FMC를 통해 FTD에 로깅 구성

목차

소개

이 문서에서는 Firepower Management Center(FMC)를 통한 FirePOWER Threat Defense(FTD)의 로깅 설정을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower 기술
- ASA(Adaptive Security Appliance)
- Syslog 프로토콜

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 6.0.1 이상을 실행하는 ASA(5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X)용 ASA Firepower 위협 방어 이미지

- 소프트웨어 버전 6.0.1 이상을 실행하는 ASA(5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X)용 ASA Firepower Threat Defense 이미지
- FMC 버전 6.0.1 이상

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.

배경 정보

FTD 시스템 로그는 FTD 어플라이언스를 모니터링하고 문제를 해결하기 위한 정보를 제공합니다.

로그는 일상적인 트러블슈팅 및 인시던트 처리에 모두 유용합니다. FTD 어플라이언스는 로컬 및 외부 로깅을 모두 지원합니다.

로컬 로깅을 통해 실시간 문제를 해결할 수 있습니다. 외부 로깅은 FTD 어플라이언스에서 외부 Syslog 서버로 로그를 수집하는 방법입니다.

중앙 서버에 로깅하면 로그와 경고를 종합하는 데 도움이 됩니다. 외부 로깅은 로그 상관관계 및 인시던트 처리에 도움이 될 수 있습니다.

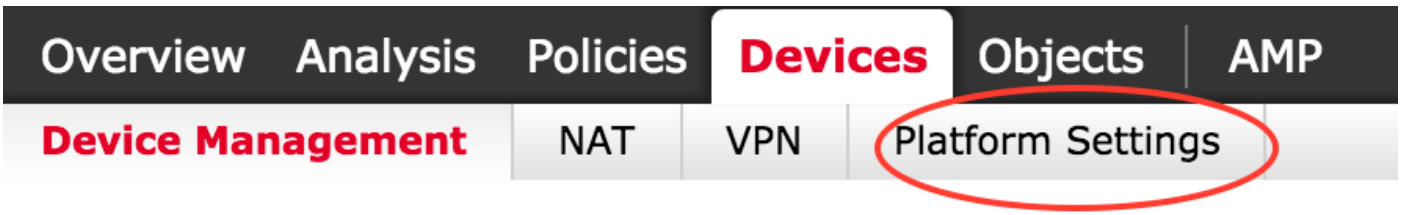
로컬 로깅의 경우 FTD 어플라이언스는 콘솔, 내부 버퍼 옵션 및 SSH(Secure Shell) 세션 로깅을 지원합니다.

외부 로깅의 경우 FTD 어플라이언스는 외부 Syslog 서버 및 이메일 릴레이 서버를 지원합니다.

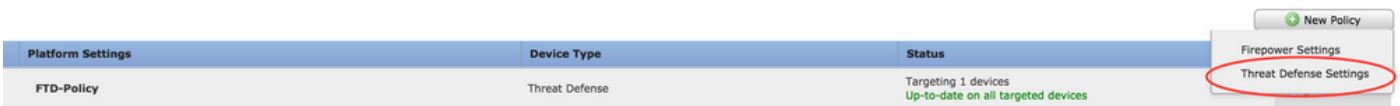
참고: 많은 양의 트래픽이 어플라이언스를 통과하는 경우 로깅/심각도/속도 제한 유형에 유의하십시오. 로그 수를 제한하여 방화벽에 영향을 주지 않도록 하려면 이 작업을 수행합니다.

구성

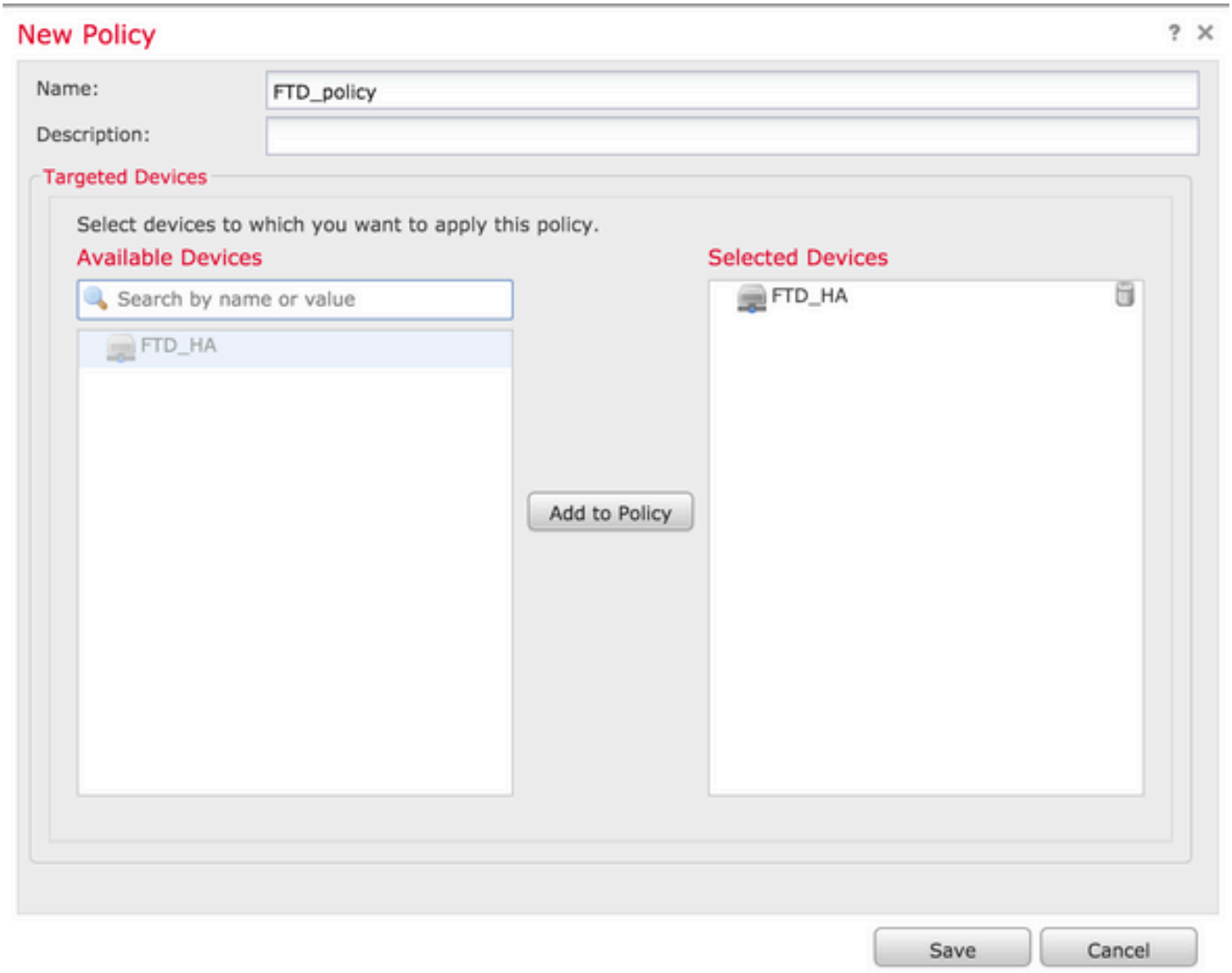
모든 로깅 관련 컨피그레이션은 해당 탭 아래의 탭으로 Platform Settings 이동할 때 구성할 수 Devices 있습니다. 이 이미지Devices > Platform Settings 에 표시된 대로 선택합니다.



