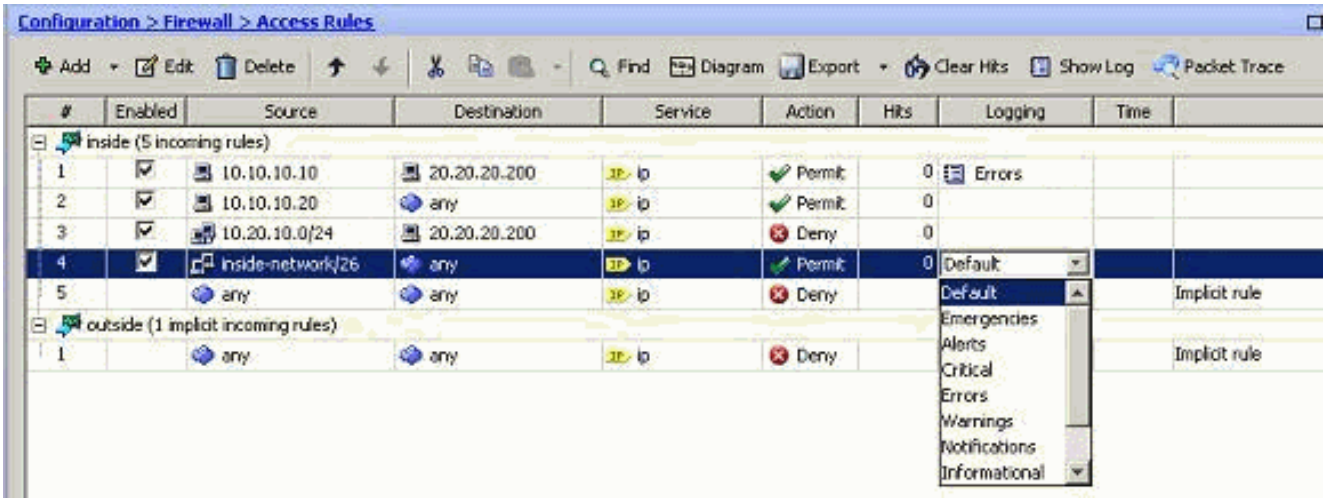
2. Enable logging(로깅 *활성화*) 옵션을 선택하고 필요한 심각도 수준을 지정합니다.그런 다음 *확인*을 클릭합니다



. **참고:** More *options* 드롭다운 탭을 클릭하면 *Logging Interval* 옵션을 볼 수 있습니다.이 옵션은 위의 *Enable Logging* 옵션이 선택된 경우에만 강조 표시됩니다.이 타이머의 기본값은 300초입니다.이 설정은 해당 액세스 규칙에 일치하는 항목이 없을 때 삭제될 flow-statistics에 대한 시간 제한 값을 지정하는 데 유용합니다.적중 사항이 있는 경우 ASA는 Logging Interval(로깅 간격) 시간 전까지 기다렸다가 syslog에 전송합니다.

3. 수정 사항이 여기에 표시됩니다.또는 특정 액세스 규칙의 *Logging* 필드를 두 번 클릭하고 심각도 수준을 설정할 수 있습니다

.



참고: 동일한 *액세스 규칙 창*에서 두 번을 눌러 로깅 *레벨*을 지정하는 대체 방법은 수동으로 생성된 액세스 규칙 항목에만 적용되지만 암시적 규칙에는 적용되지 않습니다.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

구성

이 문서에서는 다음 구성을 사용합니다.

CiscoASA

```
: Saved
:
ASA Version 8.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.0
!
interface Ethernet0/2
 nameif inside
```

```
 security-level 100
 ip address 10.78.177.11 255.255.255.192
!
!!--- Output Suppressed ! access-list inside_access_in
extended permit ip host 10.10.10.10 host 20.20.20.200
log errors
access-list inside_access_in extended permit ip host
10.10.10.20 any
access-list inside_access_in extended deny ip 10.20.10.0
255.255.255.0 host 20.20.20.200
access-list inside_access_in extended permit ip
10.78.177.0 255.255.255.192 any log emergencies
pager lines 24
logging enable
logging list user-auth-syslog level warnings class auth
logging list TCP-conn-syslog message 302013-302018
logging list syslog-sev-error level errors
logging list vpnclient-errors level errors class vpnc
logging list vpnclient-errors level errors class ssl
logging buffered user-auth-syslog
logging mail alerts
logging from-address test123@example.com
logging recipient-address monitorsyslog@example.com
level errors
logging queue 1024
logging host inside 172.16.11.100
logging ftp-bufferwrap
logging ftp-server 172.16.18.10 syslog testuser ****
logging permit-hostdown
no logging message 302015
no logging message 302016
logging rate-limit 600 86400 level 7
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-623.bin
asdm history enable
arp timeout 14400
!!--- Output Suppressed ! timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00
sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00 timeout sip-provisional-media 0:02:00 uauth
0:05:00 absolute timeout TCP-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy ! !---
Output Suppressed ! ! telnet timeout 5 ssh timeout 5
console timeout 0 threat-detection basic-threat threat-
detection statistics access-list no threat-detection
statistics TCP-intercept ! !--- Output Suppressed !
username test password /FzQ9W6s1KjC0YQ7 encrypted
privilege 15 ! ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global smtp-server 172.18.10.20
prompt hostname context
Cryptochecksum:ad941fe5a2bbea3d477c03521e931cf4
: end
```

