Firepower Module(온박스 관리)에서 침입 정책 및 시그니처 컨피그레이션 구성

목차

소개

이 문서에서는 FirePOWER 모듈의 IPS(Intrusion Prevention System)/IDS(Intrusion Detection System) 기능과 FirePOWER Module에서 탐지 정책을 만드는 다양한 침입 정책 요소에 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

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)

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

배경 정보

FirePOWER IDS/IPS는 네트워크 트래픽을 검사하고 네트워크/시스템 공격을 나타내는 악성 패턴(또는 서명)을 식별하도록 설계되었습니다.FirePOWER 모듈은 ASA의 서비스 정책이 모니터 모드(프로미스큐어스)에서 특별히 구성된 경우 IDS 모드에서 작동하며, 그렇지 않은 경우 인라인 모드에서 작동합니다.

FirePOWER IPS/IDS는 시그니처 기반 탐지 방식입니다. IDS 모드의 FirePOWERmodule은 시그니처가 악성 트래픽과 일치하면 알림을 생성하고, IPS 모드의 FirePOWER 모듈은 알림을 생성하고 악성 트래픽을 차단합니다.

: FirePOWER Module **Protect** . Configuration() **> ASA FirePOWER Configuration(ASA FirePOWER) > License() .**

구성

1단계. 침입 정책 구성

1.1단계. 침입 정책 생성

침입 정책을 구성하려면 ASDM(Adaptive Security Device Manager)에 로그인하여 다음 단계를 완료합니다.

1단계. Configuration(구성) **> ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션) > Policies(정책) > Intrusion Policy(침입 정책) > Intrusion Policy(침입 정책)로 이동합니다**.

2단계. Create **Policy(정책 생성)를 클릭합니다**.

3단계. **Name** of the Intrusion Policy를 입력합니다.

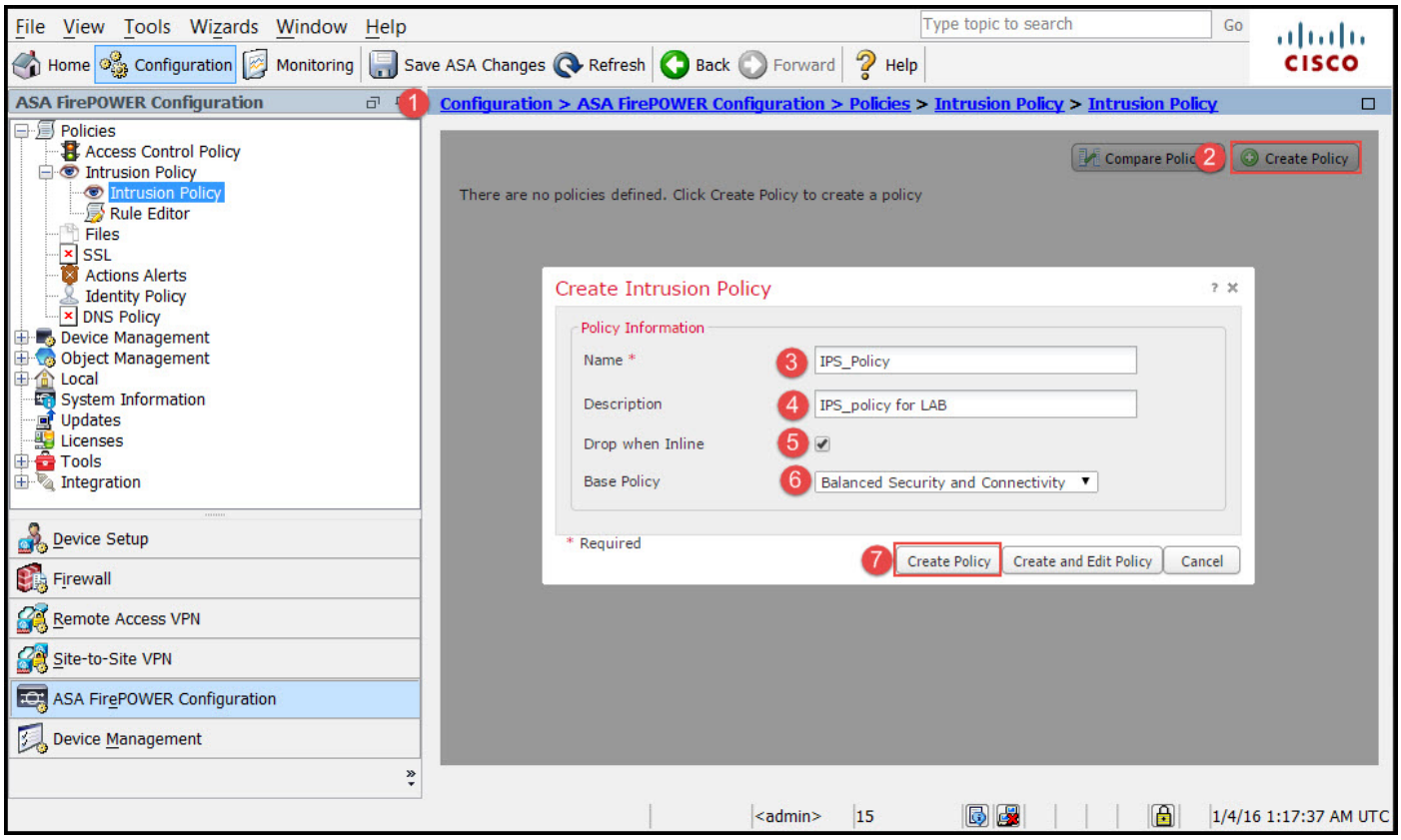
4단계. **Description** of the Intrusion Policy(침입 정책 설명(선택 사항)를 입력합니다.

5단계. Drop when Inline 옵션**을** 지정합니다.

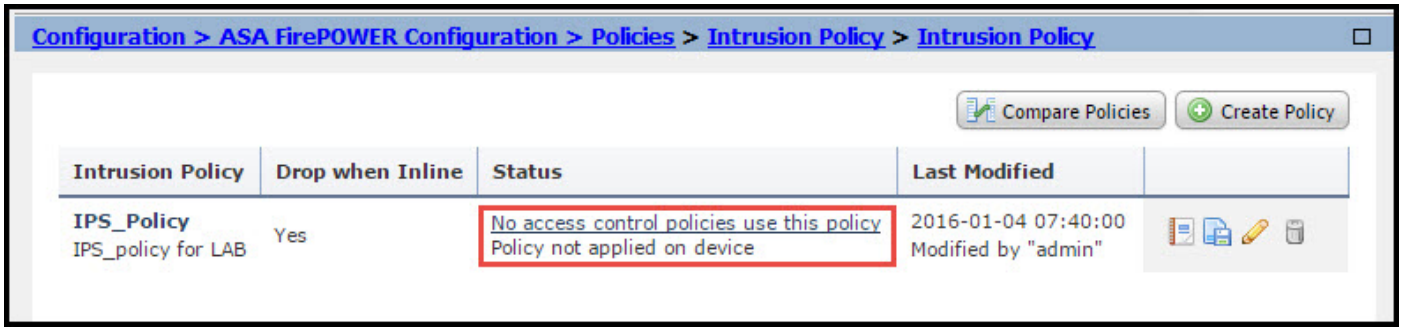
6단계. 드롭다운 목록에서 **Base Policy**를 선택합니다.

7단계. Create **Policy(정책 생성)**를 클릭하여 침입 정책 생성을 완료합니다.