존재하는 정책을 수정하려면 연필 아이콘을 클릭하고, 이 이미지 **New Policy**에 표시된 대로 새 FTD 정책 **Threat Defense Settings**을 생성하려면 를 클릭합니다.



이 정책을 적용할 FTD 어플라이언스를 선택하고 이 이미지 **Save** 에 표시된 대로 클릭합니다.



전역 Syslog 구성

로컬 및 외부 로깅에 모두 적용할 수 있는 특정 컨피그레이션이 있습니다. 이 섹션에서는 Syslog에 대해 구성할 수 있는 필수 및 선택적 매개변수에 대해 설명합니다.

로깅 설정

로깅 설정 옵션은 로컬 및 외부 로깅에 적용됩니다. 로깅 설정을 구성하려면 을 선택합니다 **Devices** > **Platform Settings**.

를 **Syslog** > **Logging Setup**선택합니다.

기본 로깅 설정

- Enable Logging: 로깅을 **Enable Logging** 활성화하려면 확인란을 선택합니다. 이는 필수 옵션입니다.
- Enable Logging on the failover standby unit: FTD **Enable Logging on the failover standby unit** 고가용성 클러스터의 일부인 대기 FTD에서 로깅을 구성하려면 확인란을 선택합니다.

- Send syslogs in EMBLEM format: 모든 **Send syslogs in EMBLEM format** 대상에 대해 Syslog as EMBLEM 형식을 활성화하려면 확인란을 선택합니다. EMBLEM 형식은 주로 CiscoWorks RME(Resource Manager Essentials) Syslog 분석기에 사용됩니다. 이 형식은 라우터 및 스위치에서 생성된 Cisco IOS Software Syslog 형식과 일치합니다. UDP Syslog 서버에서만 사용할 수 있습니다.

- Send debug messages as syslogs: 디버그 **Send debug messages as syslogs** 로그를 Syslog 서버로 Syslog 메시지로 전송하려면 확인란을 선택합니다.

- Memory size of the Internal Buffer: FTD가 로그 데이터를 저장할 수 있는 내부 메모리 버퍼 크기를 입력합니다. 로그 데이터는 해당 버퍼 제한에 도달하면 회전됩니다.

FTP 서버 정보(선택 사항)

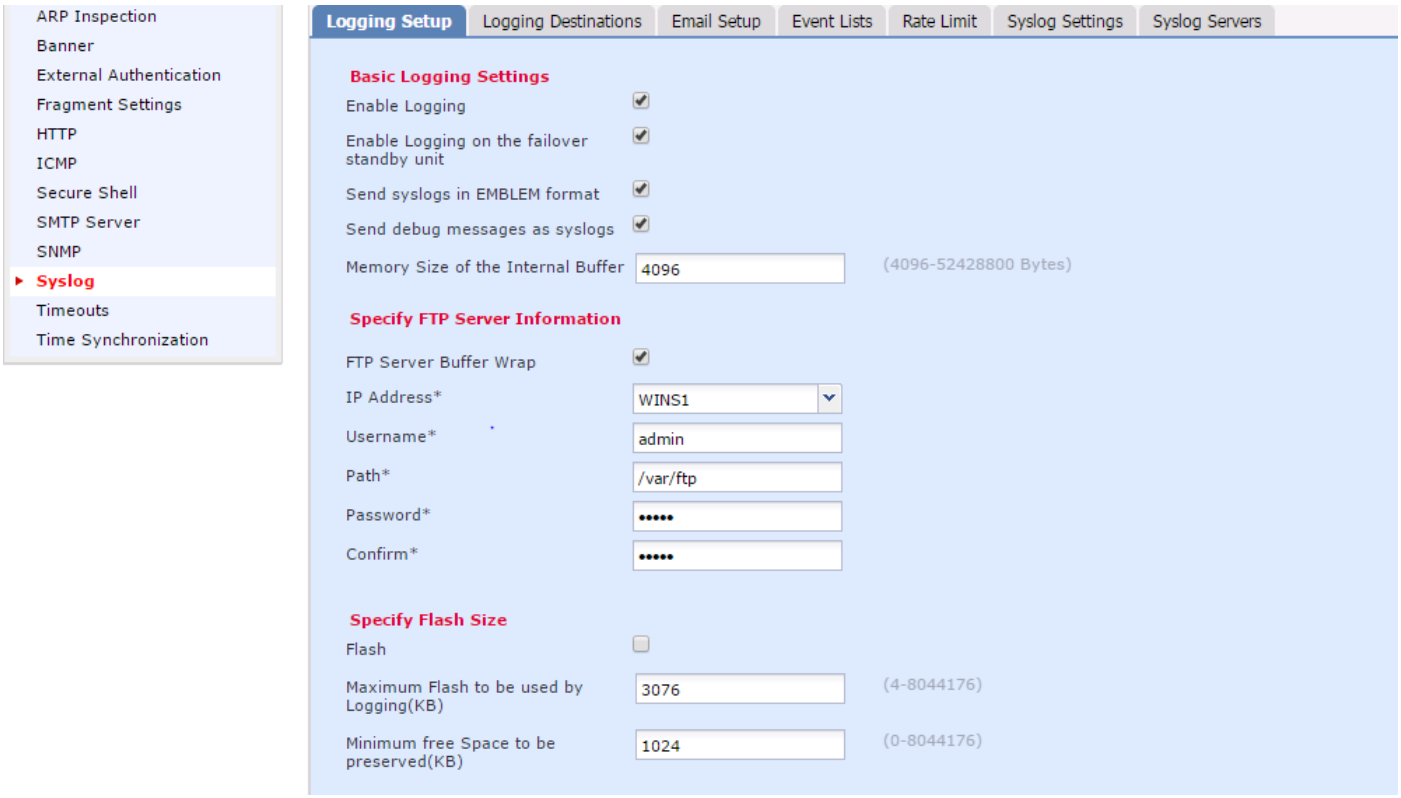
내부 버퍼를 덮어쓰기 전에 로그 데이터를 FTP 서버로 전송하려면 FTP 서버 세부 정보를 지정합니다.

- FTP Server Buffer Wrap: 버퍼 로그 **FTP Server Buffer Wrap** 데이터를 FTP 서버로 전송하려면 확인란을 선택합니다.
- IP Address: FTP 서버의 IP 주소를 입력합니다.
- Username: FTP 서버의 사용자 이름을 입력합니다.
- Path: FTP 서버의 디렉토리 경로를 입력합니다.
- Password: FTP 서버의 비밀번호를 입력합니다.
- Confirm: 동일한 비밀번호를 다시 입력합니다.

