ASDM을 사용하여 시스템/트래픽 이벤트에 대한 Firepower 모듈의 로깅 구성(온박스 관리)

목차

소개

이 문서에서는 Firepower 모듈의 시스템/트래픽 이벤트 및 이러한 이벤트를 외부 로깅 서버로 전송하는 다양한 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA(Adaptive Security Appliance) 방화벽, ASDM(Adaptive Security Device Manager)에 대한 지식
- Firepower 어플라이언스 지식
- Syslog, SNMP 프로토콜 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 5.4.1 이상을 실행하는 ASA Firepower 모듈(ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X).
- 소프트웨어 버전 6.0.0 이상을 실행하는 ASA Firepower 모듈(ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X)
- ASDM 7.5(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 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이벤트 유형

Firepower Module 이벤트는 두 가지 유형으로 분류할 수 있습니다.

1. Traffic Events(Connection events/Intrusion Events/Security Intelligence Events/SSL Events/Malware/File Events).
2. 시스템 이벤트(Firepower OS(운영 체제) 이벤트).

구성

출력 대상 구성

1단계. Syslog 서버 컨피그레이션

트래픽 이벤트에 대한 Syslog 서버를 구성하려면 Configuration(컨피그레이션) **> ASA Firepower Configuration(ASA Firepower 컨피그레이션) > Policies(정책) > Actions Alerts(작업 알림)로 이동하고 Create Alert(경고 생성)** 드롭다운 메뉴를 클릭하고 Create Syslog Alert(Syslog 경고 생성) 옵션을 선택합니다.Syslog 서버의 값을 입력합니다.

이름: Syslog 서버를 고유하게 식별하는 이름을 지정합니다.

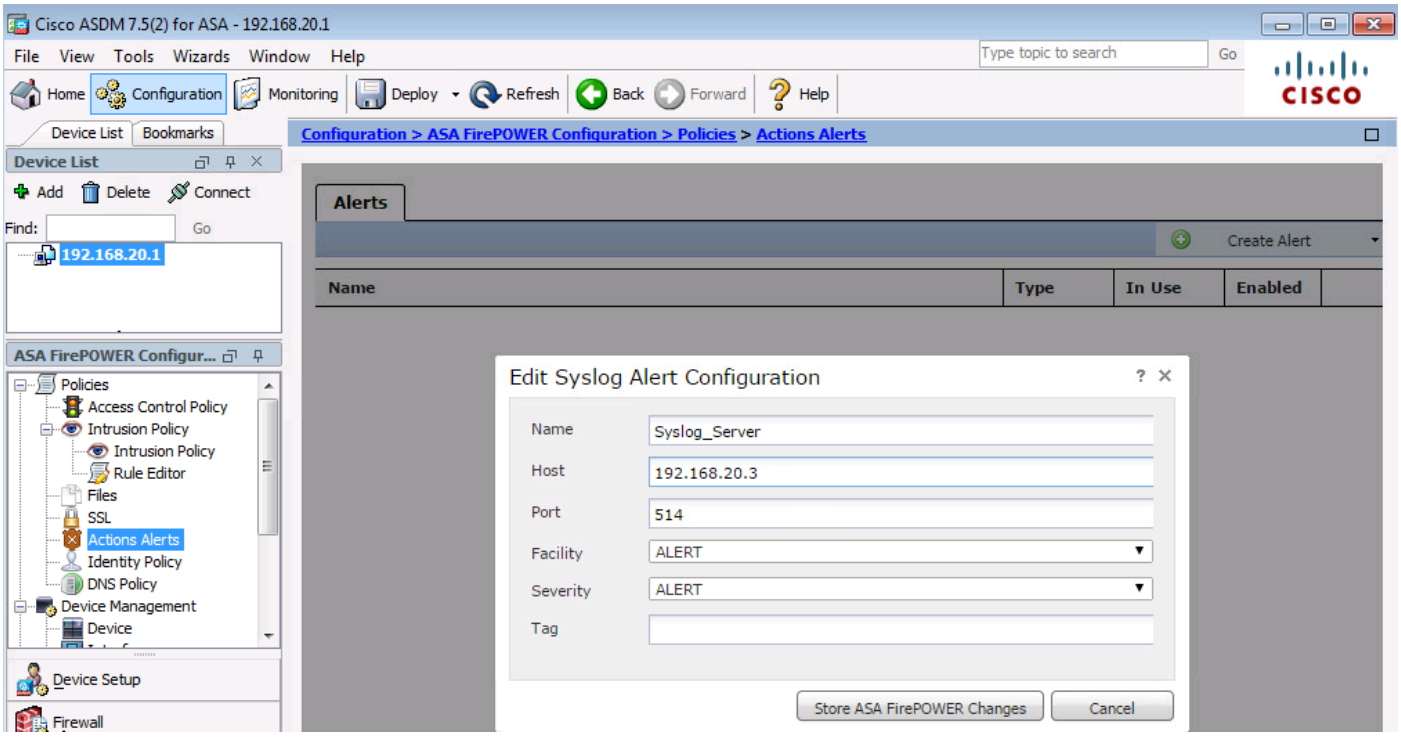
Host: Syslog 서버의 IP 주소/호스트 이름을 지정합니다.