: Inline

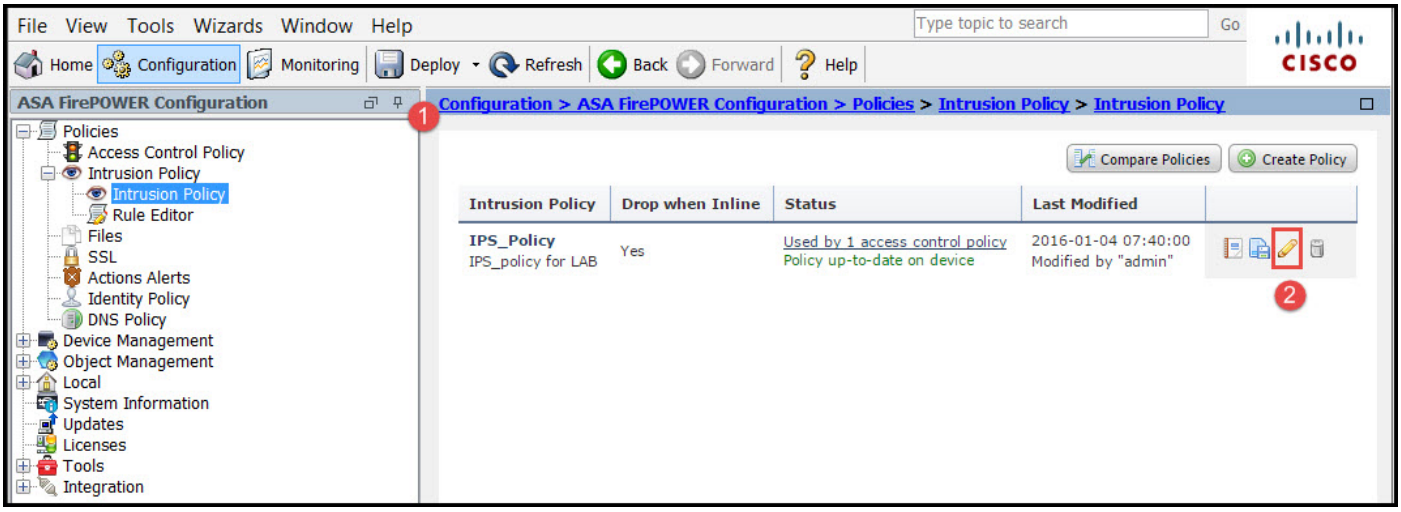


그러나 정책이 구성되었지만 어떤 디바이스에도 적용되지 않습니다.



1.2단계. 침입 정책 수정

Intrusion Policy를 수정하려면 Configuration(컨피그레이션) **> ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션) > Policies(정책) > Intrusion Policy(침입 정책) > Intrusion Policy(침입 정책)로 이동하고 Edit(수정)** 옵션을 선택합니다.

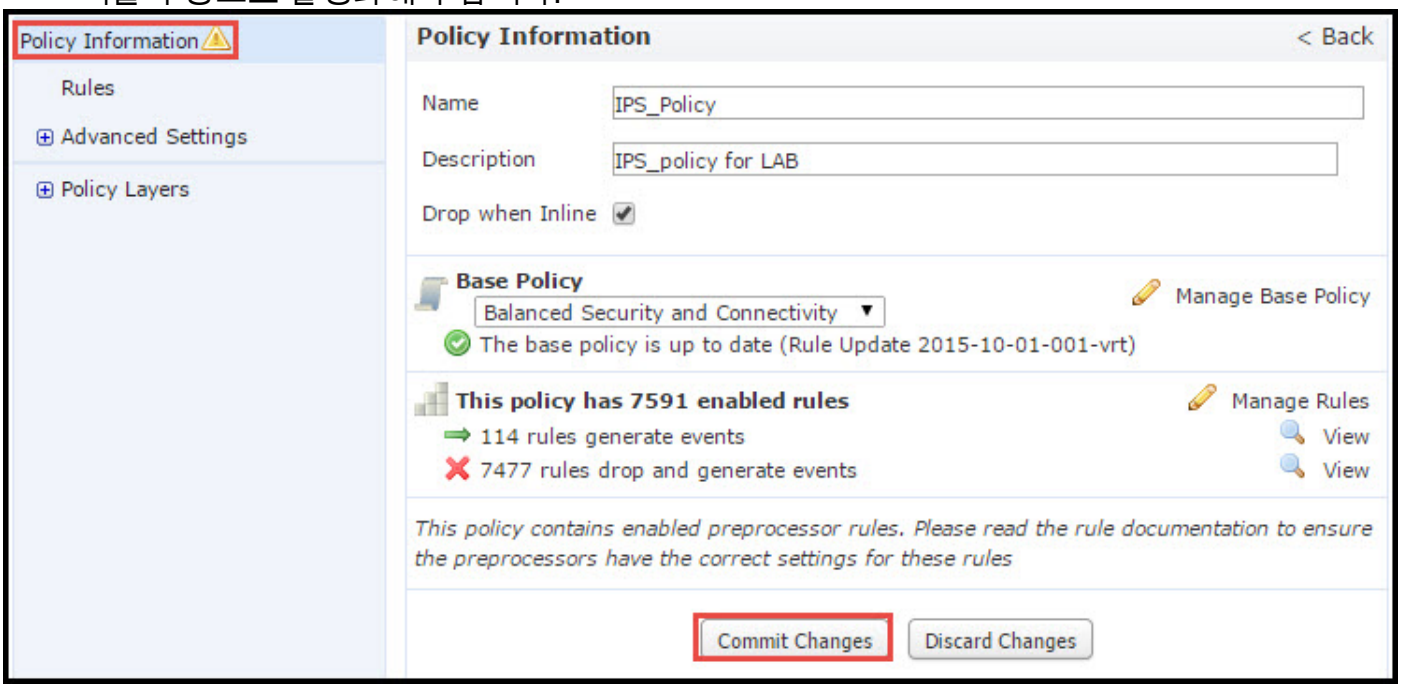


1.3단계. 기본 정책 수정

Intrusion Policy Management(침입 정책 관리) 페이지는 Inline/Save and Discard(인라인/저장 및 폐기 시 기본 정책/삭제) 옵션을 변경할 수 있는 옵션을 제공합니다.

기본 정책에는 기본 제공 정책인 일부 시스템 제공 정책이 포함되어 있습니다.

1. 균형 잡힌 보안 및 연결: 보안 및 연결 측면에서 최적의 정책입니다.이 정책에는 약 7,500개의 규칙이 활성화되었으며, 그중 일부는 이벤트만 생성하는 반면, 나머지는 이벤트를 생성하고 트래픽을 삭제합니다.
2. 연결에 대한 보안:기본 설정이 보안인 경우 연결 정책보다 보안을 선택할 수 있으므로 활성화된 규칙의 수가 늘어납니다.
3. 보안보다 연결: 기본 설정이 보안보다 연결인 경우 보안 정책보다 연결을 선택하여 활성화된 규칙의 수를 줄일 수 있습니다.
4. Maximum Detection(최대 탐지) - 최대 탐지를 얻으려면 이 정책을 선택합니다.
5. No Rule Active(활성 규칙 없음) - 이 옵션은 모든 규칙을 비활성화합니다.보안 정책에 따라 규칙을 수동으로 활성화해야 합니다.