플래시 크기(선택 사항)

내부 버퍼가 가득 차면 로그 데이터를 플래시에 저장하려면 플래시 크기를 지정합니다.

- Flash: 로그 **Flash** 데이터를 내부 플래시로 전송하려면 확인란을 선택합니다.
- Maximum Flash to be used by Logging(KB): 로깅에 사용할 수 있는 플래시 메모리의 최대 크기(KB)를 입력합니다.
- Minimum free Space to be preserved(KB): 보존해야 하는 플래시 메모리의 최소 크기(KB)를 입력합니다.



플랫폼 설정 **Save** 을 저장하려면 를 클릭합니다. 옵션 **Deploy** 을 선택하고 변경 사항을 적용할 FTD 어플라이언스를 선택한 다음 플랫폼 설정 **Deploy** 의 구축을 시작하려면 을 클릭합니다.

이벤트 목록

Configure Event Lists 옵션을 사용하면 이벤트 목록을 생성/편집하고 이벤트 목록 필터에 포함할 로그 데이터를 지정할 수 있습니다. Logging destinations(로깅 대상)에서 Logging Filters(로깅 필터)를 구성할 때 Event Lists(이벤트 목록)를 사용할 수 있습니다.

시스템에서는 두 가지 옵션에서 사용자 지정 이벤트 목록의 기능을 사용할 수 있습니다.

- 클래스 및 심각도
- 메시지 ID

사용자 지정 이벤트 목록을 구성하려면 을 선택하고 **Device** > **Platform Setting** > **Threat Defense Policy** > **Syslog** > **Event List** 을 클릭합니다 **Add**. 다음 옵션을 사용할 수 있습니다.

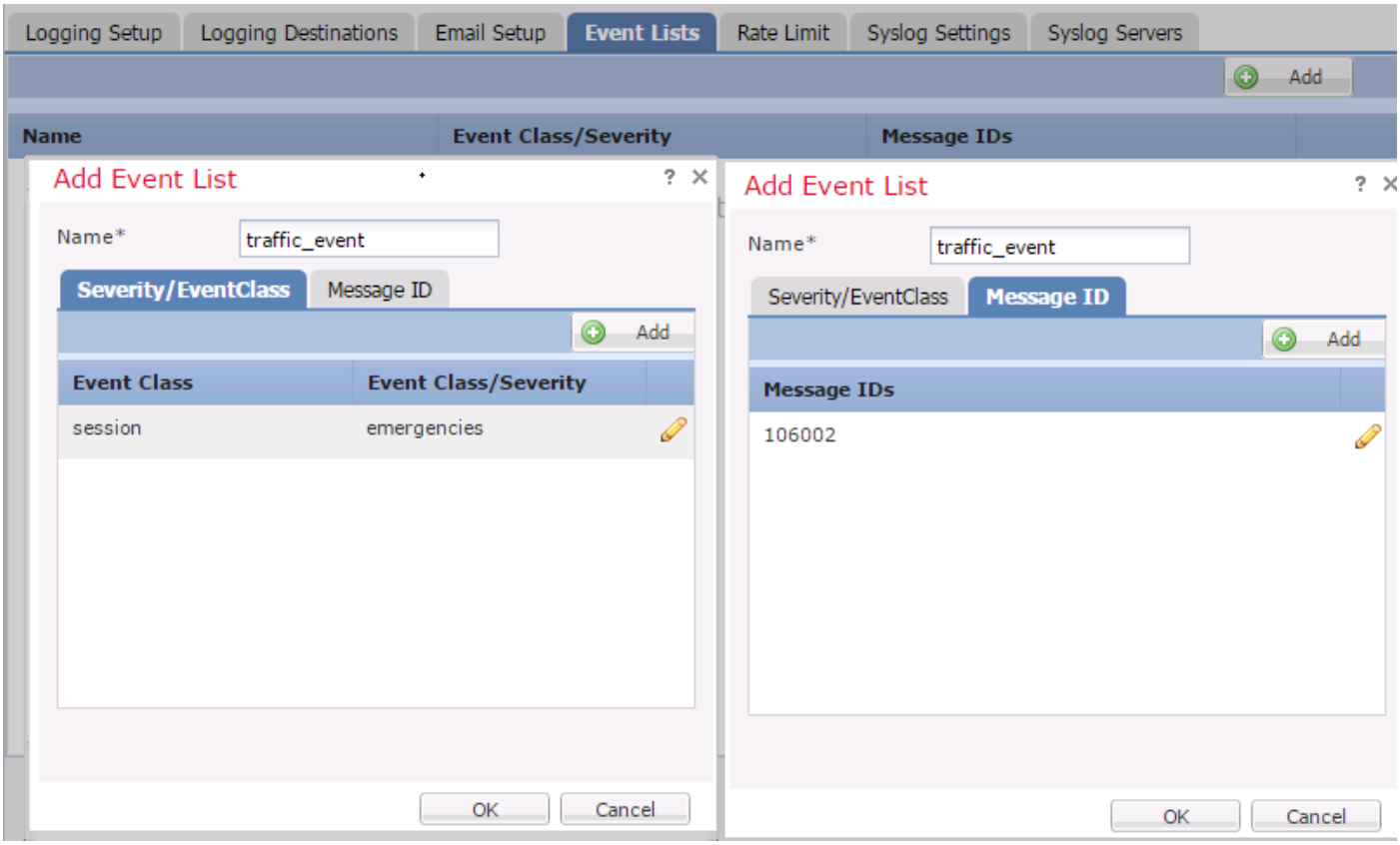
- Name: 이벤트 목록의 이름을 입력합니다.
- Severity/Event Class: Severity/Event Class(심각도/이벤트 클래스) 섹션에서 을 **Add**클릭합니다.
- Event Class: 드롭다운 목록에서 원하는 로그 데이터 유형에 대한 이벤트 클래스를 선택합니다. 이벤트 클래스는 동일한 기능을 나타내는 Syslog 규칙 집합을 정의합니다.

예를 들어 세션과 관련된 모든 Syslog를 포함하는 세션에 대한 Event Class가 있습니다.

- Syslog Severity: 선택한 이벤트 클래스의 드롭다운 목록에서 심각도를 선택합니다. 심각도의 범위는 0(긴급)에서 7(디버깅)까지입니다.

- Message ID: 메시지 ID와 관련된 특정 로그 데이터에 관심이 있는 경우 메시지 ID **Add** 에 따라 필터를 추가하려면 을 클릭합니다.

- Message IDs: 메시지 ID를 개별/범위 형식으로 지정합니다.



컨피그레이션 **OK** 을 저장하려면 를 클릭합니다.

플랫폼 설정 **Save** 을 저장하려면 를 클릭합니다. 변경 **Deploy**사항을 적용할 FTD 어플라이언스를 선택하고 를 클릭하여 플랫폼 설정 **Deploy**의 구축을 시작합니다.

속도 제한 Syslog

Rate limit(속도 제한) 옵션은 구성된 모든 대상에 전송할 수 있는 메시지 수를 정의하고 속도 제한을 할당할 메시지의 심각도를 정의합니다.