포트: Syslog 서버의 포트 번호를 지정합니다.

기능: Syslog 서버에 구성된 기능을 선택합니다.

심각도: Syslog 서버에 구성된 심각도를 선택합니다.

태그: Syslog 메시지에 표시할 태그 이름을 지정합니다.



2단계.SNMP 서버 구성

트래픽 이벤트에 대한 SNMP 트랩 서버를 구성하려면 ASDM Configuration(ASDM 컨피그레이션) **> ASA Firepower Configuration(ASA Firepower 컨피그레이션) > Policies(정책) > Actions Alerts(작업 알림)로** 이동하고 Create Alert(**알림 생성**) 드롭다운 메뉴를 클릭하고 Create SNMP Alert(SNMP 알림 생성) 옵션을 선택합니다.

이름: SNMP 트랩 서버를 고유하게 식별하는 이름을 지정합니다.

트랩 서버: SNMP 트랩 서버의 IP 주소/호스트 이름을 지정합니다.

버전: Firepower Module은 SNMP v1/v2/v3을 지원합니다. 드롭다운 메뉴에서 SNMP 버전을 선택합니다.

커뮤니티 문자열: **Version** 옵션에서 v1 또는 v2를 선택한 경우 SNMP 커뮤니티 이름을 지정합니다.

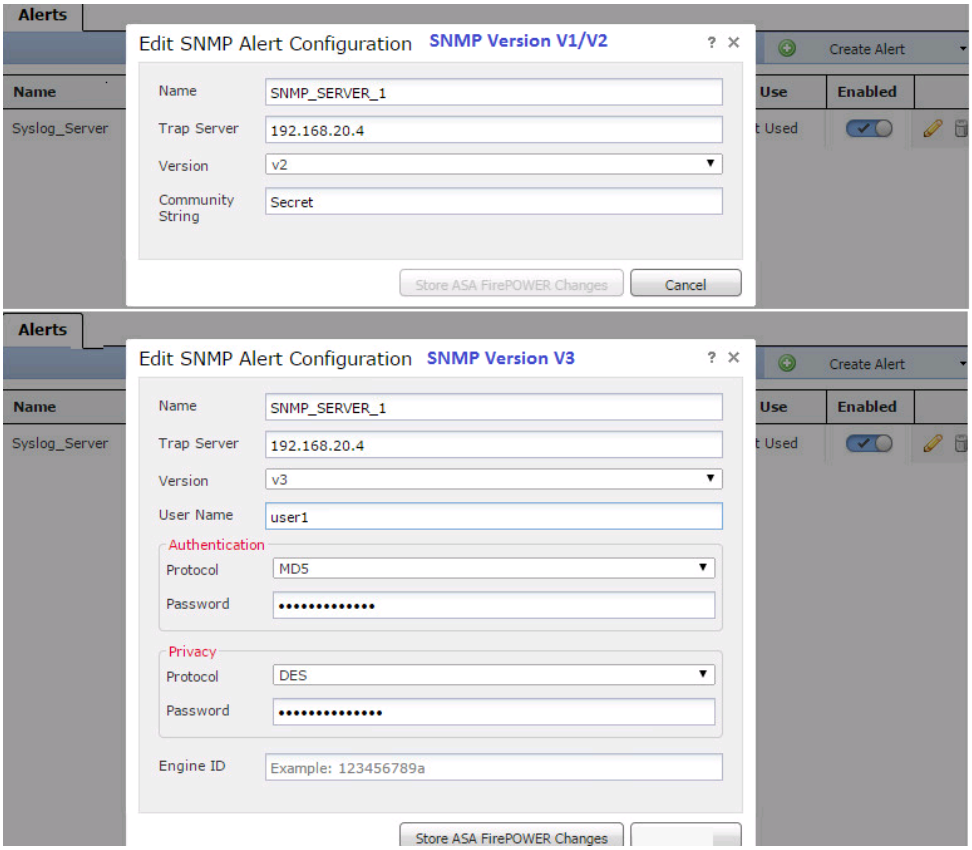
사용자 이름: **버전** 옵션에서 v3을 선택하면 시스템에서 **사용자 이름** 필드를 표시합니다.사용자 이름을 지정합니다.