1.4단계. 필터 막대 옵션을 사용한 서명 필터링

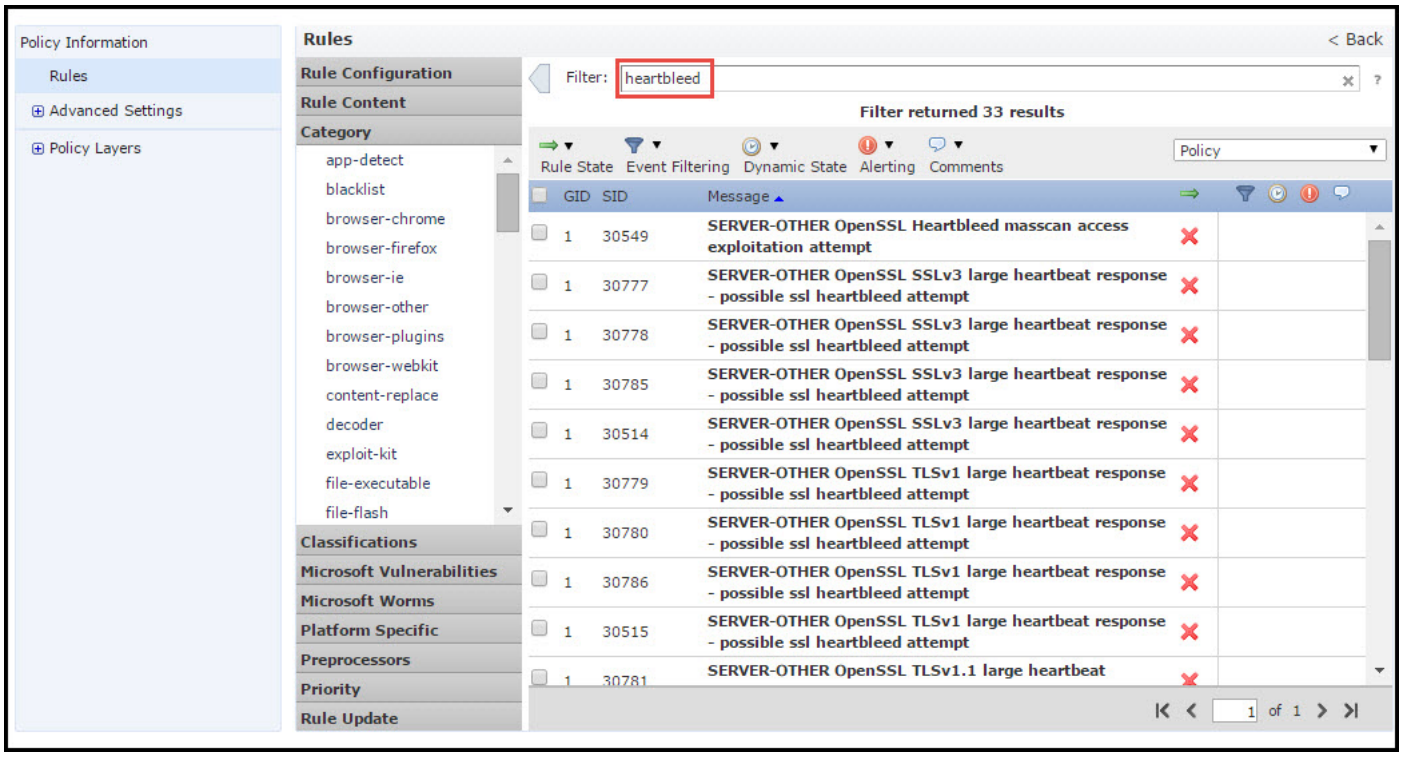
탐색 패널에서 **Rules** 옵션으로 이동하고 Rule Management 페이지가 나타납니다.Rule 데이터베이스에는 수천 개의 규칙이 있습니다.필터 표시줄에서는 규칙을 효과적으로 검색할 수 있는 좋은 검색 엔진 옵션을 제공합니다.

필터 표시줄에 키워드를 삽입할 수 있으며 시스템에서 결과를 가져옵니다.SSL(Secure Sockets Layer) 하트블리드 취약성에 대한 시그니처를 찾기 위한 요구 사항이 있는 경우 필터 막대에서 키워드 heartbleed를 검색할 수 있으며, 하트블리드 취약성에 대한 시그니처를 가져옵니다.

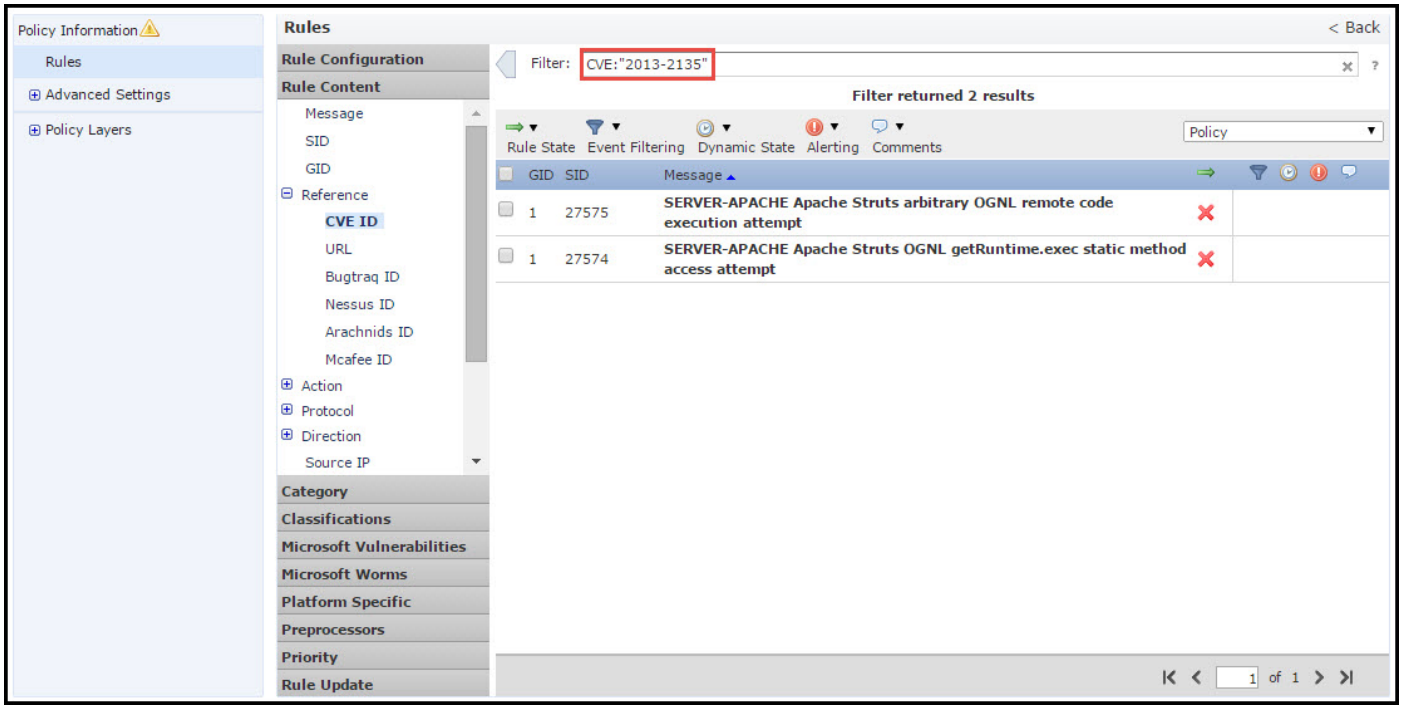
> **팁**: 필터 표시줄에 여러 키워드가 사용된 경우 시스템은 AND 논리를 사용하여 복합 검색을 생성합니다.

SID(Signature ID), GID(Generator ID), Category(카테고리)를 사용하여 규칙을 검색할 수도 있습니다.도 등

규칙은 Category/Classification/Microsoft Vulnerabilities/Microsoft Worms/Platform Specific과 같은 여러 가지 방법으로 효과적으로 분류됩니다.이러한 규칙 연결은 고객이 쉽게 올바른 서명을 받고 고객이 서명을 효과적으로 조정할 수 있도록 도와줍니다.