사용자 지정 이벤트 목록을 구성하려면 을 선택합니다 **Device** > **Platform Setting** > **Threat Defense Policy** > **Syslog** > **Rate Limit**. 속도 제한을 지정할 수 있는 두 가지 옵션이 있습니다.

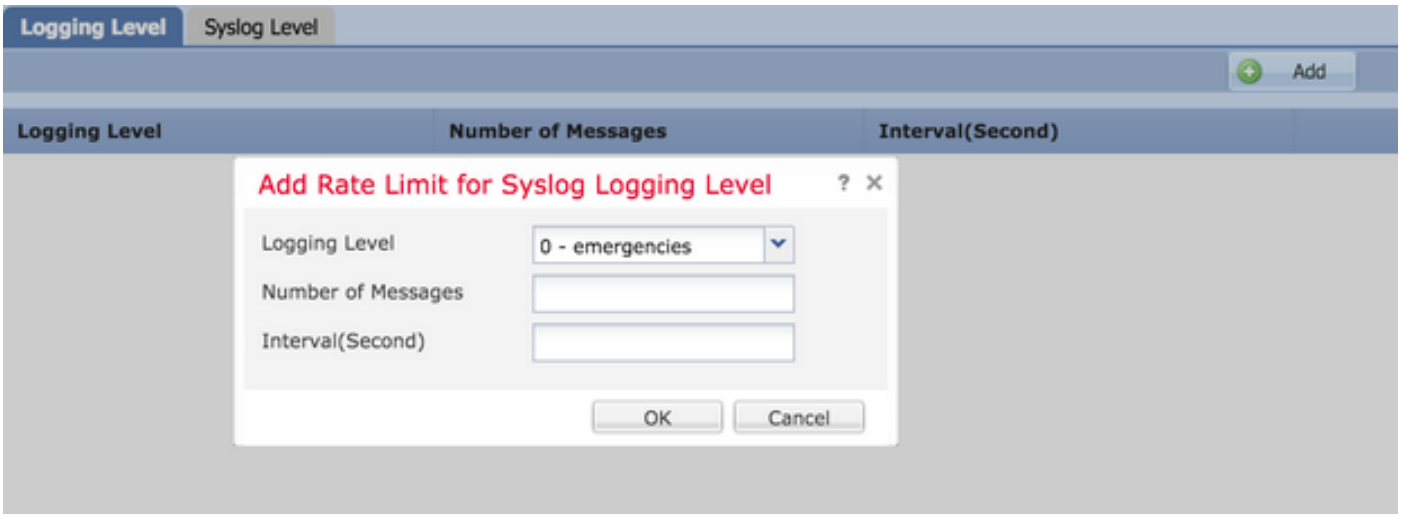
- Logging Level(로깅 레벨)

- Syslog 레벨

로깅 레벨 기반 속도 제한을 활성화하려면 을 선택하고 **Logging Level** 을 클릭합니다 **Add**.

- Logging Level: **Logging Level** 드롭다운 목록에서 속도 제한을 수행할 로깅 레벨을 선택합니다.
- Number of Messages: 지정된 간격 내에 수신할 최대 Syslog 메시지 수를 입력합니다.
- Interval(Second): 이전에 구성된 Number of Messages(메시지 수) 매개변수에 따라 고정 Syslog 메시지 집합을 수신할 수 있는 시간 간격을 입력합니다.

Syslog의 속도는 메시지/간격의 수입니다.

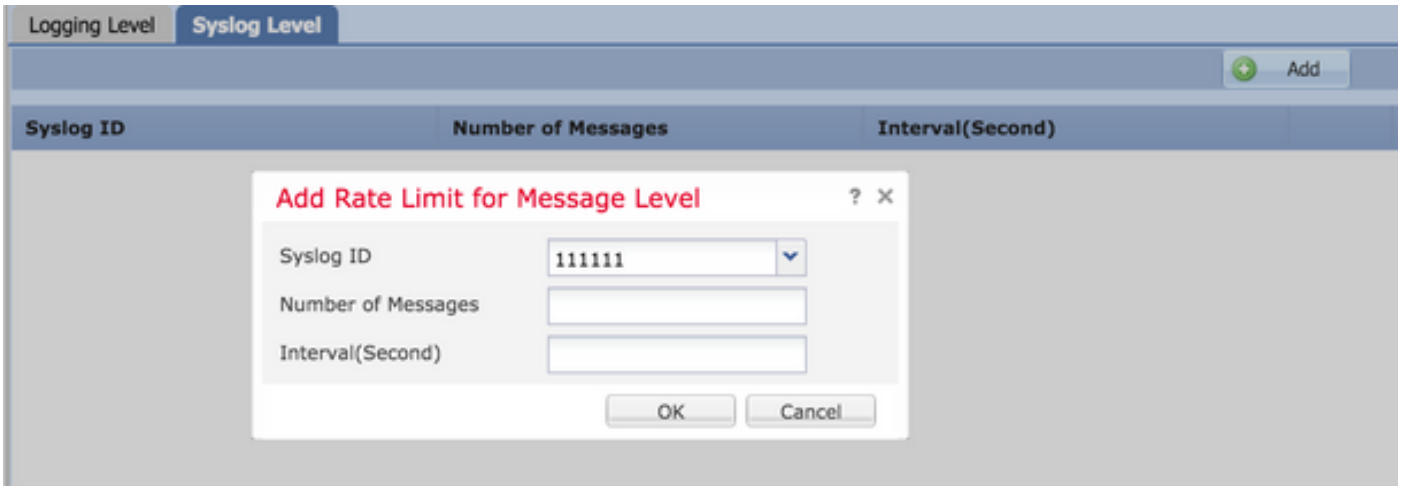


로깅 레벨 컨피그레이션 **OK** 을 저장하려면 를 클릭합니다.

로깅 레벨 기반 속도 제한을 활성화하려면 을 선택하고 **Logging Level** 을 클릭합니다 **Add**.

- Syslog ID: Syslog ID는 Syslog 메시지를 고유하게 식별하는 데 사용됩니다. 드롭다운 **Syslog ID** 목록에서 Syslog ID를 선택합니다.
- Number of Messages: 지정된 간격 내에 수신할 최대 syslog 메시지 수를 입력합니다.
- Interval(Second): 이전에 구성된 Number of Messages(메시지 수) 매개변수에 따라 고정 Syslog 메시지 집합을 수신할 수 있는 시간 간격을 입력합니다.

Syslog의 속도는 메시지 수/간격입니다.



Syslog 레벨 컨피그레이션 **OK** 을 저장하려면 를 클릭합니다.

