Cisco Firepower System에서 통과 규칙 구성

목차

소개

이 문서에서는 통과 규칙, 규칙 생성 방법 및 침입 정책에서 이를 활성화하는 방법에 대해 설명합니다.

통과 규칙에 정의된 기준을 충족하는 패킷이 경고 규칙을 비활성화하는 대신 특정 상황에서 경고 규칙을 트리거하지 않도록 통과 규칙을 생성할 수 있습니다.기본적으로 통과 규칙은 경고 규칙을 재정의합니다.Firepower System은 각 규칙에 지정된 조건과 패킷을 비교하며, 패킷 데이터가 규칙에 지정된 모든 조건과 일치하면 규칙이 트리거됩니다.규칙이 경고 규칙이면 침입 이벤트가 생성됩니다.통과 규칙이면 트래픽을 무시합니다.

예를 들어, FTP 서버에 "anonymous" 사용자로 로그인하려는 시도를 찾는 규칙이 활성 상태를 유지하도록 할 수 있습니다.그러나 네트워크에 하나 이상의 합법적인 익명 FTP 서버가 있는 경우 해당 특정 서버에 대해 익명 사용자가 원래 규칙을 트리거하지 않도록 지정하는 통과 규칙을 작성하고 활성화할 수 있습니다.

> **주의:**통과 규칙이 기반으로 하는 원래 규칙이 개정을 수신하면 통과 규칙이 자동으로 업데이트되지 않습니다.따라서, 패스하는 것은 유지하기가 어려울 수 있다.

> **참고:**규칙에 대해 Suppression 기능을 활성화하면 해당 규칙에 대한 이벤트 알림이 억제됩니다.그러나 규칙은 여전히 평가됩니다.예를 들어 삭제 규칙을 누르면 규칙과 일치하는 패킷이 자동으로 삭제됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

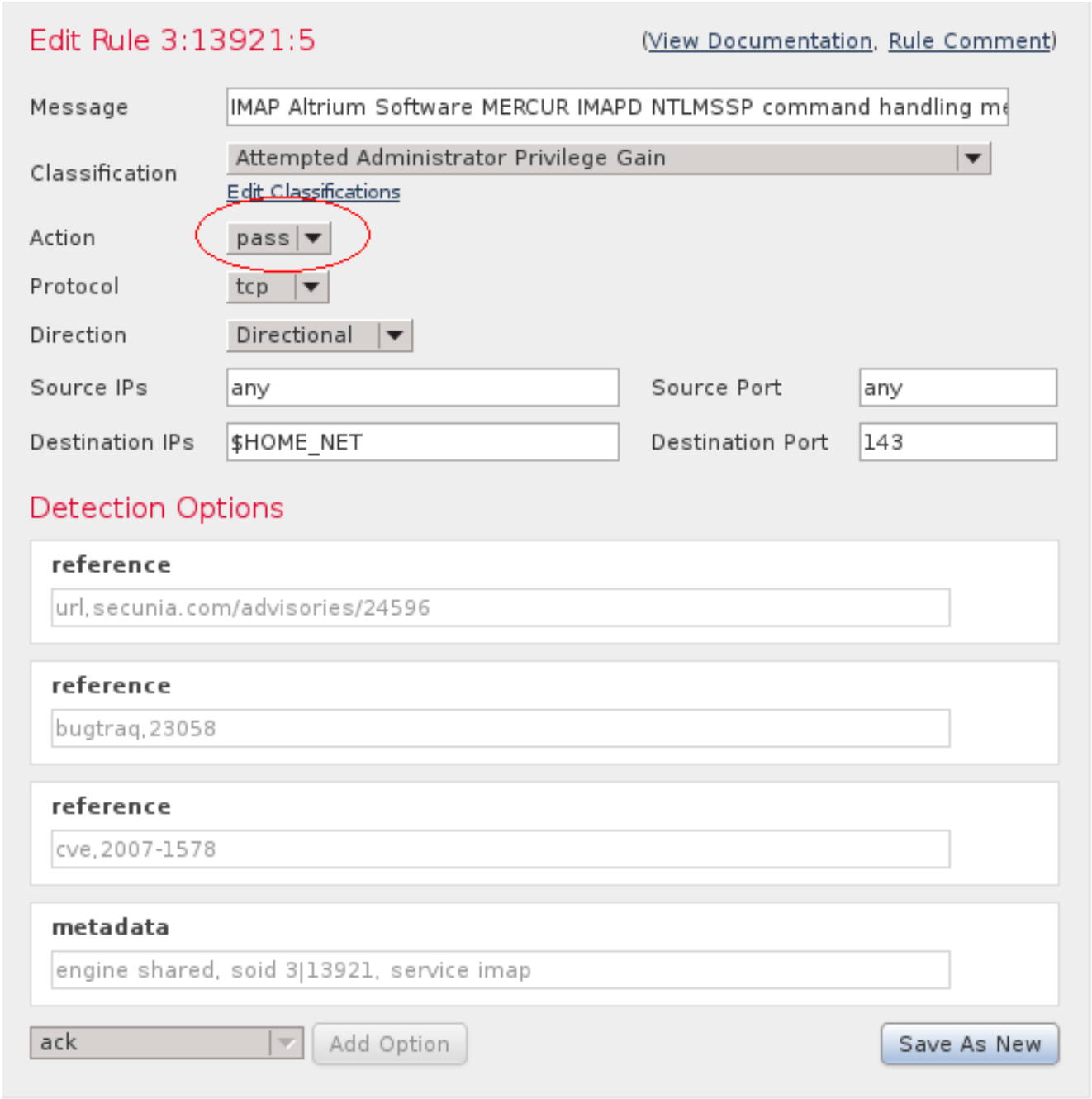
이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

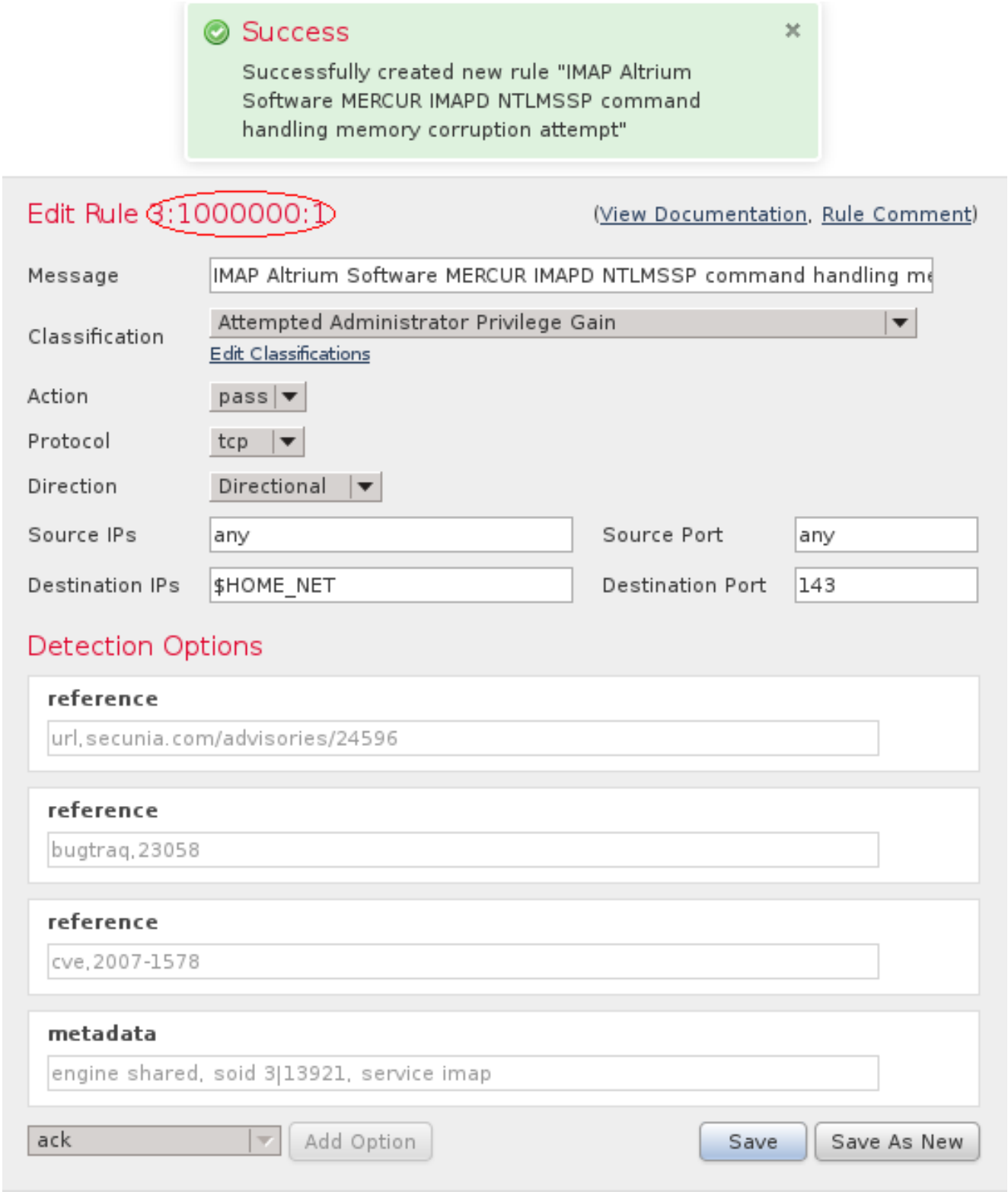
구성

통과 규칙 만들기

1. Objects **> Intrusion Rules로 이동합니다**.규칙 카테고리 목록이 나타납니다.
2. 필터링할 규칙과 연결된 규칙 카테고리를 찾습니다.화살표 아이콘을 사용하여 카테고리 목록에서 규칙 카테고리를 확장하고 통과 규칙을 만들 규칙을 찾습니다.또는 규칙 검색 상자를 사용할 수 있습니다.
3. 원하는 규칙을 찾은 후 규칙을 수정하려면 옆에 있는 연필 아이콘을 클릭합니다.
4. 규칙을 수정할 때 다음 단계를 완료합니다. 규칙에 해당하는 **Edit** 버튼을 클릭합니다.Action(작업) 드롭다운 목록에서 **pass(통과)**를 선택합니다.Source IPs(소스 IPs) 필드 및 Destination IPs(대상 IPs) 필드를 규칙에서 경고하지 않을 호스트 또는 네트워크로 변경합니다.Save **As New를 클릭합니다**
   .



5. 새 규칙의 ID 번호를 확인합니다.예를 들어, 1000000입니다.



통과 규칙 활성화

지정한 소스 또는 목적지 주소에서 트래픽을 전달하려면 적절한 침입 정책에서 새 규칙을 활성화해야 합니다.통과 규칙을 활성화하려면 다음 단계를 수행합니다.

1. 활성 침입 정책을 수정합니다. Policies(정책) **> Access Control(액세스 제어) > Intrusion(침입)으로 이동합니다**.활성 침입 정책 옆에 있는 **Edit**를 클릭합니다.
2. 규칙 목록에 새 규칙을 추가합니다. 왼쪽 창에서 Rules를 클릭합니다.필터 상자에 앞서 언급한 규칙 ID를 입력합니다.Rules 확인란을 선택하고 Rule State를 Generate Events로 **변경합니다** .왼쪽 창에서 **Policy Information**을 클릭합니다.Commit **Changes를 클릭합니다**.

3. 디바이스에 변경 사항을 구축하려면 Deploy를 클릭합니다.

다음을 확인합니다.

정의된 소스 또는 대상 IP 주소에 대해 이 특정 규칙에 대해 이벤트가 생성되지 않도록 하려면 일정 기간 동안 새 이벤트를 모니터링해야 합니다.

문제 해결

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