CVE 번호로 검색하여 해당 번호를 포함하는 규칙을 찾을 수도 있습니다.CVE 구문을 사용할 수 **있습니다.<cve-number>.**



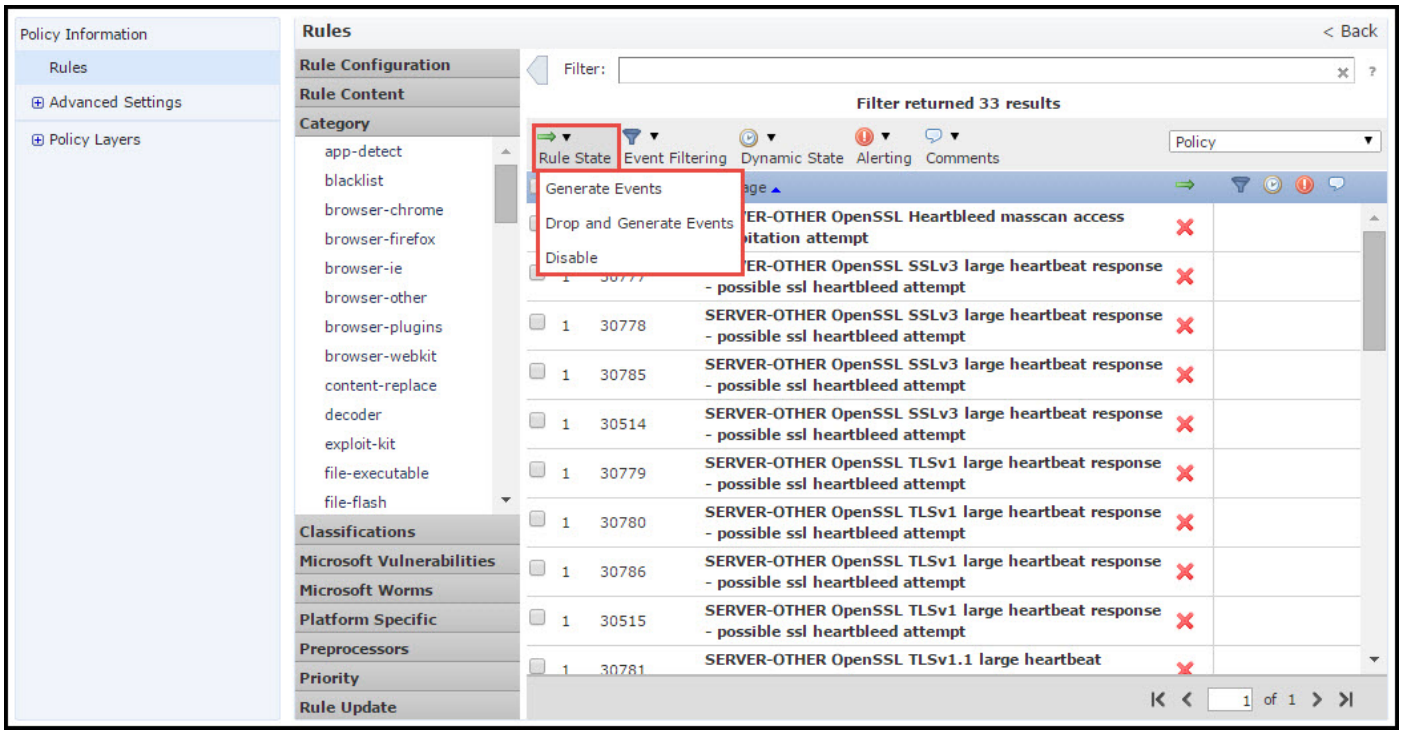
1.5단계. 규칙 상태 구성

다음으로 이동 **규칙** 탐색 패널의 옵션 및 Rule Management 페이지가 나타납니다..규칙을 선택하고 **Rule State** 옵션을 선택하여 규칙의 상태를 구성합니다.규칙에 대해 구성할 수 있는 세 가지 상태가 있습니다.

1. **이벤트 생성**이 옵션은 규칙이 트래픽과 매칭할 때 이벤트를 생성합니다.

2. **이벤트 삭제 및 생성:** 이 옵션은 규칙이 트래픽과 일치할 때 이벤트를 생성하고 트래픽을 삭제합니다.

3. **사용 안 함:**이 옵션은 규칙을 비활성화합니다.



1.6단계. 이벤트 필터 구성

침입 이벤트의 중요도는 발생 빈도 또는 소스 또는 대상 IP 주소를 기반으로 할 수 있습니다.경우에 따라 이벤트가 특정 횟수만큼 발생할 때까지 이벤트에 대해 신경 쓰지 않을 수도 있습니다.예를 들어, 특정 횟수에 오류가 발생할 때까지 서버에 로그인을 시도해도 문제가 발생하지 않을 수 있습니다.다른 경우에는 규칙 적중 횟수가 몇 번 발생해도 광범위한 문제가 있는지 확인할 수 있습니다.

이를 달성할 수 있는 두 가지 방법이 있습니다.

1. 이벤트 임계값

2. 이벤트 억제

이벤트 임계값

발생 수를 기준으로 이벤트 표시 빈도를 지정하는 임계값을 설정할 수 있습니다.이벤트당 및 정책별로 임계값을 구성할 수 있습니다.

이벤트 임계값을 구성하는 단계:

1단계. **이벤트 임계값**을 구성하려는 규칙을 선택합니다.

2단계. **Event Filtering(이벤트 필터링)을 클릭합니다**.

3단계. Threshold(임계값)를 **클릭합니다**.

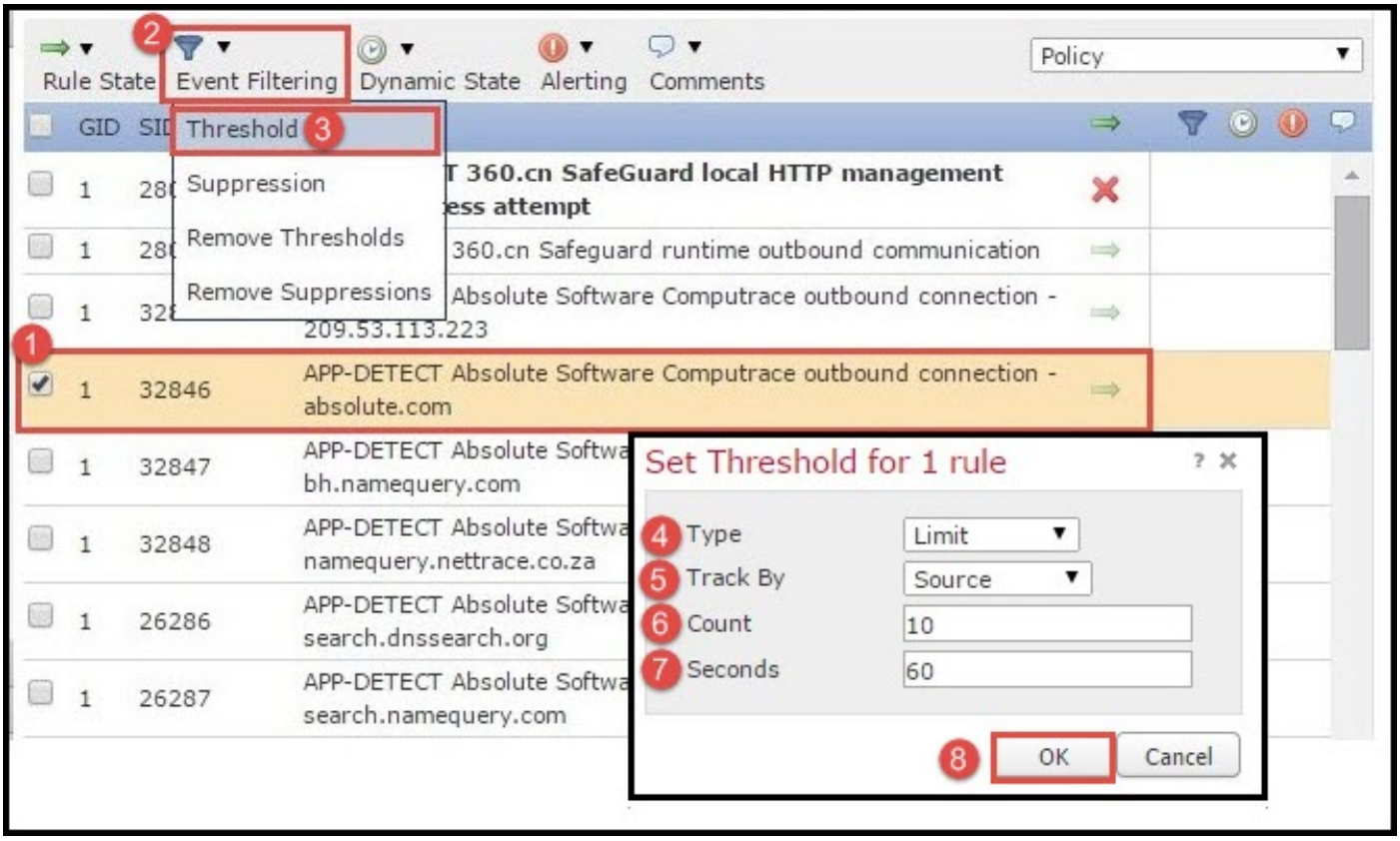
4단계. 드롭다운 목록에서 유형을 선택합니다.(제한 또는 임계값 또는 둘 다).

5단계. 추적 기준 드롭다운 상자에서 추적 방법**을** 선택합니다.(소스 또는 대상).

6단계. 임계값을 충족할 이벤트 수를 입력합니다.

7단계. 카운트가 재설정되기 전에 경과할 **초**를 입력합니다.

8단계. **확인**을 클릭하여 완료합니다.