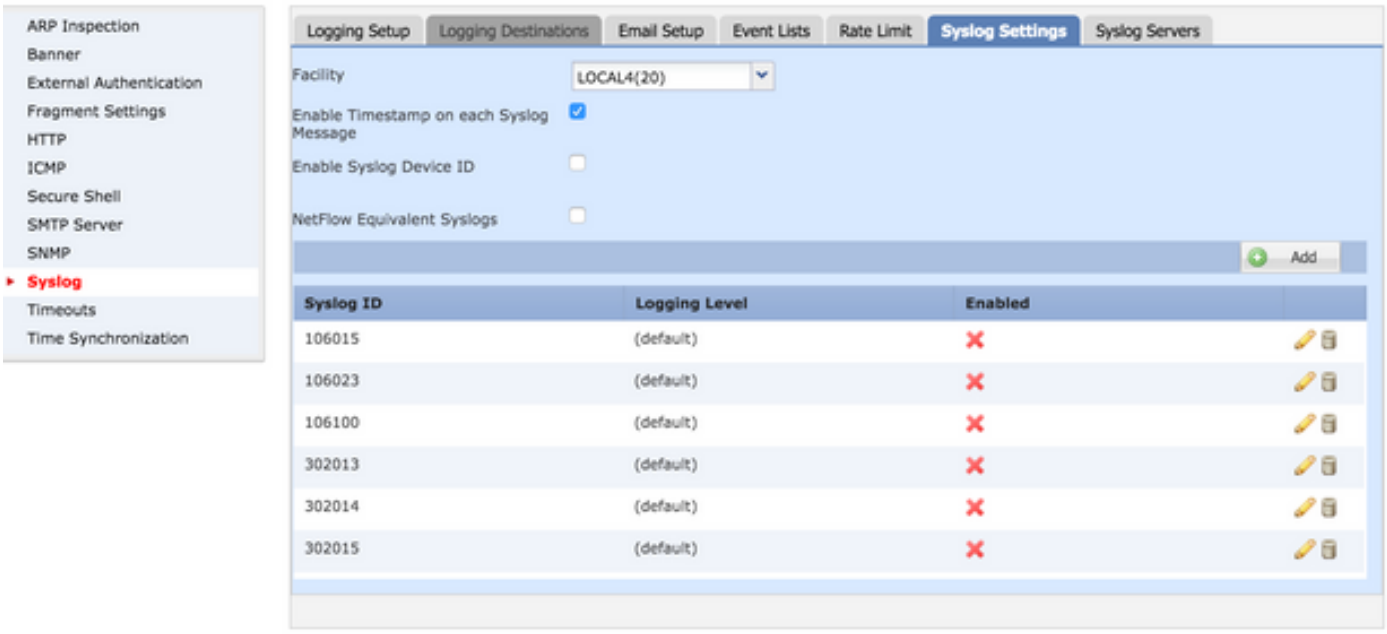
플랫폼 설정 **Save** 을 저장하려면 를 클릭합니다. 변경 **Deploy**사항을 적용할 FTD 어플라이언스를 선택하고 를 클릭하여 플랫폼 설정 **Deploy** 의 구축을 시작합니다.

Syslog 설정

Syslog 설정을 사용하면 Facility(기능) 값을 Syslog 메시지에 포함할 수 있습니다. 또한 로그 메시지 및 기타 Syslog 서버 관련 매개변수에 타임스탬프를 포함할 수 있습니다.

사용자 지정 이벤트 목록을 구성하려면 을 선택합니다 **Device** > **Platform Setting** > **Threat Defense Policy** > **Syslog** > **Syslog Settings**.

- Facility: 기능 코드는 메시지를 로깅하는 프로그램의 유형을 지정하는 데 사용됩니다. 기능이 다른 메시지는 다르게 처리할 수 있습니다. 드롭다운 **Facility** 목록에서 기능 값을 선택합니다.
- Enable Timestamp on each Syslog Message: Syslog **Enable Timestamp on each Syslog Message** 메시지에 타임스탬프를 포함하려면 확인란을 선택합니다.
- Enable Syslog Device ID: 비 EMBLEM **Enable Syslog Device ID** 형식 Syslog 메시지에 디바이스 ID를 포함하려면 확인란을 선택합니다.
- Netflow Equivalent Syslogs: NetFlow에 **Netflow Equivalent Syslogs** 해당하는 Syslog를 전송하려면 확인란을 선택합니다. 어플라이언스의 성능에 영향을 미칠 수 있습니다.
- Add Specific Syslog ID(특정 Syslog ID 추가): 추가 Syslog ID를 지정하려면 **Add** 확인란을 클릭하고 **Syslog ID/ Logging Level** 지정합니다.



플랫폼 설정 **Save** 을 저장하려면 를 클릭합니다. 변경 **Deploy**사항을 적용할 FTD 어플라이언스를 선택하고 를 클릭하여 플랫폼 설정 **Deploy** 의 구축을 시작합니다.

로컬 로깅 구성

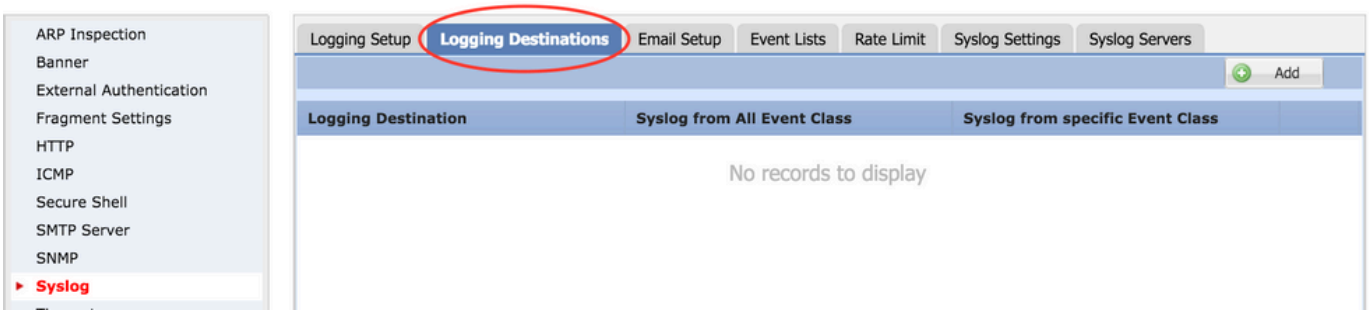
Logging Destination 섹션에서는 특정 대상에 대한 로깅을 구성할 수 있습니다.

사용 가능한 내부 로깅 대상은 다음과 같습니다.

- Internal Buffer(내부 버퍼): 내부 로깅 버퍼에 기록합니다(로깅 버퍼됨).
- Console: 콘솔(로깅 콘솔)로 로그를 보냅니다.
- SSH 세션: SSH 세션에 Syslog 기록(터미널 모니터)

Local Logging(로컬 로깅)을 구성하는 세 단계는 다음과 같습니다.

1단계. 를 **Device** > **Platform Setting** > **Threat Defense Policy** > **Syslog** > **Logging Destinations**선택합니다.



2단계. 특정 **Add** 에 대한 로깅 필터를 추가하려면 를 클릭합니다 **logging destination**.

Logging Destination(로깅 대상): **Logging Destination** 드롭다운 목록에서 필요한 로깅 대상을 Internal Buffer, Console 또는 SSH 세션으로 선택합니다.