인증: 이 옵션은 SNMP v3 컨피그레이션의 일부입니다.해시를 기반으로 인증을 제공합니다.

MD5 또는 SHA 알고리즘을 사용하는 알고리즘입니다.Protocol 드롭다운 메뉴에서 해시 알고리즘을 선택하고 Enter 키를 누릅니다.

암호 옵션의 암호입니다.이 기능을 사용하지 않으려면 **없음** 옵션을 선택합니다.

개인 정보:이 옵션은 SNMP v3 컨피그레이션의 일부입니다.DES 알고리즘을 사용하여 암호화를 제공합니다.Protocol 드롭다운 메뉴에서 옵션을 **DES**로 선택하고 **Password** 필드에 암호를 입력합니다.데이터 암호화 기능을 사용하지 않으려면 **없음** 옵션을 선택합니다.



트래픽 이벤트 전송을 위한 컨피그레이션

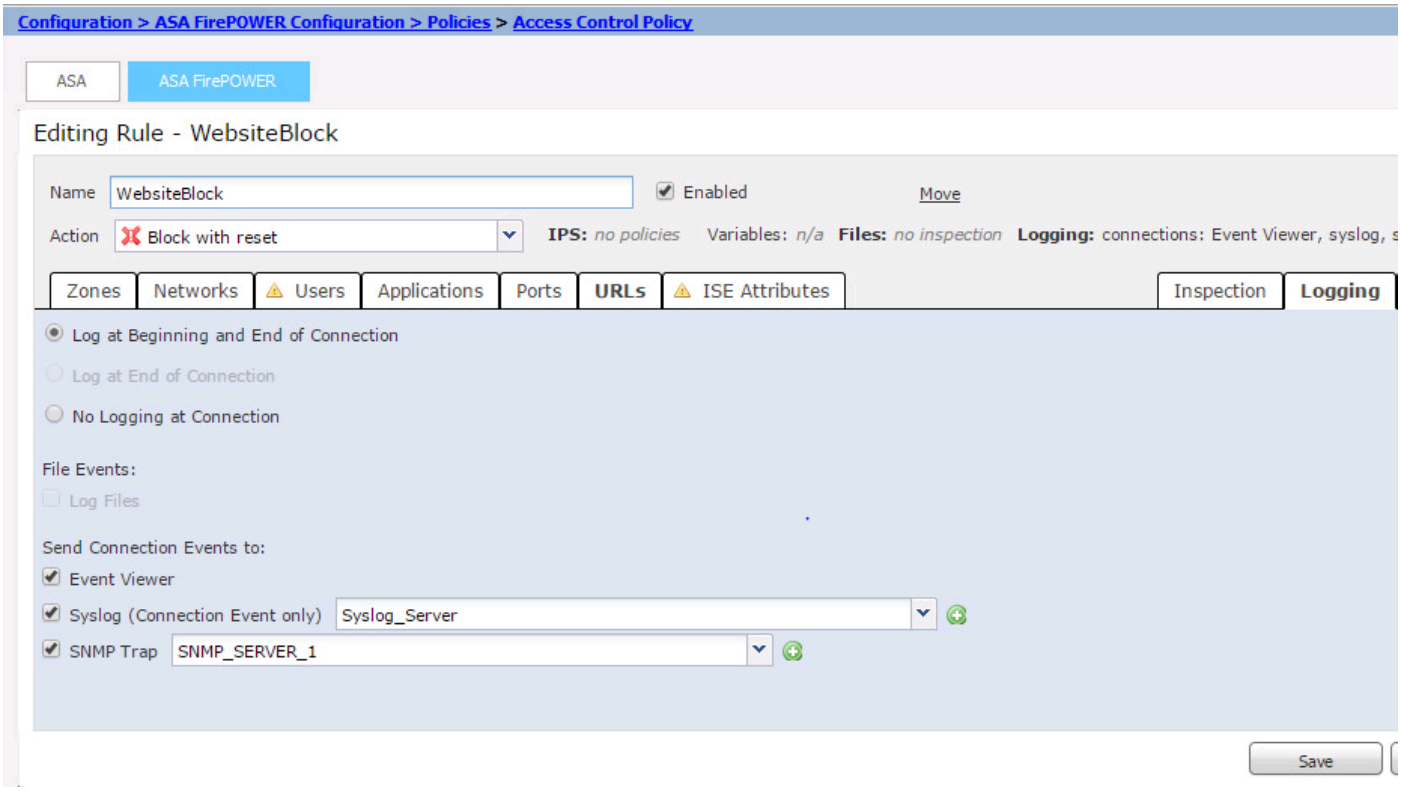
연결 이벤트에 대한 외부 로깅 사용

트래픽이 로깅이 활성화된 액세스 규칙에 도달하면 연결 이벤트가 생성됩니다.연결 이벤트에 대한 외부 로깅을 활성화하려면 **(ASDM Configuration > ASA Firepower Configuration > Policies > Access Control Policy)**에서 **액세스 규칙**을 **편집하고 logging** 옵션으로 **이동합니다**.

로깅 옵션을 Beginning **and End of Connection** 또는 Log at **End of Connection으로 선택합니다** .Send **Connection Events to** 옵션**으로** 이동하고 이벤트를 보낼 위치를 지정합니다.

외부 Syslog 서버로 이벤트를 전송하려면 **Syslog**를 선택한 다음 드롭다운 목록에서 Syslog 알림 응답을 선택합니다.선택적으로, 추가 **아이콘**을 클릭하여 Syslog 알림 응답을 추가할 수 있습니다.