이벤트 필터가 규칙에 추가되면 규칙 표시 옆에 필터 아이콘이 표시될 수 있습니다. 이 경우 이 규칙에 대해 활성화된 이벤트 필터링이 있음을 알 수 있습니다.

이벤트 억제

지정된 이벤트 알림은 소스/대상 IP 주소 또는 규칙에 따라 억제할 수 있습니다.

참고:규칙에 대한 이벤트 억제를 추가할 때서명 검사는 정상적으로 작동하지만 트래픽이 시그니처와 일치하는 경우 시스템은 이벤트를 생성하지 않습니다.특정 Source/Destination을 지정하면 이 규칙의 특정 소스/대상에 대해서만 이벤트가 나타나지 않습니다.전체 규칙을 억제하도록 선택하면 시스템은 이 규칙에 대한 이벤트를 생성하지 않습니다.

이벤트 임계값을 구성하는 단계:

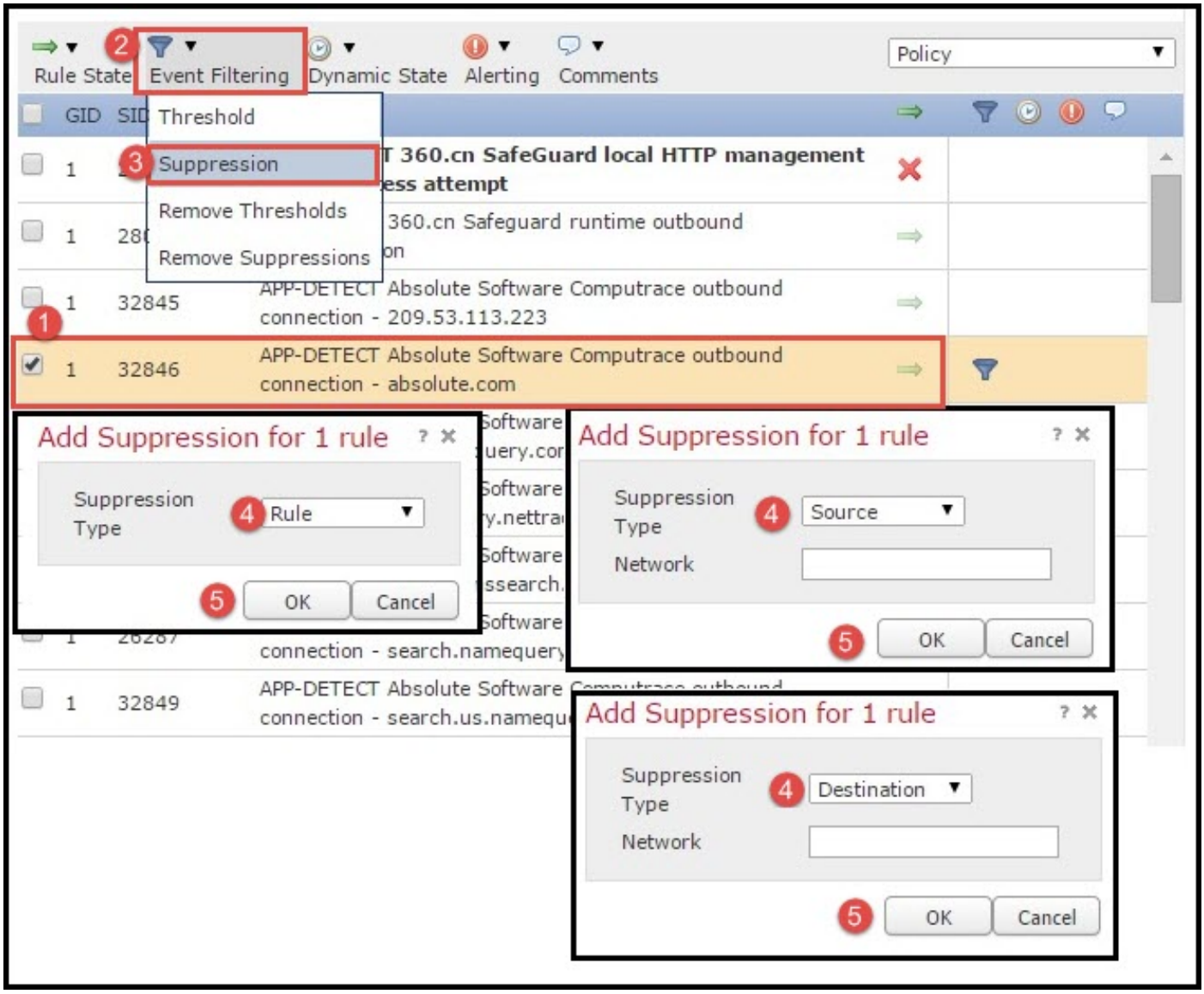
1단계. **이벤트 임계값**을 구성하려는 규칙을 선택합니다.

2단계. **Event Filtering을 클릭합니다**.

3단계. 삭제를 **누릅니다.**

4단계. 드롭다운 목록에서 억제 유형을 선택합니다.(규칙 또는 소스 또는 대상).

5단계. **확인**을 클릭하여 완료합니다.



이 규칙에 이벤트 필터가 추가된 후에는 규칙 표시 옆에 카운트 2가 있는 필터 아이콘을 볼 수 있어야 합니다. 이 경우 이 규칙에 대해 활성화된 두 개의 이벤트 필터가 있음을 나타냅니다.

1.7단계. 동적 상태 구성

지정된 조건이 일치하는 경우 규칙의 상태를 변경할 수 있는 기능입니다.

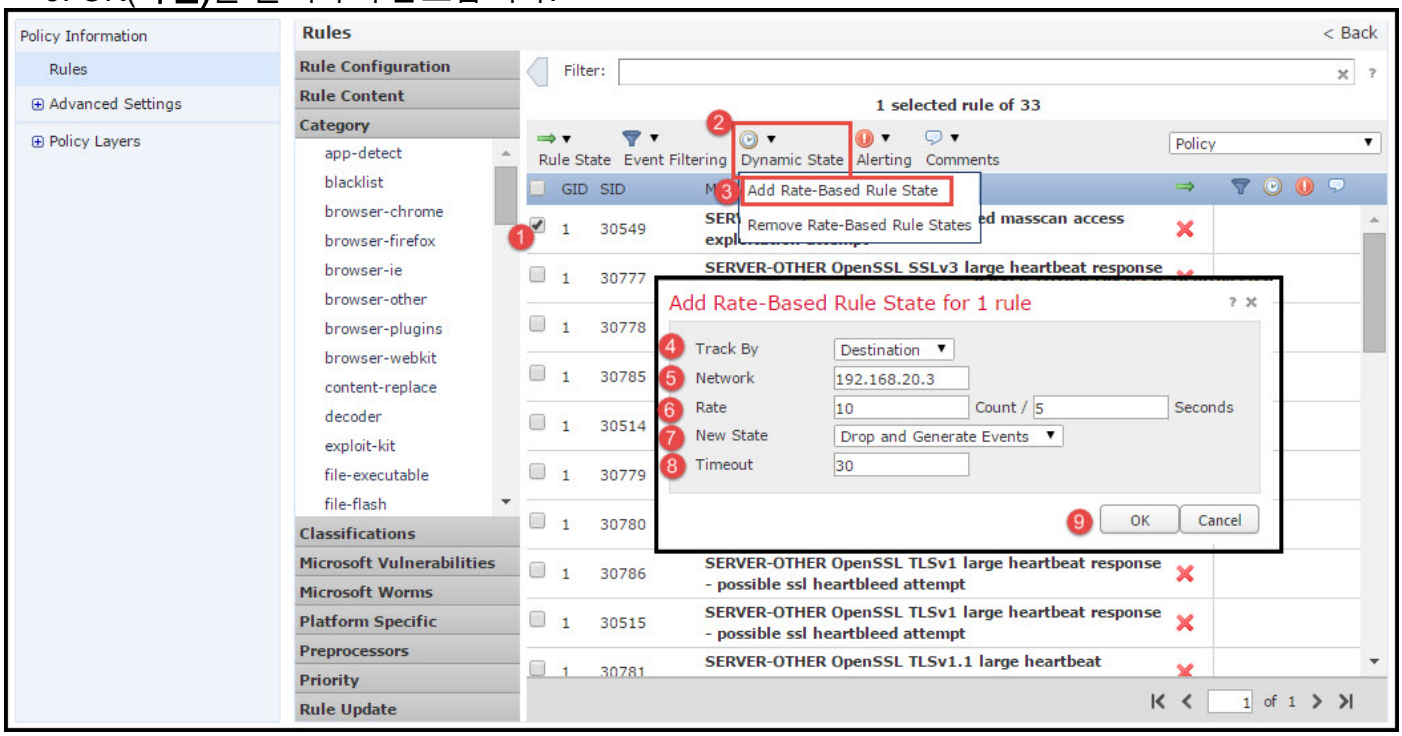
무작위 대입 공격으로 비밀번호를 해독하는 시나리오를 가정해 보겠습니다.서명이 비밀번호 실패 시도를 탐지하고 규칙 작업은 이벤트를 생성하는 것입니다.시스템은 비밀번호 실패 시도에 대한 경고를 계속 생성합니다.이 경우 **동적 상태**를 사용하여 **Generate Events**의 작업을 Drop and Generate Events로 변경하여 무작위의 대입 공격을 차단할 수 있습니다.