Event Class(이벤트 클래스): **Event Class** 드롭다운 목록에서 이벤트 클래스를 선택합니다. 앞에서 설명한 것처럼 Event Classes(이벤트 클래스)는 동일한 기능을 나타내는 Syslog 집합입니다. 이벤트 클래스는 다음과 같은 방법으로 선택할 수 있습니다.

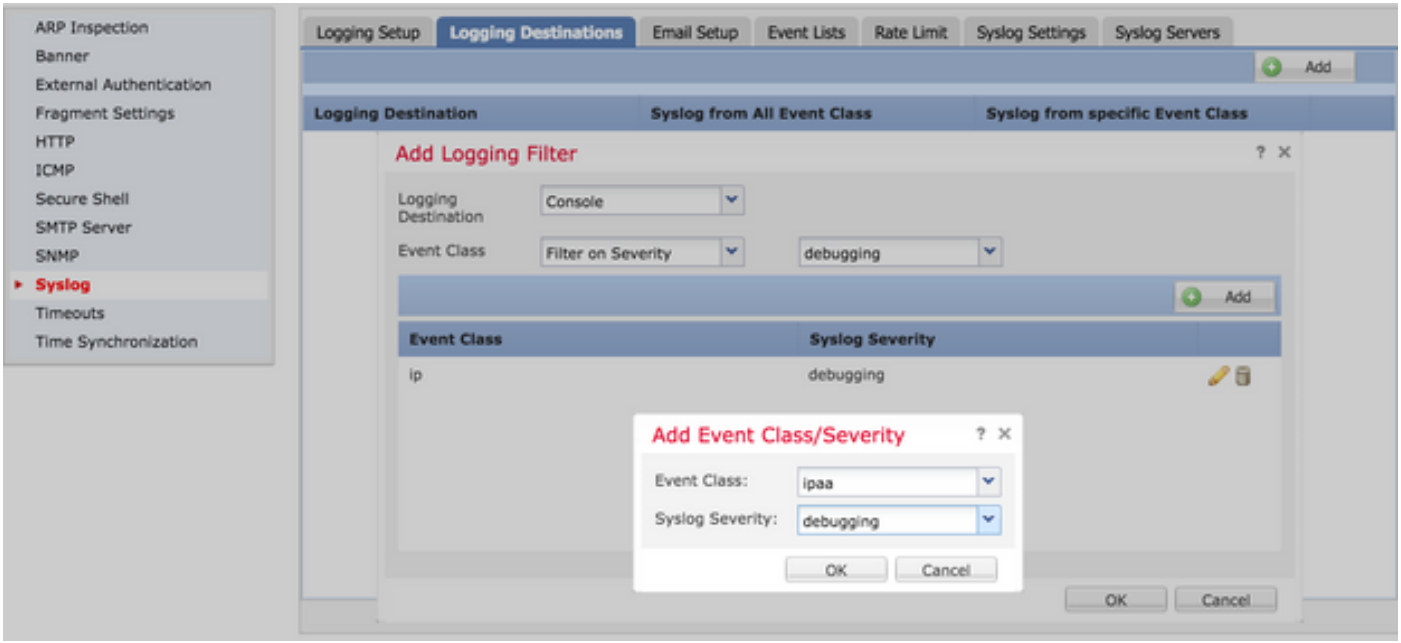
- Filter on Severity: 이벤트 클래스는 Syslog의 심각도를 기반으로 필터링합니다.
- User Event List: 관리자는 고유한 사용자 지정 이벤트 클래스를 사용하여 특정 이벤트 목록(이전에 설명됨)을 만들고 이 섹션에서 이를 참조할 수 있습니다.
- Disable Logging: 선택한 로깅 대상 및 로깅 레벨에 대한 로깅을 비활성화하려면 이 옵션을 사용합니다.

로깅 레벨: 드롭다운 목록에서 로깅 레벨을 선택합니다. 로깅 레벨 범위는 0(긴급)에서 7(디버깅)까지입니다.

3단계. 이 로깅 필터에 별도의 이벤트 클래스를 추가하려면 를 **Add**클릭합니다.

Event Class: **Event Class** 드롭다운 목록에서 Event Class를 선택합니다.

Syslog Severity: **Syslog Severity** 드롭다운 목록에서 Syslog 심각도를 선택합니다.



특정 로깅 대상에 대한 필터를 추가하도록 필터가 구성된 **OK** 후 클릭합니다.

플랫폼 설정 **Save** 을 저장하려면 를 클릭합니다. 변경 **Deploy**사항을 적용할 FTD 어플라이언스를 선택하고 플랫폼 설정 구축 **Deploy** 을 시작하려면 를 클릭합니다.

외부 로깅 구성

외부 로깅을 구성하려면 을 선택합니다 **Device** > **Platform Setting** > **Threat Defense Policy** > **Syslog** > **Logging Destinations**.

FTD는 이러한 유형의 외부 로깅을 지원합니다.

- Syslog 서버: 원격 Syslog 서버에 로그를 보냅니다.
- SNMP 트랩: 로그를 SNMP 트랩으로 보냅니다.
- E-Mail(이메일): 사전 구성된 메일 릴레이 서버를 사용하여 이메일을 통해 로그를 보냅니다.

외부 로깅과 내부 로깅의 컨피그레이션은 동일합니다. 로깅 대상을 선택하면 구현되는 로깅 유형이 결정됩니다. 원격 서버에 대한 사용자 지정 이벤트 목록을 기반으로 이벤트 클래스를 구성할 수 있습니다.

원격 Syslog 서버

FTD에서 원격으로 로그를 분석하고 저장하도록 Syslog 서버를 구성할 수 있습니다.

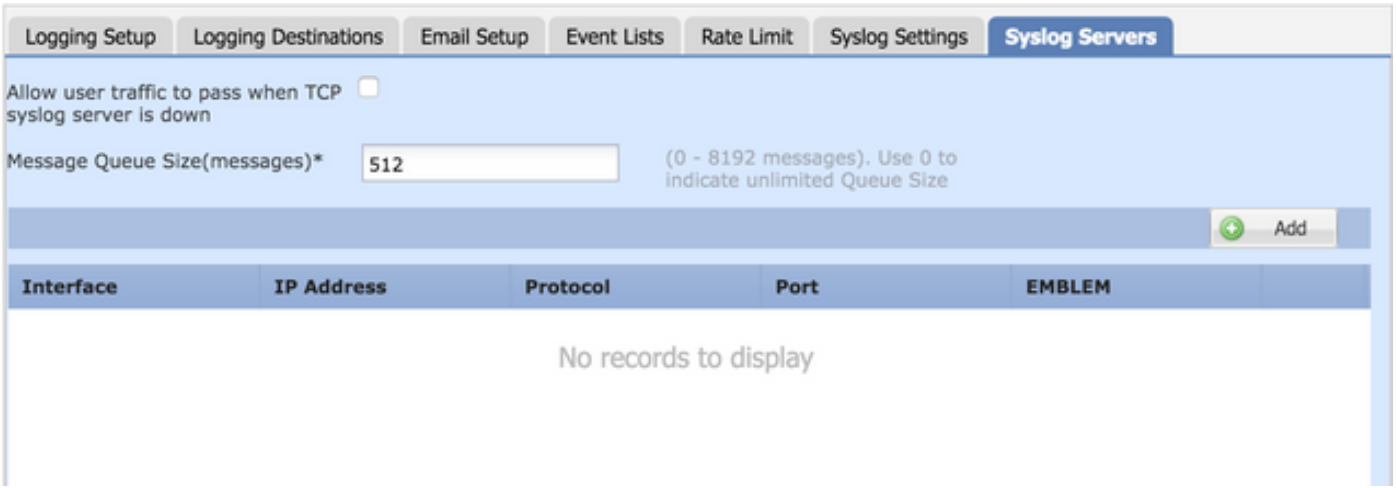
원격 Syslog 서버를 구성하는 세 단계는 다음과 같습니다.