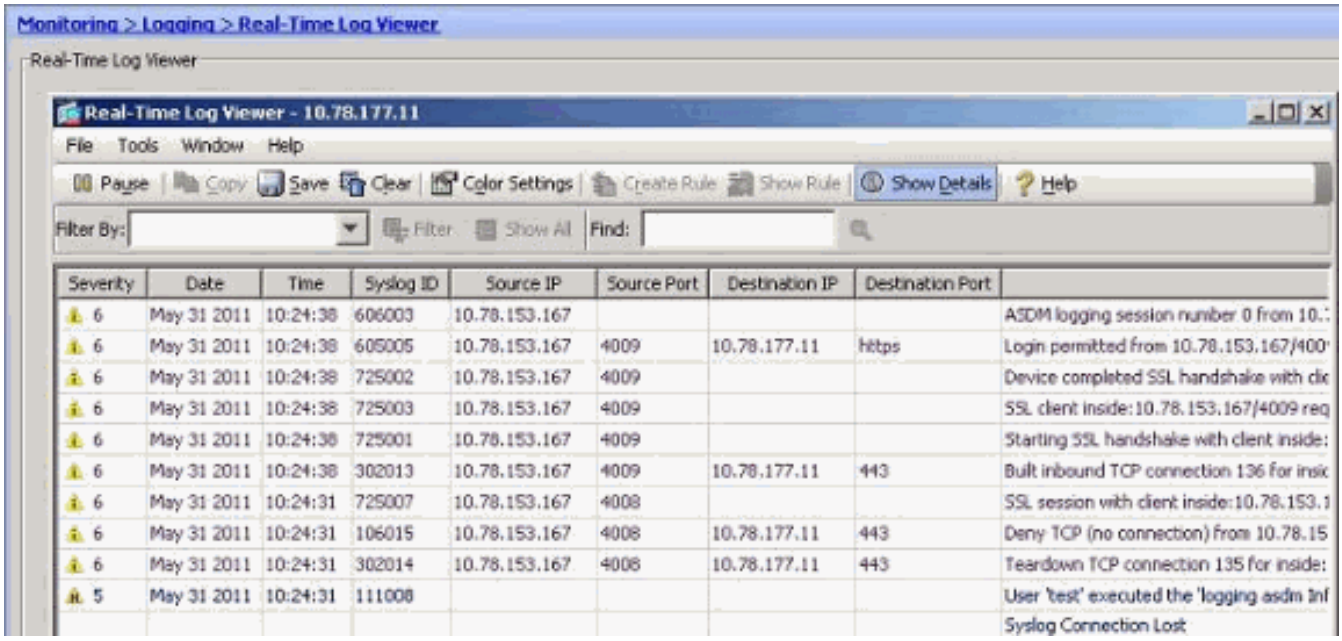
다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- ASDM에서 syslog를 볼 수 있습니다.Monitoring **> Logging > Real Time Log Viewer를 선택합니다**.샘플 출력은 다음과 같습니다

.



문제 해결

문제/장애:연결 손실 — Syslog 연결이 종료됨 —

모든 컨텍스트에 대해 디바이스 대시보드에서 ASDM 로깅을 활성화하려고 할 때 이 오류가 발생합니다.

```
"  – Syslog   –"
```

ASDM을 사용하여 관리 컨텍스트에 직접 연결하고 ADSM 로깅이 비활성화된 경우 하위 컨텍스트로 전환하고 ASDM 로깅을 활성화합니다.오류가 수신되지만 syslog 메시지는 syslog 서버에 거의 영향을 미치지 않습니다.

솔루션

이는 Cisco ASDM의 알려진 동작이며 Cisco 버그 ID CSCsd10699에 문서화되어 있습니다(등록된 고객만 해당). 이를 해결하려면 관리자 컨텍스트에 로그인할 때 asdm 로깅을 활성화합니다.

Cisco ASDM에서 실시간 로그를 볼 수 없음

문제는 ASDM에서 실시간 로그를 볼 수 없다는 것입니다.어떻게 구성됩니까?

솔루션

Cisco ASA에서 다음을 구성합니다.

```
ciscoasa(config)#logging monitor 6
ciscoasa(config)#terminal monitor
ciscoasa(config)#logging on
ciscoasa(config)#logging trap 6
```

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliances 지원
- 기술 지원 및 문서 – Cisco Systems