SNMP 트랩 서버로 연결 이벤트를 보내려면 **SNMP Trap**을 선택한 다음 드롭다운 목록에서 SNMP 알림 응답을 선택합니다.선택적으로, 추가 **아이콘**을 클릭하여 SNMP 알림 응답을 추가할 수 있습니다.



침입 이벤트에 대한 외부 로깅 활성화

시그니처(snort 규칙)가 일부 악성 트래픽과 일치할 때 침입 이벤트가 생성됩니다. 침입 이벤트에 대한 외부 로깅을 활성화하려면 ASDM Configuration(ASDM 컨피그레이션) > ASA Firepower Configuration(ASA Firepower 컨피그레이션) > Policies(**정책) > Intrusion Policy(침입 정책) > Intrusion Policy(침입 정책)로** 이동합니다.새 침입 정책을 생성하거나 기존 침입 정책을 수정합니다 .Advanced **Setting(고급 설정)** > External Responses(**외부 응답)로 이동합니다.**

침입 이벤트를 외부 SNMP 서버로 전송하려면 SNMP Alerting(SNMP 알림)에서 **Enabled(활성화됨)** 옵션을 선택한 다음 Edit(**수정)** 옵션을 클릭합니다.

트랩 유형:트랩 유형은 경고에 나타나는 IP 주소에 사용됩니다.네트워크 관리 시스템에서 INET_IPV4 주소 유형을 올바르게 렌더링하는 경우 이진으로 선택할 수 있습니다.그렇지 않으면 String으로 선택합니다.

SNMP 버전: 다음 중 하나를 선택합니다. **버전 2** 또는 **버전 3** 라디오 버튼.

SNMP v2 옵션

트랩 서버:이 이미지에 표시된 대로 SNMP 트랩 서버의 IP 주소/호스트 이름을 지정합니다.

커뮤니티 문자열:커뮤니티 이름을 지정합니다.