1단계. 를 **Device** > **Platform Setting** > **Threat Defense Policy** > **Syslog** > **Syslog Servers**선택합니다.

2단계. Syslog 서버 관련 매개변수를 구성합니다.

- Allow user traffic to pass when TCP syslog server is down(TCP syslog 서버가 다운되었을 때 사용자 트래픽 전달 허용): TCP Syslog 서버가 네트워크에 구축되었지만 도달할 수 없는 경우 ASA를 통과하는 네트워크 트래픽은 거부됩니다. 이는 ASA와 Syslog 서버 간의 전송 프로토콜이 TCP인 경우에만 적용됩니다. Syslog **Allow user traffic to pass when TCP syslog server is down** 서버가 다운되었을 때 트래픽이 인터페이스를 통과하도록 허용하려면 확인란을 선택합니다.

- 메시지 큐 크기: 메시지 큐 크기는 원격 Syslog 서버가 사용 중일 때 FTD에서 대기하며 로그 메시지를 수락하지 않는 메시지 수입니다. 기본값은 512개 메시지이며 최소값은 1개 메시지입니다. 이 옵션에 0을 지정하면 큐 크기가 무제한으로 간주됩니다.



3단계. 원격 Syslog 서버를 추가하려면 를 **Add**클릭합니다.

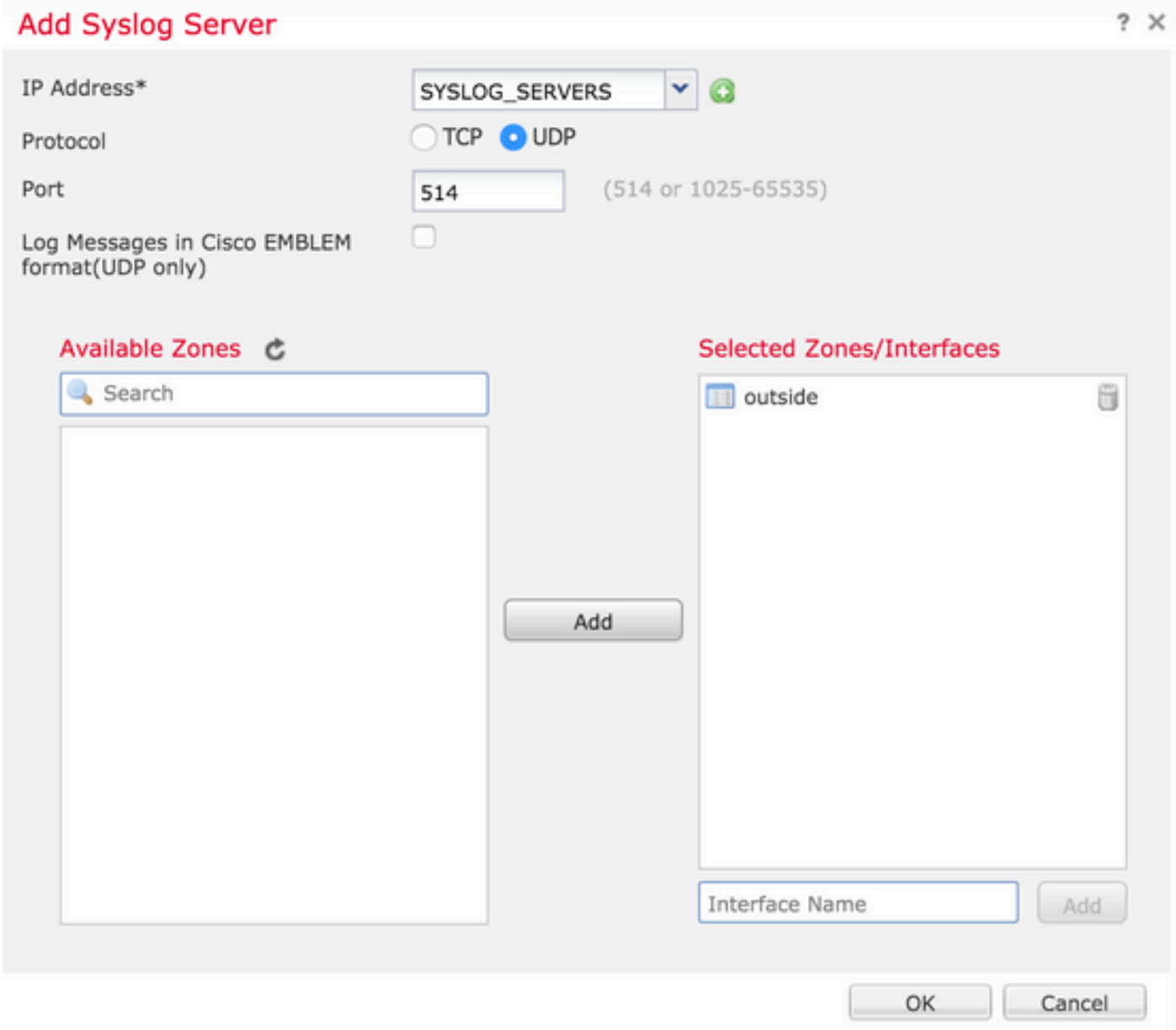
IP Address: **IP Address** 드롭다운 목록에서 Syslog 서버가 나열된 네트워크 객체를 선택합니다. 네트워크 객체를 생성하지 않은 경우 플러스(+) 아이콘을 클릭하여 새 객체를 생성합니다.

Protocol: Syslog 통신에 **TCP** 대한 또는 **UDP** 라디오 버튼을 클릭합니다.

Port: Syslog 서버 포트 번호를 입력합니다. 기본적으로 514입니다.

Log Messages in Cisco EMBLEM format(UDP only): Cisco **Log Messages in Cisco EMBLEM format (UDP only)** EMBLEM 형식으로 메시지를 기록해야 하는 경우 이 옵션을 활성화하려면 확인란을 클릭합니다. 이는 UDP 기반 Syslog에만 적용됩니다.

Available Zones: Syslog 서버에 연결할 수 있는 보안 영역을 입력하고 Selected Zones/ Interfaces(선택한 영역/인터페이스) 열로 이동합니다.