다음으로 이동 **규칙** 옵션이 탐색 패널에 표시되고 Rule Management 페이지가 나타납니다 .Dynamic(동적) 상태를 활성화할 규칙을 선택하고 옵션 Dynamic State(동적 상태) **> Add a Rate-base Rule State(속도 기반 규칙 상태 추가)를 선택합니다.**

속도 기반 규칙 상태를 구성하려면

1. 이벤트 임계값**을** 구성할 규칙을 선택합니다.
2. **Dynamic State(동적 상태)를 클릭합니다**.
3. Add **Rate-Based Rule State를 클릭합니다**.

4. Track By(추적 기준) 드롭다운 상자에서 규칙 상태를 추적할 방법을 선택합니다.(**규칙 또는 소스 또는 대상**).
5. **네트워크를 입력합니다**.단일 IP 주소, 주소 블록, 변수 또는 이러한 조합으로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다.
6. 이벤트 **수**와 타임스탬프를 초 단위로 입력합니다.
7. 규칙에 **대해** 정의할 **New State**를 선택합니다.
8. 규칙 상태를 **되돌리기** 전까지 Timeout을 입력합니다.
9. OK(**확인**)를 클릭하여 완료합니다.



2단계. NAP(Network Analysis Policy) 및 변수 집합 구성(선택 사항)

네트워크 분석 정책 구성

네트워크 액세스 정책을 프리프로세서로 합니다.프리프로세서는 패킷 리어셈블리를 수행하고 트래픽을 표준화합니다.부적절한 헤더 옵션 식별에 대한 네트워크 레이어 및 전송 레이어 프로토콜 이상을 식별하는 데 도움이 됩니다.

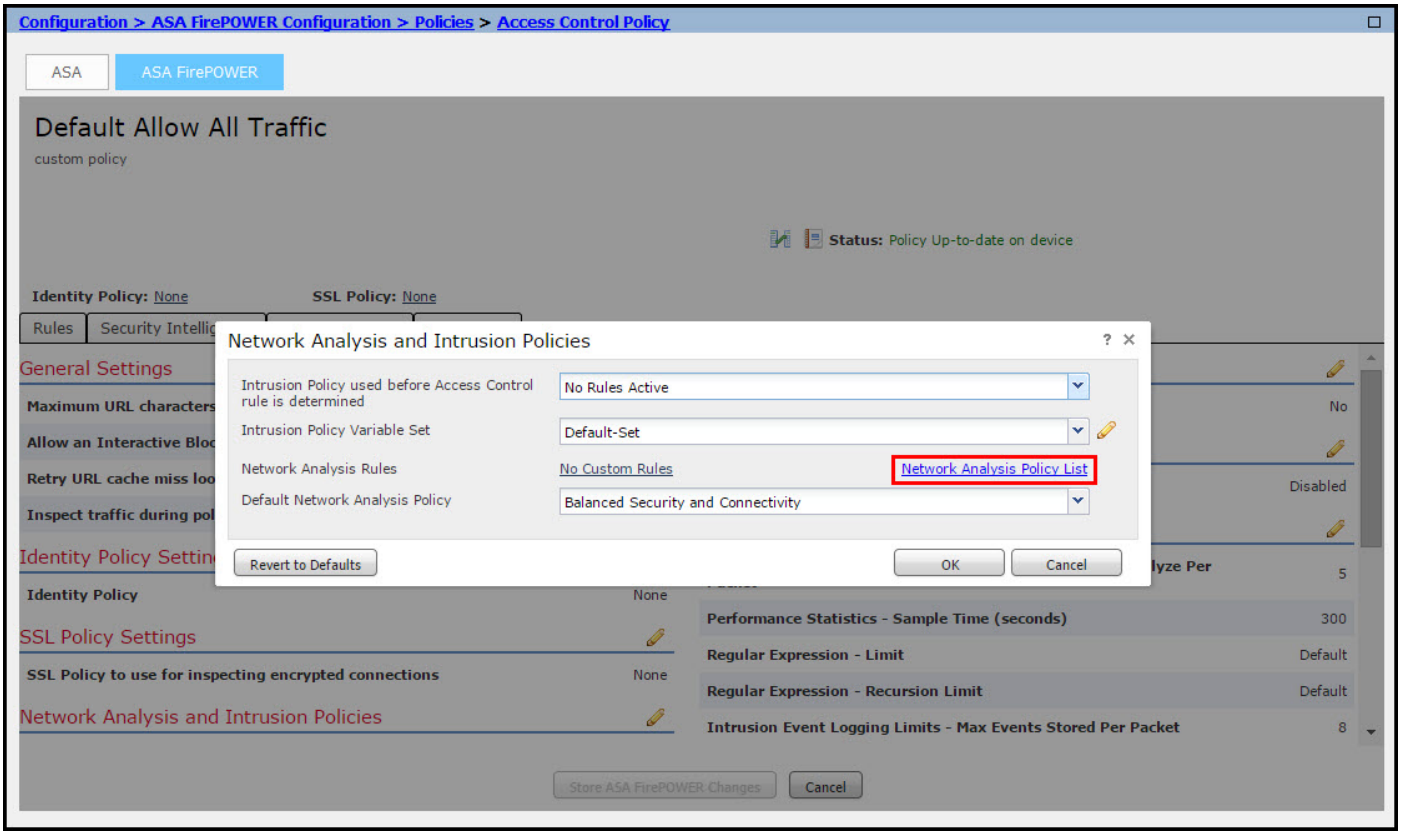
NAP는 IP 데이터그램의 디프래그먼트화를 수행하고, TCP 상태 저장 검사 및 스트림 리어셈블리를 제공하고, 체크섬을 검증합니다. 프리프로세서는 트래픽을 표준화하고, 프로토콜 표준을 검증 및 확인합니다.

각 프리프로세서에는 고유한 GID 번호가 있습니다.패킷에 의해 트리거된 프리프로세서를 나타냅니다.

네트워크 분석 정책을 구성하려면 Configuration(구성) **> ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책) > Advanced(고급) > Network Analysis and Intrusion Policy(네트워크 분석 및 침입 정책)로 이동합니다.**

기본 네트워크 분석 정책은 최적의 권장 정책인 Balanced Security and Connectivity입니다.드롭다운 목록에서 선택할 수 있는 NAP 정책을 제공하는 다른 3가지 시스템이 추가로 있습니다.

옵션 **Network Analysis Policy** List를 선택하여 사용자 지정 NAP 정책을 생성합니다.



변수 집합 구성

변수 집합은 소스 및 대상 주소와 포트를 식별하는 데 침입 규칙에서 사용됩니다.변수가 네트워크 환경을 보다 정확하게 반영하는 경우 규칙이 더 효과적입니다.변수는 성능 튜닝에서 중요한 역할을 합니다.