SNMP v3 옵션

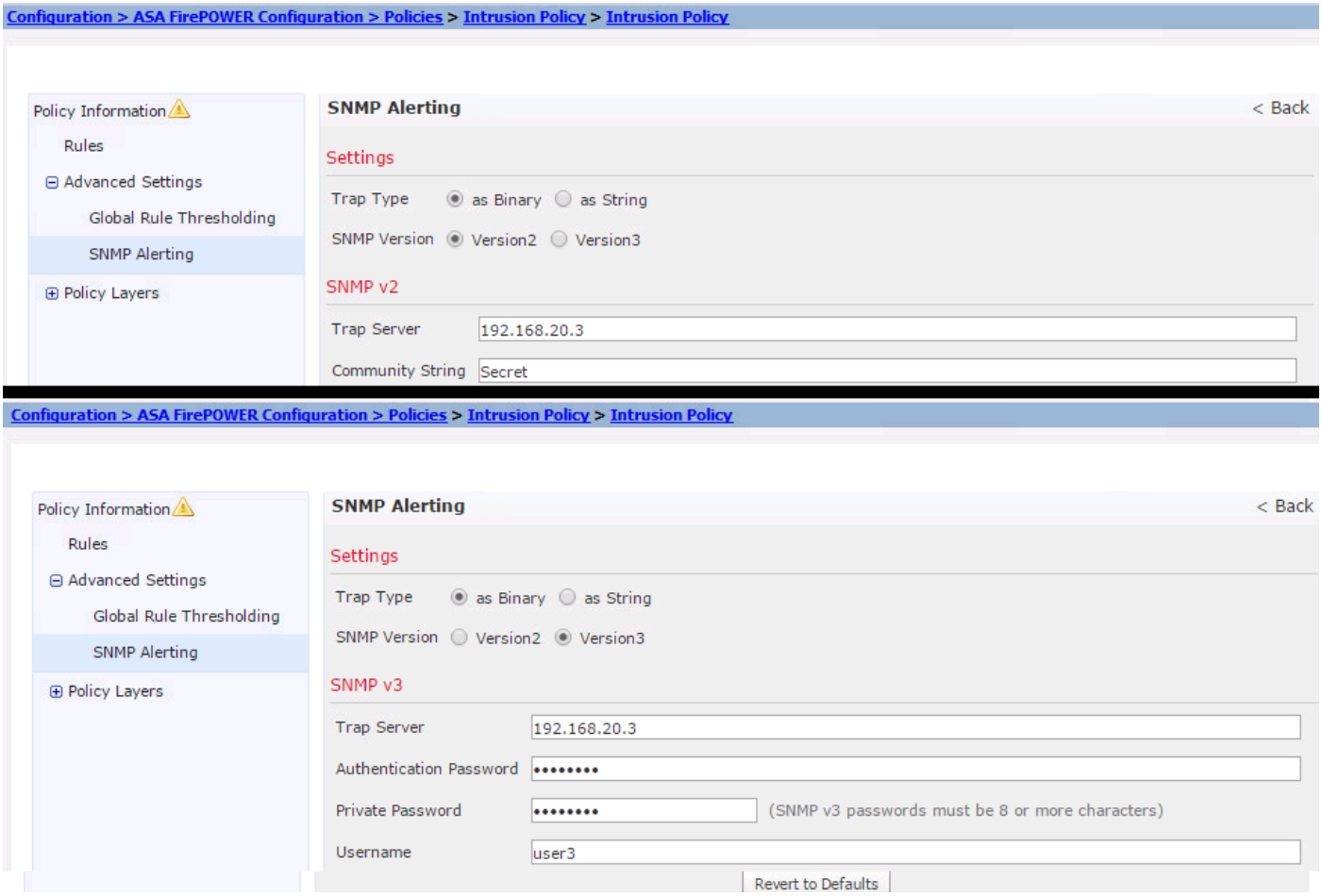
트랩 서버:이 이미지에 표시된 대로 SNMP 트랩 서버의 IP 주소/호스트 이름을 지정합니다.

인증 암호:지정인증에 필요한 암호입니다.SNMP v3에서는 해시 함수를 사용하여 비밀번호를 인증합니다.

Private Password: 암호화에 대한 비밀번호를 지정합니다.SNMP v3는 DES(Data Encryption

Standard) 블록 암호를 사용하여 이 비밀번호를 암호화합니다.

사용자 이름:사용자 이름을 지정합니다.



외부 Syslog 서버로 침입 이벤트를 전송하려면 옵션을 선택합니다 **사용** Syslog **내 경고** 그런 다음 **편집** 옵션을 선택합니다.

로깅 호스트: Syslog 서버의 IP 주소/호스트 이름을 지정합니다.

기능: 협업공간 선택 Syslog 서버에 구성되어 있습니다

심각도:Syslog 서버에 구성된 심각도를 선택합니다.