컨피그레이션 **OK** 을 **Save** 저장하려면 및 를 클릭합니다.

플랫폼 설정 **Save** 을 저장하려면 를 클릭합니다. 변경 **Deploy**사항을 적용할 FTD 어플라이언스를 선택하고 를 클릭하여 플랫폼 설정 **Deploy** 의 구축을 시작합니다.

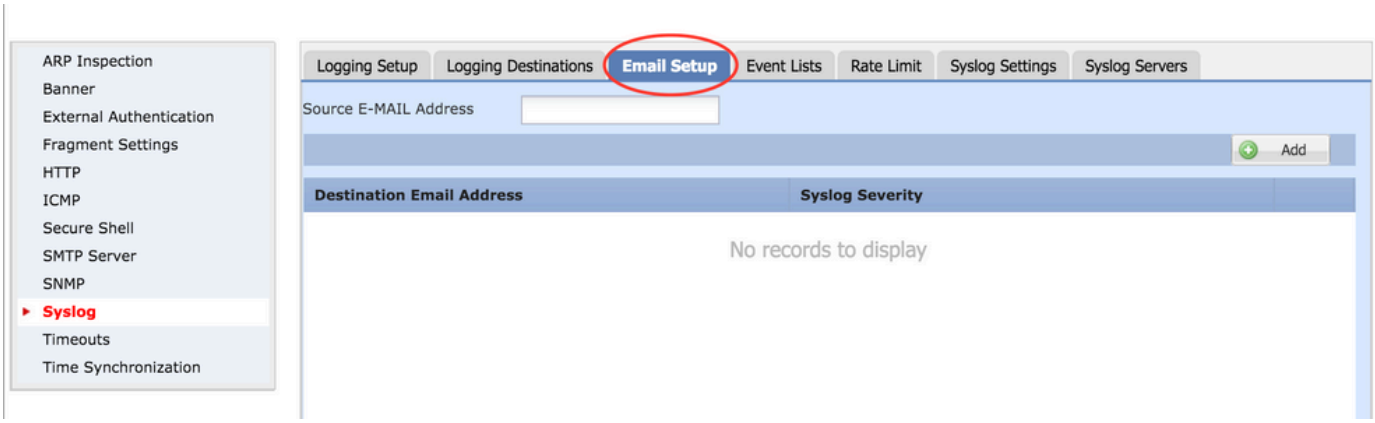
로깅을 위한 이메일 설정

FTD를 사용하면 특정 이메일 주소로 Syslog를 전송할 수 있습니다. 이메일 릴레이 서버가 이미 구성된 경우에만 이메일을 로깅 대상으로 사용할 수 있습니다.

Syslog에 대한 이메일 설정을 구성하는 2단계가 있습니다.

1단계. 를 **Device** > **Platform Setting** > **Threat Defense Policy** > **Syslog** >**Email Setup**선택합니다.

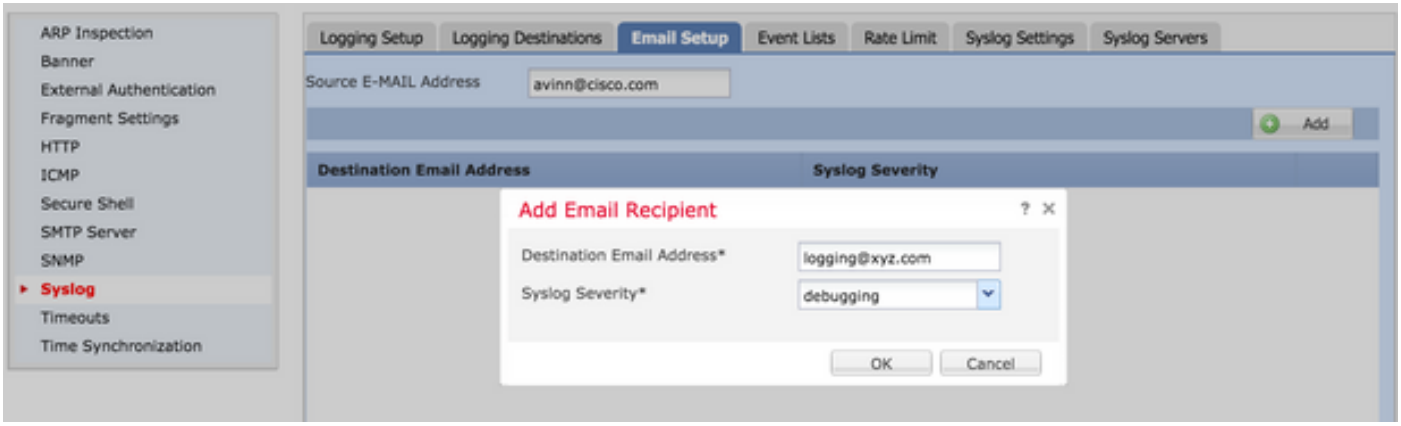
Source E-MAIL Address: Syslog가 포함된 FTD에서 전송된 모든 이메일에 표시되는 소스 이메일 주소를 입력합니다.



2단계. 대상 이메일 주소 및 Syslog 심각도를 구성하려면 을(를) **Add**클릭합니다.

Destination Email Address: Syslog 메시지가 전송되는 대상 이메일 주소를 입력합니다.

Syslog Severity: **Syslog Severity** 드롭다운 목록에서 Syslog 심각도를 선택합니다.



컨피그레이션 **OK** 을 저장하려면 를 클릭합니다.

플랫폼 설정 **Save** 을 저장하려면 를 클릭합니다. 변경 **Deploy**사항을 적용할 FTD 어플라이언스를 선택하고 를 클릭하여 플랫폼 설정 **Deploy** 의 구축을 시작합니다.

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

- FTD CLI에서 FTD Syslog 컨피그레이션을 확인합니다. FTD의 관리 인터페이스에 로그인하고 명령을 입력하여 **system support diagnostic-cli** 진단 CLI에 대한 콘솔을 활성화합니다.

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
><Press Enter>
firepower# sh run logging
logging enable
logging console emergencies
logging buffered debugging
logging host inside 192.168.0.192
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
logging permit-hostdown
```

- FTD에서 Syslog 서버에 연결할 수 있는지 확인합니다. SSH를 통해 FTD 관리 인터페이스에 로그인하고 명령을 사용하여 연결을 **ping** 확인합니다.

```
Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)

> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower# ping 192.168.0.192
```

- FTD와 Syslog 서버 간의 연결을 확인하기 위해 패킷 캡처를 수행할 수 있습니다. SSH를 통해 FTD 관리 인터페이스에 로그인하고 명령을 입력합니다 **system support diagnostic-cli**. 패킷 캡처 명령에 대해서는 CLI 및 ASDM 컨피그레이션 예제를 사용한 ASA Packet Captures를 참조하십시오.

- 정책 배포가 성공적으로 적용되었는지 확인합니다.

관련 정보

- ASA용 Cisco Firepower Threat Defense 빠른 시작 설명서
- 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.