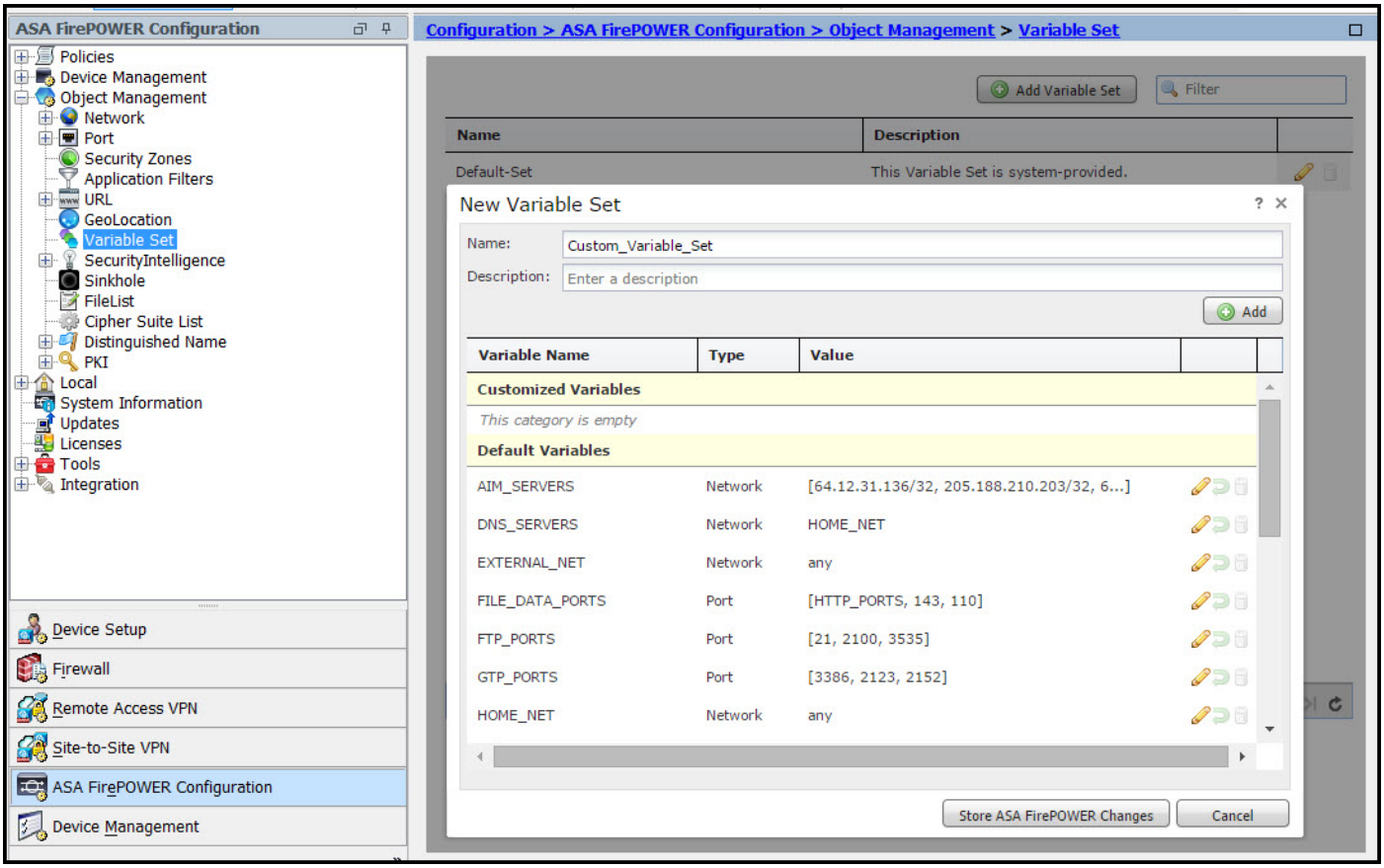
변수 집합이 기본 옵션(Network/Port)으로 이미 구성되었습니다. 기본 컨피그레이션을 변경하려면 새 변수 집합을 추가합니다.

변수 집합을 구성하려면 Configuration(구성) **> ASA Firepower Configuration(ASA Firepower 구성) > Object Management(개체 관리) > Variable Set(변수 집합)로 이동합니다**.Add Variable **Set** 옵션**을 선택하여** 새 변수 집합을 추가합니다.변수 집합 **이름**을 입력하고 설명을 **지정합니다.**

특정 포트에서 사용자 지정 애플리케이션이 작동하는 경우 Port number(포트 번호) 필드에 포트 번호를 정의합니다.네트워크 매개변수를 구성합니다.

$Home_NET에서 내부 네트워크를 지정합니다.

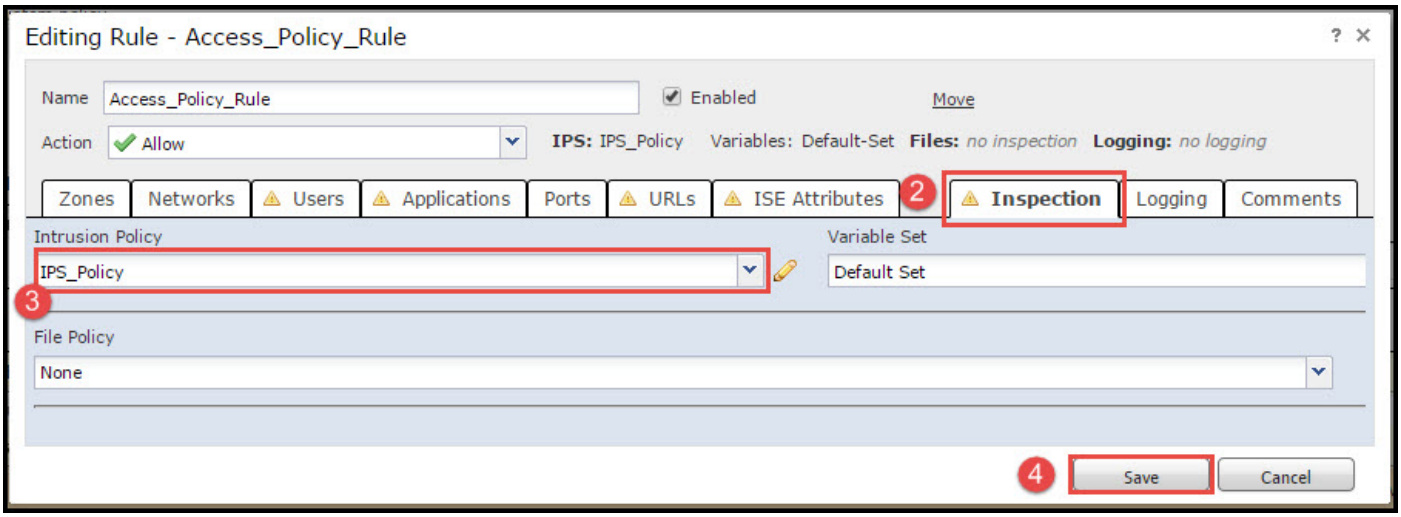
$External_NET에서 외부 네트워크를 지정합니다.



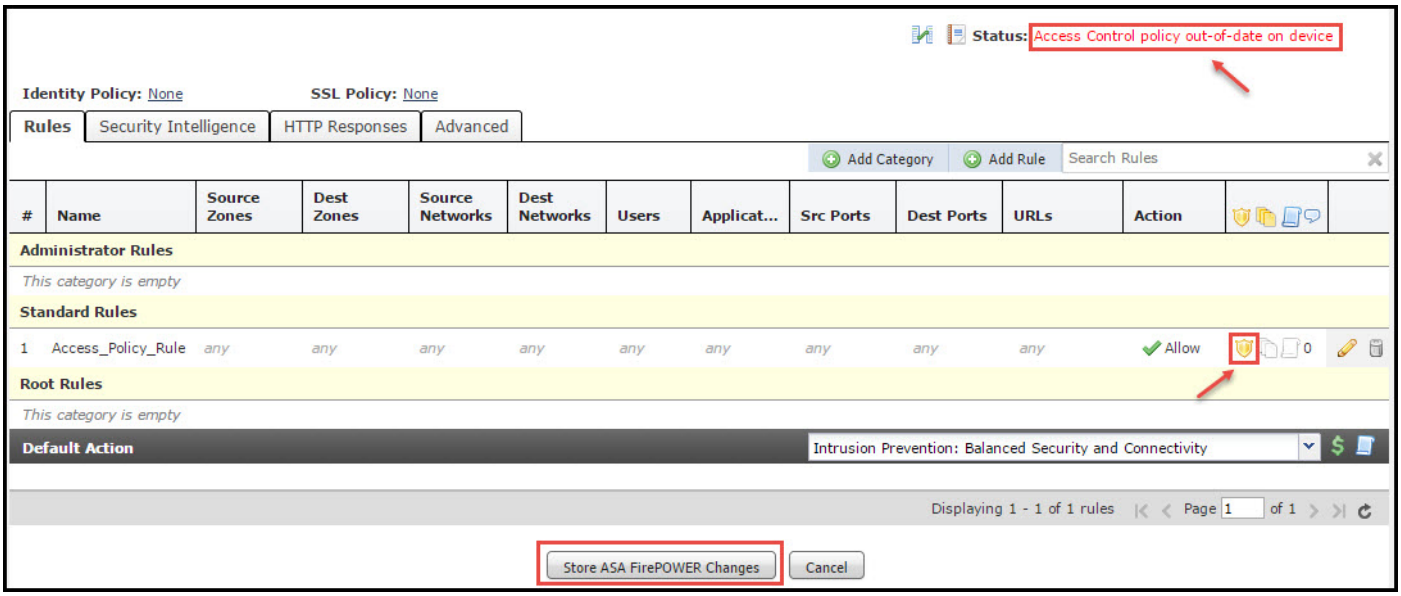
3단계:침입 정책/NAP/변수 집합을 포함하도록 액세스 제어 구성

Configuration(컨피그레이션) > **ASA Firepower Configuration(ASA Firepower 컨피그레이션) > Policies(정책) > Access Control Policy(액세스 제어 정책)로 이동합니다.**다음 단계를 완료해야 합니다.

1. 침입 정책을 할당할 Access Policy 규칙을 수정합니다.
2. 검사 탭을 **선택합니다.**
3. 드롭다운 목록에서 **Intrusion Policy**를 선택하고 **Variable Sets** from 드롭다운 목록을 선택합니다.
4. 저장을 **클릭합니다.**



침입 정책이 이 액세스 정책 규칙에 추가되었으므로침입 정책이 활성화되었음을 나타내는 실드 아이콘이 Golden Color에 표시됩니다.

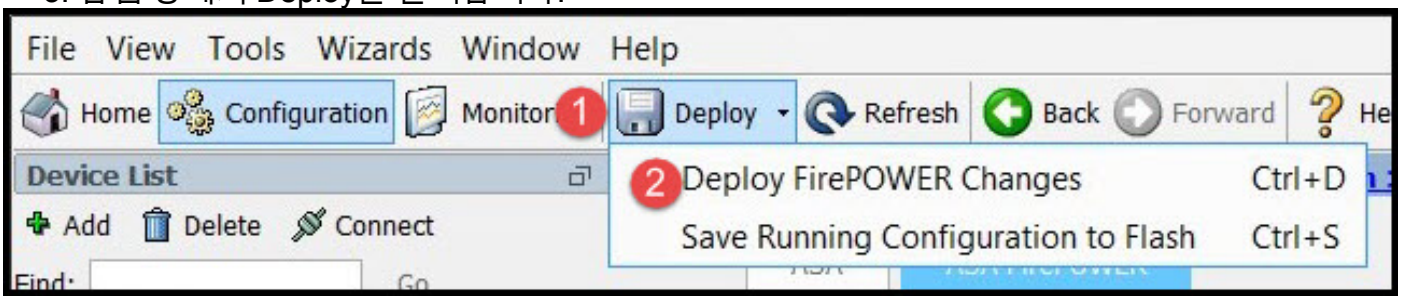


Store **ASA FirePOWER changes**를 클릭하여 변경 사항을 저장합니다.

4단계. 액세스 제어 정책 구축

이제 액세스 제어 정책을 구축해야 합니다.정책을 적용하기 전에 장치에 액세스 제어 정책이 최신 상태가 아님을 표시합니다. 센서에 변경 사항을 배포하려면 다음을 수행합니다.

1. Deploy를 **클릭합니다**.
2. Deploy **FirePOWER Changes를 클릭합니다**.
3. 팝업 창에서 Deploy를 클릭합니다.

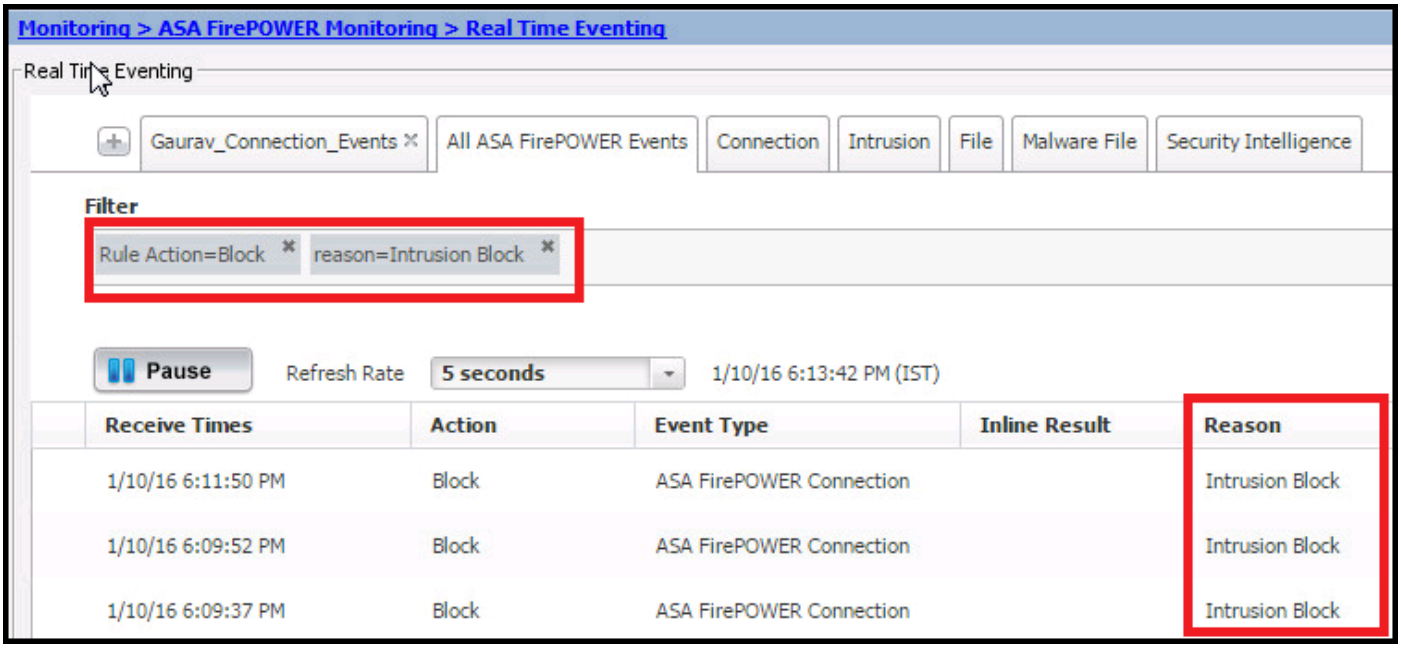


: 5.4.x Apply ASA FirePOWER Changes(ASA FirePOWER) .

: Monitoring() > **ASA Firepower Monitoring(ASA Firepower) > Task Status( ) .** .

5단계. 침입 이벤트 모니터링

FirePOWER Module에서 생성된 침입 이벤트를 보려면 **Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Real Time Eventing(실시간 이벤트 처리).**



다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

1단계. Rule State of Rules가 적절하게 구성되었는지 확인합니다.

2단계. 올바른 IPS 정책이 액세스 규칙에 포함되었는지 확인합니다.

3단계. 변수 집합이 올바르게 구성되었는지 확인합니다.변수 집합이 올바르게 구성되지 않으면 시그니처가 트래픽과 일치하지 않습니다.

4단계. 액세스 제어 정책 구축이 성공적으로 완료되었는지 확인합니다.

5단계. 연결 이벤트 및 침입 이벤트를 모니터링하여 트래픽 흐름이 올바른 규칙에 부합하는지 확인합니다.