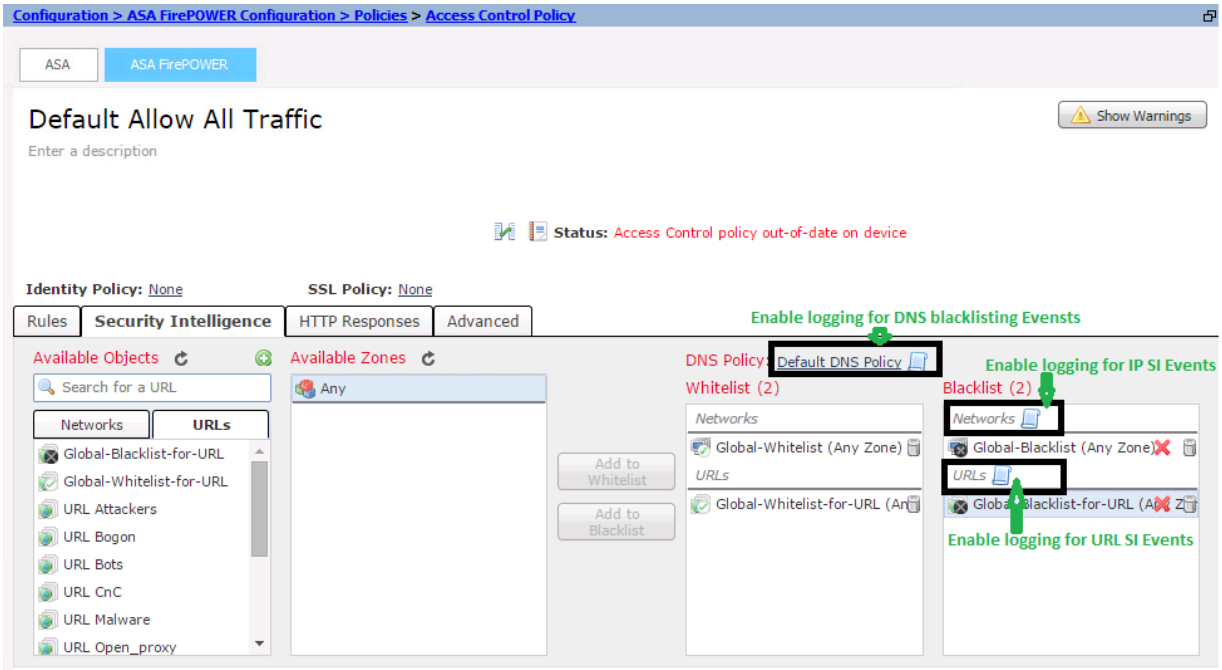
IP 보안 인텔리전스/DNS 보안 인텔리전스/URL 보안 인텔리전스에 대한 외부 로깅 활성화

IP Security Intelligence/DNS Security Intelligence/URL Security Intelligence 이벤트는 트래픽이 IP 주소/도메인 이름/URL Security Intelligence 데이터베이스와 일치할 때 생성됩니다.IP/URL/DNS 보안 인텔리전스 이벤트에 대한 외부 로깅을 활성화하려면 **(ASDM Configuration > ASA Firepower Configuration > Policies > Access Control Policy > Security Intelligence)**,

IP/DNS/URL 보안 인텔리전스에 대한 로깅을 활성화하려면 이미지에 표시된 **아이콘**을 클릭합니다 .아이콘을 클릭하면 외부 서버로 이벤트를 전송하는 로깅 및 옵션을 활성화하는 대화 상자가 표시됩니다.

외부 Syslog 서버로 이벤트를 전송하려면 **Syslog**를 선택한 다음 드롭다운 목록에서 Syslog 알림 응답을 선택합니다.선택적으로, 추가 아이콘을 클릭하여 Syslog 알림 응답을 추가할 수 있습니다.

SNMP 트랩 서버로 연결 이벤트를 보내려면 **SNMP Trap**을 선택한 다음 드롭다운 목록에서 SNMP 알림 응답을 선택합니다.선택적으로, 추가 아이콘을 클릭하여 SNMP 알림 응답을 추가할 수 있습니다.



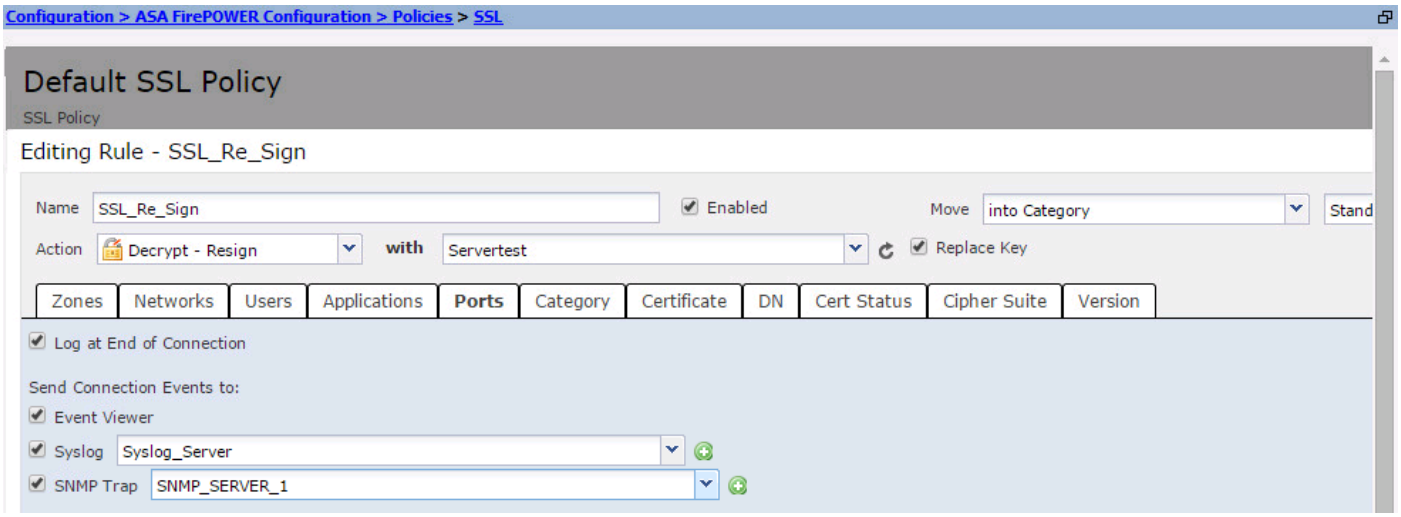
SSL 이벤트에 대한 외부 로깅 사용

SSL 이벤트는 트래픽이 로깅이 활성화된 SSL 정책의 모든 규칙과 일치할 때 생성됩니다.SSL 트래픽에 대한 외부 로깅을 활성화하려면 **ASDM Configuration(ASDM 구성) > ASA Firepower Configuration(ASA Firepower 구성) > Policies(정책) > SSL**로 이동합니다. 기존 규칙을 편집하거나 새 규칙을 생성하고 로깅 옵션**으로** 이동합니다.End of Connection(연결 종료) 옵션**에서 로그를 선택합니다**.

그런 다음 Send **Connection Events to(연결 이벤트 보내기)로** 이동하고 이벤트를 전송할 위치를 지정합니다.

외부 Syslog 서버로 이벤트를 보내려면 **Syslog**를 선택한 다음 드롭다운 목록에서 Syslog 알림 응답을 선택합니다.선택적으로, 추가 아이콘을 클릭하여 Syslog 알림 응답을 추가할 수 있습니다.

SNMP 트랩 서버로 연결 이벤트를 보내려면 **SNMP Trap**을 선택한 다음 드롭다운 목록에서 SNMP 알림 응답을 선택합니다.선택적으로, 추가 아이콘을 클릭하여 SNMP 알림 응답을 추가할 수 있습니다.



시스템 이벤트 전송을 위한 구성

시스템 이벤트에 대한 외부 로깅 사용

시스템 이벤트는 Firepower 운영 체제의 상태를 표시합니다.SNMP 관리자를 사용하여 이러한 시스템 이벤트를 폴링할 수 있습니다.

Firepower Module에서 시스템 이벤트를 폴링하기 위해 SNMP 서버를 구성하려면 SNMP 서버에서 폴링할 수 있는 Firepower MIB(Management Information Base)에서 정보를 사용할 수 있도록 하는 시스템 정책을 구성해야 합니다.

ASDM Configuration(**ASDM 컨피그레이션) > ASA Firepower Configuration(ASA Firepower 컨피그레이션) > Local(로컬) > System Policy(시스템 정책**)로 이동하고 **SNMP**를 클릭합니다.

SNMP 버전: Firepower Module은 SNMP v1/v2/v3을 지원합니다. SNMP 버전을 지정하십시오.

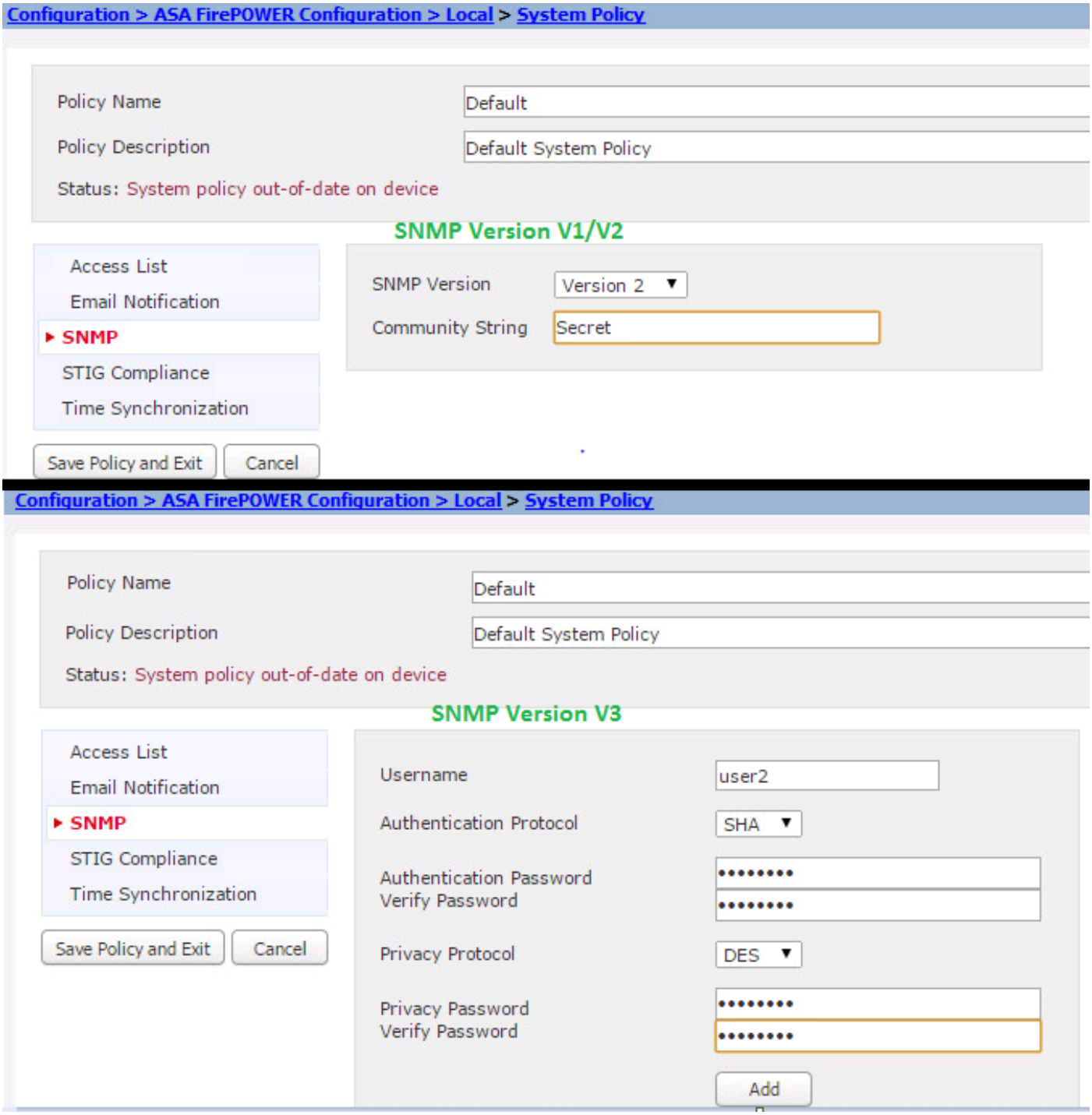
커뮤니티 문자열: SNMP 버전 옵션**에서 v1/v2**를 선택한 경우 Community String 필드에 SNMP 커뮤니티 이름을 입력합니다.

사용자 이름: version 옵션에서 **v3** 옵션을 선택한 경우Add **User(사용자 추가**) 버튼을 클릭하고 **Username**(사용자 이름) 필드에 Username(사용자 이름)을 지정합니다.

인증: 이 옵션은 SNMP v3 컨피그레이션의 일부입니다.MD5 또는 SHA 알고리즘을 사용하여 해시된 메시지 인증 코드를 기반으로 인증을 제공합니다.해시 알고리즘**을** 선택하고 비밀번호를 입력합니다.

in **Password**(비밀번호) 필드인증 기능을 사용하지 않으려면 **None** 옵션을 선택합니다.

개인 정보: 이 옵션은 SNMP v3 컨피그레이션의 일부입니다.DES/AES 알고리즘을 사용하여 암호화를 제공합니다.암호화 프로토콜을 선택하고 **Password** 필드에 암호를 입력합니다.데이터 암호화 기능을 사용하지 않으려면 **None** 옵션을 선택합니다.



: MIB(Management Information Base) . Firepower Module MIB (DCEALERT.MIB) (/etc/sf/DCEALERT.MIB) .

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems