Snort 3 네트워크 분석 정책 시작하기

이 장에서는 네트워크 분석 정책의 기본 사항, 전제 조건, 네트워크 분석 정책을 관리하는 방법에 대한 인사이트를 제공합니다. 또한 사용자 지정 네트워크 분석 정책 생성 및 네트워크 분석 정책 설정에 대한 정보도 제공합니다.

네트워크 분석 정책 개요

네트워크 분석 정책은 많은 트래픽 전처리 옵션을 관리하며, 액세스 제어 정책의 고급 설정에 의해 호출됩니다. 네트워크 분석 관련 전처리는 보안 인텔리전스 매칭 및 SSL 암호 해독 후, 그리고 액세스 제어 규칙이 패킷을 자세히 조사하기 전과 모든 침입 또는 파일 검사가 시작되기 전에 수행됩니다.

기본적으로, 시스템은 *Balanced Security and Connectivity*(균형 잡힌 보안 및 연결성) 네트워크 분석 정책을 사용하여 액세스 제어 정책에서 처리된 모든 트래픽을 전처리합니다. 그러나, 사용자는 이 전처리를 수행하는 기타 기본 네트워크 분석 정책을 선택할 수 있습니다. 사용자 편의를 위해, 시스템은 Cisco Talos(Talos Intelligence Group)가 보안 및 연결의 특정 균형을 위해 조정한 변경할 수 없는 여러 네트워크 분석 정책 선택권을 제공합니다. 또한 맞춤형 전처리 설정이 있는 맞춤형 네트워크 분석 정책을 만들 수도 있습니다.

팁 시스템이 제공하는 침입 및 네트워크 분석 정책은 이름은 유사하지만 다른 구성을 포함합니다. 예를 들어, Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책 및 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입 정책은 함께 작동하며 침입 규칙 업데이트에서 모두 업데이트될 수 있습니다. 하지만, 네트워크 분석 정책은 주로 전처리 옵션을 제어하는 반면, 침입 정책은 주로 침입 규칙을 제어합니다. 네트워크 분석 및 칩임 정책은 함께 작동하여 트래픽을 검색합니다.

또한 여러 맞춤형 네트워크 분석 정책을 작성한 다음, 다른 트래픽을 전처리하도록 할당하여 특정 보안 영역, 네트워크 및 VLAN에 맞게 트래픽 전처리 옵션을 조정할 수도 있습니다. (ASA FirePOWER은 VLAN에 의한 전처리를 제한할 수 없는 점에 유의하십시오.)

네트워크 분석 정책 관리

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

툴바에서 사용자 이름 하단에 시스템이 사용 가능한 도메인 트리를 표시합니다. 도메인을 전환하려면 액세스하려는 도메인을 선택합니다.

단계 **1** 네트워크 분석 정책에 액세스하려면 다음 경로 중 하나를 선택합니다.

- **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**
- **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**
- **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policy(**네트워크 분석 정책**)**

참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

단계 **2** 네트워크 분석 정책을 관리합니다.

- 비교 - **Compare Policies(**정책 비교**)**를 클릭합니다(*Cisco Secure Firewall Management Center* 구성 가이드에 있는 정책 비교 참조).

  참고 Snort 2 정책만 비교할 수 있습니다.

- 생성 - 새 네트워크 분석 정책을 생성하려면 **Create Policy(**정책 생성**)**를 클릭합니다.

  네트워크 분석 정책의 두 가지 버전인 **Snort 2 Version(Snort 2** 버전**)**과 **Snort 3 Version(Snort 3** 버전**)**이 생성됩니다.

  - Snort 2 버전의 경우 *Cisco Secure Firewall Management Center* 구성 가이드에 있는 *Snort 2*에 대한 사용자 지정 네트워크 분석 정책 생성을 참조하십시오.
  - Snort 3 버전의 경우 Snort 3에 대한 맞춤형 네트워크 분석 정책 생성, 5 페이지의 내용을 참조하십시오.

- 삭제 - 네트워크 분석 정책을 삭제하려면 **Delete(**삭제**)** 아이콘을 클릭하고 정책 삭제 여부를 확인합니다. 액세스 제어 정책이 네트워크 분석 정책을 참조하는 경우 이를 삭제할 수 없습니다.

  컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

- 편집 - 기존 네트워크 분석 정책을 편집하려면 **Edit(**편집**)** 아이콘을 클릭합니다.

View(보기**)** ()가 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

- 보고서 - **Report(**보고서**)** 아이콘을 클릭합니다(*Cisco Secure Firewall Management Center* 구성 가이드에 있는 현재 정책 보고서 생성 참조).

네트워크 분석 정책에 사용되는 Snort 3 정의 및 용어

다음 표에는 네트워크 분석 정책에 사용되는 Snort 3 개념과 용어가 나와 있습니다.

표 *1:* 네트워크 분석 정책에 사용되는 ***Snort 3*** 정의 및 용어

용어	설명
검사기	검사기는 Snort 2 전처리기와 유사하게 패킷을 처리하는 플러그인입니다.
바인더 검사기	바인더 검사기는 특정 검사기가 액세스하여 고려해야 하는 경우 흐름을 정의합니다. 트래픽이 바인더 검사기에 정의된 조건과 일치하면 해당 검사기의 값/구성만 적용됩니다. 자세한 내용은 Snort 3에 대한 맞춤형 네트워크 분석 정책 생성, 5 페이지의 바인더 검사기를 참조하십시오.
싱글톤 검사기	싱글톤 검사기에는 하나의 인스턴스가 포함됩니다. 싱글톤 검사기는 멀티톤 검사기와 같이 인스턴스 추가를 지원하지 않습니다. 싱글톤 검사기의 설정은 특정 트래픽 세그먼트가 아닌 해당 검사기와 일치하는 전체 트래픽에 적용됩니다. 자세한 내용은 Snort 3에 대한 맞춤형 네트워크 분석 정책 생성, 5 페이지의 싱글톤 검사기를 참조하십시오.
멀티톤 검사기	멀티톤 검사기에는 필요에 따라 구성할 수 있는 여러 인스턴스가 포함되어 있습니다. 멀티톤 검사기는 네트워크, 포트, VLAN 등의 특정 조건을 기반으로 설정 구성을 지원합니다. 지원되는 설정 세트 하나를 인스턴스라고 합니다. 자세한 내용은 Snort 3에 대한 맞춤형 네트워크 분석 정책 생성, 5 페이지의 멀티톤 검사기를 참조하십시오.

용어	설명
스키마	스키마 파일은 OpenAPI JSON 사양을 기반으로 하며 업로드되거나 다운로드되는 콘텐츠를 확인합니다. Swagger 편집기와 같은 서드파티 JSON 편집기를 사용하여 스키마 파일을 다운로드하고 열 수 있습니다. 스키마 파일은 사용할 수 있는 허용되는 값, 범위 및 허용되는 패턴을 사용하여 검사기에 대해 구성할 수 있는 매개변수를 식별하는 데 도움이 됩니다. 자세한 내용은 네트워크 분석 정책 사용자 정의, 13 페이지를 참고하십시오.
샘플 파일	예제 구성이 포함된 기본 제공 템플릿으로, 검사기를 구성하는 데 도움이 됩니다. 샘플 파일에 포함된 예제 구성을 참조하여 필요에 따라 변경할 수 있습니다. 자세한 내용은 네트워크 분석 정책 사용자 정의, 13 페이지를 참고하십시오.
전체 구성	전체 검사기 구성을 단일 파일로 다운로드할 수 있습니다. 검사기 구성과 관련된 모든 정보를 이 파일에서 사용할 수 있습니다. 전체 구성은 기본 구성(Cisco Talos에서 LSP 업데이트의 일부로 배포)과 사용자 지정 NAP 검사기 구성을 병합한 구성입니다. 자세한 내용은 네트워크 분석 정책 사용자 정의, 13 페이지를 참고하십시오.

용어	설명
재정의된 구성	네트워크 분석 정책의 **Snort 3 Version(Snort 3 버전)** 페이지에서 다음과 같이 합니다. • **Actions(작업)** > **Upload(업로드)**에서 **Overridden Configuration(재정의된 구성)**을 클릭하여 재정의된 구성이 포함된 JSON 파일을 업로드할 수 있습니다. • **Actions(작업)** > **Download(다운로드)**에서 **Overridden Configuration(재정의된 구성)**을 클릭하여 재정의된 검사기 구성을 다운로드할 수 있습니다. 검사기 구성을 재정의하지 않은 경우 이 옵션은 비활성화됩니다. 검사기 구성을 재정의하면 이 옵션이 자동으로 활성화되어 다운로드할 수 있습니다. 자세한 내용은 네트워크 분석 정책 사용자 정의, 13 페이지를 참고하십시오.

관련 항목

Snort 3에 대한 맞춤형 네트워크 분석 정책 생성, 5 페이지
네트워크 분석 정책 사용자 정의, 13 페이지
네트워크 분석 정책 매핑, 11 페이지

네트워크 분석 및 침입 정책 사전 요건

Snort 검사기 엔진이 침입 및 악성코드 분석을 위해 트래픽을 처리하도록 허용하려면 Threat Defense 디바이스에 대해 활성화된 IPS 라이선스가 있어야 합니다.

네트워크 분석, 침입 정책을 관리하고 마이그레이션 작업을 수행하려면 관리자 사용자여야 합니다.

Snort 3에 대한 맞춤형 네트워크 분석 정책 생성

기본 네트워크 분석 정책은 일반적인 네트워크 요구 사항 및 최적의 성능에 맞게 조정됩니다. 일반적으로 기본 네트워크 분석 정책은 대부분의 네트워크 요구 사항을 충족하므로 정책을 사용자 정의하지 않아도 됩니다. 그러나 특정 네트워크 요구 사항이 있거나 성능 문제가 발생할 경우 기본 네트워크 분석 정책을 사용자 지정할 수 있습니다. 네트워크 분석 정책을 사용자 지정하는 것은 고급 사용자 또는 Cisco 지원만 수행해야 하는 고급 구성입니다.

Snort 3의 네트워크 분석 정책 구성은 JSON 및 JSON 스키마를 사용하는 데이터 기반 모델입니다. OpenAPI 사양을 기반으로 하는 스키마를 통해 지원되는 검사기, 설정, 설정 유형 및 유효한 값을 확

인할 수 있습니다. Snort 3 검사기는 Snort 2 전처리기와 유사하게 패킷을 처리하는 플러그인입니다. 네트워크 분석 정책 구성은 JSON 형식으로 다운로드할 수 있습니다.

Snort 3의 검사기 및 설정 목록은 Snort 2 전처리기 및 설정 목록과 일대일로 매핑되지 않습니다. 또한 Snort 3에서 지원하는 검사기 및 설정의 일부만 management center에서 사용할 수 있습니다. Snort 3에 대한 자세한 내용은 https://snort.org/snort3 항목을 참조하십시오. management center에서 사용 가능한 검사기에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors 항목을 참조하십시오.

참고

- management center를 7.0 릴리스로 업그레이드하는 동안 네트워크 분석 정책의 Snort 2 버전에서 수행된 변경 사항은 업그레이드 후에 Snort 3로 마이그레이션되지 않습니다.
- 침입 정책과 달리 Snort 2 네트워크 분석 정책 설정을 Snort 3에 동기화하는 옵션은 없습니다.

기본 검사기 업데이트

LSP(Lightweight Security Package) 업데이트에는 새 검사기 또는 기존 검사기 구성의 정수 범위 수정 사항이 포함될 수 있습니다. LSP를 설치하고 나면 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**의 **Inspectors(**검사기**)** 아래에서 새 검사기 및 업데이트된 범위를 사용할 수 있습니다.

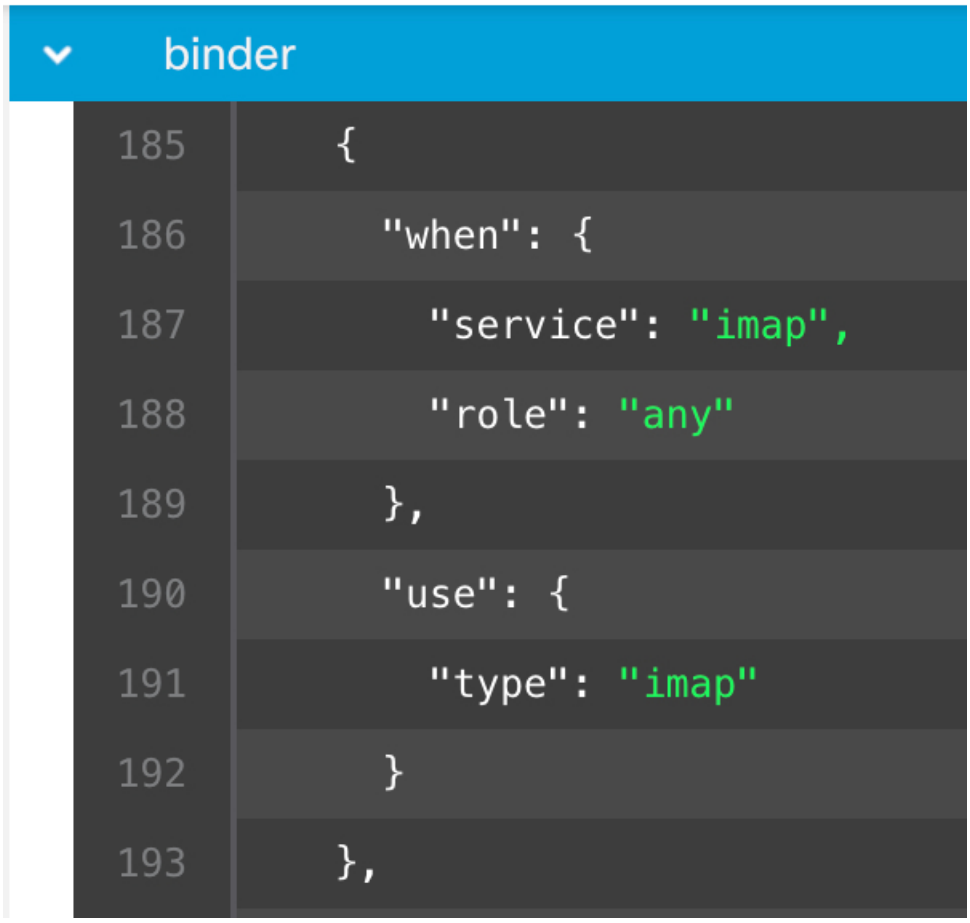
바인더 검사기

바인더 검사기는 특정 검사기가 액세스하여 고려해야 하는 경우 흐름을 정의합니다. 트래픽이 바인더 검사기에 정의된 조건과 일치하면 해당 검사기의 값/구성만 적용됩니다. 예를 들면 다음과 같습니다.

imap 검사기의 경우 바인더는 액세스할 때 다음 조건을 정의합니다. 다음의 경우에 해당합니다.

- 서비스가 imap와 같습니다.
- 역할이 any와 같습니다.

이러한 조건이 충족되면 imap 유형을 사용합니다.



싱글톤 검사기

싱글톤 검사기에는 하나의 인스턴스가 포함됩니다. 싱글톤 검사기는 멀티톤 검사기와 같이 인스턴스 추가를 지원하지 않습니다. 싱글톤 검사기의 설정은 특정 트래픽 세그먼트가 아닌 전체 트래픽에 적용됩니다.

예를 들면 다음과 같습니다.

```
{
   "normalizer":{
      "enabled":true,
      "type":"singleton",
      "data":{
         "ip4":{
            "df":true
         }
      }
   }
}
```

멀티톤 검사기

멀티톤 검사기에는 필요에 따라 구성할 수 있는 여러 인스턴스가 포함되어 있습니다. 멀티톤 검사기는 네트워크, 포트, VLAN 등의 특정 조건을 기반으로 설정 구성을 지원합니다. 지원되는 설정 세트 하나를 인스턴스라고 합니다. 기본 인스턴스가 있으며 특정 조건에 따라 인스턴스를 더 추가할 수도 있습니다. 트래픽이 해당 조건과 일치하면 해당 인스턴스의 설정이 적용됩니다. 그렇지 않은 경우 기본 인스턴스의 설정이 적용됩니다. 또한 기본 인스턴스의 이름은 검사기의 이름과 동일합니다.

멀티톤 검사기의 경우 재정의된 검사기 구성을 업로드할 때 JSON 파일의 각 인스턴스에 대해 일치하는 바인더 조건(검사기가 액세스 또는 사용되어야 하는 조건)도 포함/정의해야 합니다. 그렇지 않으면 업로드 오류가 발생합니다. 새 인스턴스를 생성할 수도 있지만 오류를 방지하기 위해 생성하는 모든 새 인스턴스에 대해 바인더 조건을 포함해야 합니다.

예를 들면 다음과 같습니다.

- 기본 인스턴스가 수정된 멀티톤 검사기

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   }
}
```

- 기본 인스턴스와 기본 바인더가 수정된 멀티톤 검사기

```
{
   "http_inspect":{
      "enabled":true,
      "type":"multiton",
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "type":"binder",
      "enabled":true,
      "rules":[
         {
            "use":{
               "type":"http_inspect"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
```

```
            }
        ]
    }
}
```

- 사용자 지정 인스턴스와 사용자 지정 바인더가 추가된 멀티톤 검사기

```
{
    "http_inspect":{
        "enabled":true,
        "type":"multiton",
        "instances":[
            {
                "name":"http_inspect1",
                "data":{
                    "response_depth":5000
                }
            }
        ]
    },
    "binder":{
        "type":"binder",
        "enabled":true,
        "rules":[
            {
                "use":{
                    "type":"http_inspect",
                    "name":"http_inspect1"
                },
                "when":{
                    "role":"any",
                    "ports":"8080",
                    "proto":"tcp",
                    "service":"http"
                }
            }
        ]
    }
}
```

CIP(Common Industrial Protocol) Safety

CIP(Common Industrial Protocol) Safety는 디바이스의 안전한 작동을 지원하는 CIP의 확장 집합입니다. 또한 CIP 네트워크의 서로 다른 노드 간 페일 세이프 통신도 제공합니다.

CIP Safety 프로토콜은 다음 두 가지 주요 구성 요소로 구성됩니다.

- CIP Safety 세그먼트 - Forward Open(전송 열기) 메시지에서 후속 보안 세션을 위한 보안 매개변수를 교환하는 데 사용됩니다.
- CIP Safety 메시지 - 실제 보안 정보 교환에 사용됩니다.

CIP 검사기는 다음 항목을 탐지 및 식별합니다.

- 서비스형 CIP 및 클라이언트
- CIP Read, CIP Admin, CIP Infrastructure, CIP Write와 같은 페이로드

CIP 검사기는 CIP 세그먼트를 구문 분석하고 Forward Open(전송 열기) 요청에서 CIP 보안 세그먼트를 탐지할 수 있습니다.

CIP Safety 기능을 테스트하려면 CIP 검사기를 활성화해야 합니다. CIP 패킷의 보안 세그먼트 탐지 및 차단, 10 페이지의 내용을 참조하십시오.

CIP 패킷의 보안 세그먼트 탐지 및 차단

활용 사례: CIP Safety 세그먼트를 탐지 및 차단하는 동시에 다른 CIP 패킷은 허용하는 경우:

- **cip_safety**라는 사용자 지정 네트워크 분석 정책을 만듭니다.
- 액세스 제어 정책에서 액세스 제어 규칙을 생성하여 CIP Safety를 차단하고 다른 모든 패킷을 허용합니다.

CIP Safety 기능을 테스트하려면 Management Center에서 CIP 검사기를 활성화하고 액세스 제어 정책에 할당합니다.

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** 생성한 네트워크 분석 정책 **cip_safety**의 **Snort 3** 버전을 클릭합니다.

단계 **3** **Inspectors(**검사기**)**에서 **cip**를 클릭하여 확장합니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다.

단계 **4** 오른쪽 열의 **Overridden Configuration(**재정의된 구성**)**에서 **Edit Inspector(**검사기 편집**)** 아이콘을 클릭하고 **cip**의 "enabled(활성화됨)" 필드를 false(기본값)에서 true로 변경합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** **cip** 검사기를 액세스 제어 정책에 할당하려면 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Edit(**편집**)**을 선택하고 패킷 플로우 라인 끝에 있는 **More(**더 보기**)** 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)** 옵션을 선택합니다.

단계 **8** **Network Analysis and Intrusion Policies(**네트워크 분석 및 침입 정책**)** 옆에 있는 수정( )을 클릭합니다.

단계 **9** **Network Analysis and Intrusion Policies(**네트워크 분석 및 침입 정책**)** 창에서 **Default Network Analysis Policy(**기본 네트워크 분석 정책**)** 드롭다운 목록에서 생성한 액세스 제어 정책 **cip_safety**를 선택합니다.

이제 CIP 검사기가 Management Center에서 활성화되며 CIP Safety를 차단하고 다른 모든 CIP 패킷을 허용하는 사용자 지정 액세스 제어 규칙을 생성할 수 있습니다.

단계 **10** CIP 안전 패킷 플로우를 포함하는 라이브 트래픽을 전송한 후에는 **Connection Events(**연결 이벤트**)**로 이동하여 페이로드가 이 절차에서 언급하는 탐지 및 차단 활용 사례에 대한 CIP Safety 패킷 로그를 포함하는 예상 페이로드인지 확인합니다. **CIP**는 애플리케이션 프로토콜 및 클라이언트로 탐지되며(**Application Protocol(**애플리케이션 프로토콜**)**, **Client(**클라이언트**)** 필드 참조), **CIP Safety**는 **Web Application(**웹 애플리케이션**)** 필드에 표시됩니다.

네트워크 분석 정책 매핑

네트워크 분석 정책의 경우 Cisco Talos는 Snort 3 버전에 해당하는 Snort 2 버전의 정책을 찾는 데 사용되는 매핑 정보를 제공합니다.

이 매핑을 통해 Snort 3 버전의 정책이 해당하는 Snort 2 버전을 사용할 수 있습니다.

네트워크 분석 정책 매핑 보기

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** **NAP Mapping(NAP** 매핑**)**을 클릭합니다.

단계 **3** **View Mappings(**매핑 보기**)**의 화살표를 확장합니다.

Snort 2에 해당하는 정책에 자동으로 매핑되는 Snort 3 네트워크 분석 정책이 표시됩니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

네트워크 분석 정책 생성

기존의 모든 네트워크 분석 정책은 해당 Snort 2 및 Snort 3 버전과 함께 management center에서 사용할 수 있습니다. 새 네트워크 분석 정책을 생성하면 정책이 Snort 2 버전과 Snort 3 버전 모두로 생성됩니다.

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** **Create Policy(**정책 생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **4** **Base Policy(**기본 정책**)**를 선택하고 **Save(**저장**)**를 클릭합니다.

새 네트워크 분석 정책을 생성하면 해당하는 **Snort 2** 버전 및 **Snort 3** 버전으로 생성됩니다.

네트워크 분석 정책 수정

네트워크 분석 정책을 수정하여 이름, 설명 또는 기본 정책을 변경할 수 있습니다.

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** **Edit(**편집**)**을 클릭하여 이름, 설명, 검사 모드 또는 기본 정책을 변경합니다.

주의 **Detection(**탐지**)** 모드 사용 중단: Management Center 7.4.0부터는 NAP(네트워크 분석 정책)의 경우 **Detection(**탐지**)** 검사 모드가 더 이상 사용되지 않으며 이후 릴리스에서 제거될 예정입니다.

Detection(탐지**)** 모드는 트래픽을 삭제(즉, 삭제될 트래픽을 표시)하도록 설정하기 전에 검사를 활성화하고 네트워크에서 작동하는 방식을 확인할 수 있도록 테스트 모드로 사용되었습니다.

모든 검사기 삭제가 규칙 상태에 의해 제어되고 각 검사기 삭제를 설정하여 이벤트를 생성할 수 있게 되면 이 동작이 개선됩니다. 이는 트래픽을 삭제하도록 규칙 상태를 구성하기 전에 테스트하기 위한 것입니다. 이제 Snort 3의 트래픽 삭제를 세부적으로 제어할 수 있으므로 **Detect(**탐지**)** 모드는 제품을 복잡하게 만들 뿐이고 필요하지 않으므로 탐지 모드가 더 이상 사용되지 않습니다.

Detection(탐지**)** 모드의 NAP를 **Prevention(**방지**)**으로 변경하는 경우 침입 이벤트의 트래픽을 처리하고 "would have dropped(삭제되었을 것)" 결과를 갖는 NAP는 이제 "삭제"되며 해당 트래픽이 이러한 이벤트의 트래픽을 삭제합니다. 이는 GID가 1 또는 3이 아닌 규칙에 적용됩니다. GID 1 및 3은 텍스트/컴파일된 규칙(일반적으로 Talos에서 제공하거나 사용자 지정/가져온 규칙)이며, 기타 모든 GID는 변칙에 대한 검사입니다. 이는 네트워크에서 트리거되는 좀 더 드문 규칙입니다. **Prevention(**방지**)** 모드로 변경하면 트래픽에 영향을 미치지 않습니다. 삭제된 트래픽에 적용 가능한 침입 규칙을 비활성화하고 단지 생성 또는 비활성화로 설정해야 합니다.

검사 모드로 **Prevention(**방지**)**을 선택하는 것이 좋지만 **Prevention(**방지**)**을 선택하는 경우 **Detection(**탐지**)** 모드로 되돌릴 수 없습니다.

참고 네트워크 분석 정책 이름, 설명, 기본 정책 및 검사 모드를 수정하면 Snort 2 및 Snort 3 버전에 모두 수정 사항이 적용됩니다. 특정 버전의 검사 모드를 변경하려는 경우 해당 버전의 네트워크 분석 정책 페이지에서 이 작업을 수행할 수 있습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

네트워크 분석 정책 페이지에서 검사기 검색

네트워크 분석 정책의 Snort 3 버전 페이지에서 검색 창에 관련 텍스트를 입력하여 검사기를 검색해야 할 수 있습니다.

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**으로 이동합니다.

단계 **3** **Search(**검색**)** 창에 검색할 검사기 이름 또는 관련 텍스트를 입력합니다.

검색한 텍스트와 일치하는 모든 검사기가 표시됩니다.

예를 들어, **pop**을 입력하면 팝 검사기와 바인더 검사기가 일치하는 결과로 화면에 표시됩니다.

관련 항목

사용자 지정 네트워크 분석 정책 구성의 예, 21 페이지
재정의 항목이 있는 검사기 목록 보기, 18 페이지

네트워크 분석 정책에 사용되는 Snort 3 정의 및 용어, 3 페이지
네트워크 분석 정책 사용자 정의, 13 페이지
검사기에 대한 인라인 수정으로 구성 재정의, 16 페이지

검사기 구성 복사

요구 사항에 따라 네트워크 분석 정책의 Snort 3 버전에 대한 검사기 구성을 복사할 수 있습니다.

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**으로 이동합니다.

단계 **3** **Inspectors(**검사기**)**에서 구성을 복사할 필수 검사기를 확장합니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다.

단계 **4** 다음 중 하나 또는 모두의 검사기 구성을 클립보드에 복사하려면 **Copy to clipboard(**클립보드에 복사**)** 아이콘을 클릭합니다.

- 왼쪽 열의 **Default Configuration(**기본 컨피그레이션**)**
- 오른쪽 열의 **Overriden Configuration(**재정의된 컨피그레이션**)**

단계 **5** 필요한 사항을 수정하려면 복사한 검사기 구성을 JSON 편집기에 붙여 넣습니다.

관련 항목

네트워크 분석 정책 사용자 정의, 13 페이지

네트워크 분석 정책 사용자 정의

요구 사항에 따라 네트워크 분석 정책의 Snort 3 버전을 사용자 정의할 수 있습니다.

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

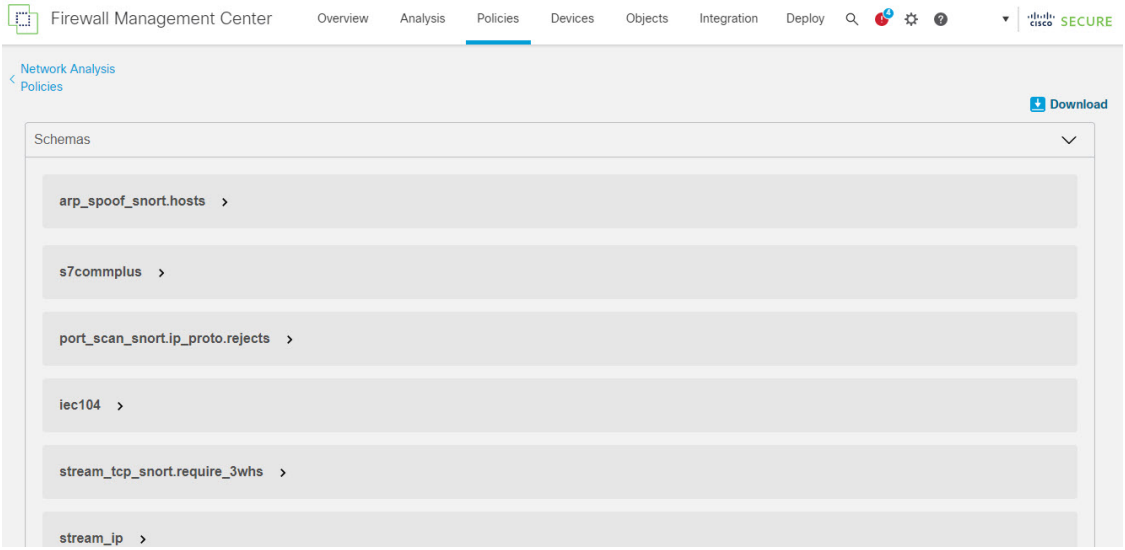
단계 **2** 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**으로 이동합니다.

단계 **3** **Actions(**작업**)** 드롭다운 메뉴를 클릭합니다.

다음 옵션이 표시됩니다.

- 스키마 보기
- 스키마 다운로드/샘플 파일/템플릿 다운로드
- 전체 설정 다운로드
- 재정의 설정 다운로드
- 재정의 설정 업로드

단계 4 브라우저에서 스키마 파일을 직접 열려면 **View Schema(**스키마 보기**)**를 클릭합니다.



단계 5 필요에 따라 스키마 파일, 샘플 파일/템플릿, 전체 구성 또는 재정의된 구성을 다운로드할 수 있습니다.

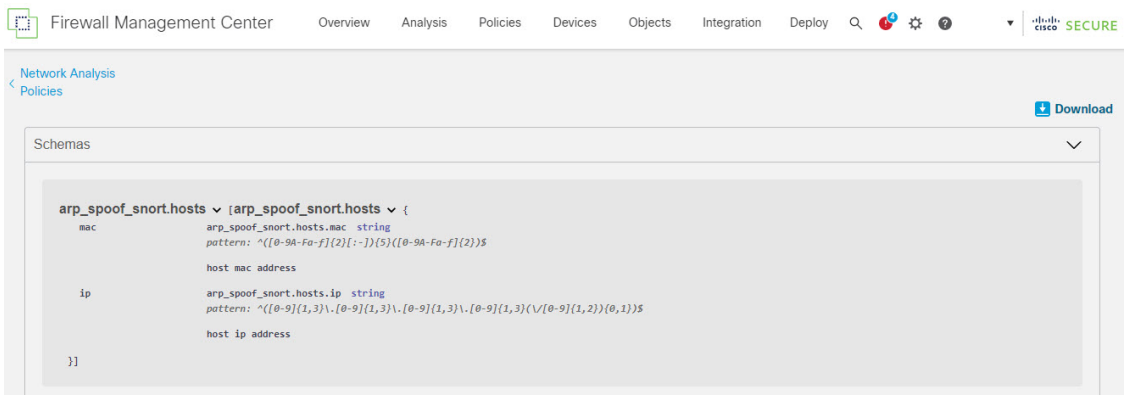
이러한 옵션은 허용되는 값, 범위 및 패턴, 기존 및 기본 검사기 구성, 재정의된 검사기 구성에 대한 통찰력을 제공합니다.

a) **Download Schema(**스키마 다운로드**)**를 클릭하여 스키마 파일을 다운로드합니다.

스키마 파일은 업로드하거나 다운로드하는 콘텐츠를 확인합니다. 서드파티 JSON 편집기를 사용하여 스키마 파일을 다운로드하고 열 수 있습니다. 스키마 파일은 사용할 수 있는 허용되는 값, 범위 및 허용되는 패턴을 사용하여 검사기에 대해 구성할 수 있는 매개변수를 식별하는 데 도움이 됩니다.

예를 들어 *arp_spoof_snort* 검사기의 경우 호스트를 구성할 수 있습니다. 호스트에는 *mac* 및 *ip* 주소 값이 포함됩니다. 스키마 파일에는 이러한 값에 대해 다음과 같은 허용 패턴이 표시됩니다.

- **mac** – 패턴: `^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$`
- **ip** – 패턴: `^([0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}(/[0-9]{1,2}){0,1})$`



검사기 구성을 성공적으로 재정의하려면 스키마 파일의 허용되는 패턴에 따라 값, 범위, 패턴을 제공해야 합니다. 그렇지 않으면 오류 메시지가 표시됩니다.

b) **Download Sample File / Template(**샘플 파일/템플릿 다운로드**)**을 클릭하여 예제 구성이 포함된 기존 템플릿을 사용하면 검사기를 구성하는 데 도움이 됩니다.

샘플 파일에 포함된 예제 구성을 참조하여 필요에 따라 변경할 수 있습니다.

c) 전체 검사기 구성을 단일 JSON 파일로 다운로드하려면 **Download Full Configuration(**전체 구성 다운로드**)**을 클릭합니다.

검사기를 개별적으로 확장하는 대신 전체 구성을 다운로드하여 필요한 정보를 찾을 수 있습니다. 검사기 구성과 관련된 모든 정보를 이 파일에서 사용할 수 있습니다.

d) **Download Overridden Configuration(**재정의된 구성 다운로드**)**을 클릭하여 재정의된 검사기 구성을 다운로드합니다.

단계 **6** 기존 구성을 재정의하려면 다음 단계를 수행합니다.

다음과 같은 방법으로 검사기 구성을 재정의하도록 선택할 수 있습니다.

- management center에서 직접 검사기에 대해 인라인 수정을 수행합니다. *Cisco Secure Firewall Management Center Snort 3* 구성 가이드의 네트워크 분석 정책 시작하기 장에 있는 검사기에 대한 인라인 수정으로 구성 재정의 항목을 참고하십시오.
- 계속해서 현재 절차를 따라 **Actions(**작업**)** 드롭다운 메뉴를 사용하여 재정의된 구성 파일을 업로드합니다.

management center에서 직접 인라인 수정을 수행하도록 선택한 경우 현재 절차를 더 이상 따를 필요가 없습니다. 그렇지 않은 경우 이 절차를 완전히 따라야 합니다.

a) **Inspectors(**검사기**)**에서 기본 구성을 재정의할 필수 검사기를 확장합니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다.

검색 창에 관련 텍스트를 입력하여 검사기를 검색해야 할 수 있습니다.

b) 기본 검사기 구성을 클립보드에 복사하려면 **Copy to clipboard(**클립보드에 복사**)** 아이콘을 클릭합니다.

c) JSON 파일을 생성하고 기본 구성을 이 파일에 붙여 넣습니다.

d) 재정의할 검사기 구성을 유지하고 JSON 파일에서 다른 모든 구성 및 인스턴스를 제거합니다.

Sample File/Template(샘플 파일/템플릿**)**을 사용하여 기본 구성을 재정의하는 방법을 이해할 수도 있습니다. 이것은 Snort 3의 네트워크 분석 정책을 사용자 지정할 수 있는 방법을 설명하는 JSON 스니펫이 포함된 샘플 파일입니다.

e) 필요에 따라 검사기 구성을 변경합니다.

변경 사항을 검증하고 스키마 파일을 준수하는지 확인합니다. 멀티톤 검사기의 경우 모든 인스턴스의 바인딩 조건이 JSON 파일에 포함되어 있는지 확인합니다. 자세한 내용은 *Cisco Secure Firewall Management Center Snort 3* 구성 가이드의 **Snort 3**에 대한 맞춤형 네트워크 분석 정책 생성 항목에서 멀티톤 검사기를 참고하십시오.

f) 추가 기본 검사기 구성을 복사하는 경우 재정의된 구성이 포함된 기존 파일에 해당 검사기 구성을 추가합니다.

참고 복사된 검사기 구성은 JSON 표준을 준수해야 합니다.

g) 재정의된 구성 파일을 시스템에 저장합니다.

단계 **7** 을 클릭**Actions(**작업**)** 드롭다운 메뉴에서 Upload Overridden Configuration(재정의된 구성 업로드)을 선택하여 재정의된 구성이 포함된 JSON 파일을 업로드할 수 있습니다.

주의 필요한 변경 사항만 업로드합니다. 전체 구성을 업로드해서는 안 됩니다. 이렇게 하면 재정의가 고정되어 이후에 LSP 업데이트의 일부로 포함되는 기본 구성 변경 사항이 적용되지 않습니다.

파일을 끌어다 놓거나 클릭하여 시스템에 저장된 재정의된 검사기 구성이 포함된 JSON 파일을 찾아 볼 수 있습니다.

- **Merge inspector overrides(**검사기 재정의 병합**)** - 공용 검사기가 없는 경우 업로드된 파일의 콘텐츠가 기존 구성과 병합됩니다. 공용 검사기가 있는 경우 업로드된 파일의 콘텐츠(공용 검사기 사용 대상)가 이전 콘텐츠보다 우선하며 해당 검사기의 이전 구성을 대체합니다.
- **Replace inspector overrides(**검사기 재정의 교체**)** - 이전의 모든 재정의를 제거하고 업로드된 파일의 새 콘텐츠로 대체합니다.

  주의 이 옵션을 선택하면 이전의 모든 재정의가 삭제됩니다. 이 옵션을 사용하여 구성을 재정의하기 전에 정보에 입각한 결정을 내리십시오.

재정의된 검사기를 업로드하는 동안 오류가 발생할 경우 **Upload Overriden Configuration File(**재정의된 구성 파일 업로드**)** 팝업 창에 오류가 표시됩니다. 오류가 있는 파일을 다운로드한 다음 오류를 해결하고 파일을 다시 업로드할 수도 있습니다.

단계 **8** **Upload Overridden Configuration File(**재정의된 구성 파일 업로드**)** 팝업 창에서 **Import(**가져오기**)**를 클릭하여 재정의된 검사기 구성을 업로드합니다.

재정의된 검사기 구성을 업로드하면 검사기 옆에 재정의된 검사기임을 나타내는 주황색 아이콘이 표시됩니다.

또한 검사기 아래의 **Overridden Configuration(**재정의된 구성**)** 열에 재정의된 값이 표시됩니다.

Search(검색) 표시줄 옆에 있는 **Show Overrides Only(**재정의 항목만 표시**)** 체크 박스를 사용하여 재정의된 모든 검사기를 볼 수도 있습니다.

참고 항상 재정의된 구성을 다운로드한 다음 JSON 파일을 열고 이 파일의 검사기 구성에 새로운 변경/재정의를 추가하십시오. 이 작업은 기존의 재정의된 구성을 잃지 않도록 하는 데 필요합니다.

단계 **9** (선택 사항) 새 검사기 구성을 변경하기 전에 시스템에서 재정의된 구성 파일을 백업합니다.

팁 검사기 구성을 재정의할 때 수시로 백업을 수행하는 것이 좋습니다.

관련 항목

재정의된 구성을 기본 구성으로 되돌리기, 18 페이지
재정의 항목이 있는 검사기 목록 보기, 18 페이지
네트워크 분석 정책 페이지에서 검사기 검색, 12 페이지
검사기 구성 복사 , 13 페이지

검사기에 대한 인라인 수정으로 구성 재정의

네트워크 분석 정책의 Snort 3 버전의 경우, 검사기 구성을 인라인으로 수정하여 요구 사항에 따라 구성을 재정의할 수 있습니다.

또는 **Actions(**작업**)** 드롭다운 메뉴를 사용하여 재정의된 구성 파일을 업로드할 수도 있습니다. 자세한 내용은 네트워크 분석 정책 사용자 정의, 13 페이지를 참조하십시오.

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**으로 이동합니다.

단계 **3** **Inspectors(**검사기**)**에서 기본 설정을 재정의할 필수 검사기를 확장합니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다.

단계 **4** 오른쪽 열의 **Overridden Configuration(**재정의된 구성**)**에서 **Edit Inspector(**검사기 편집**)**(연필) 아이콘을 클릭하여 검사기 구성을 변경합니다.

필요한 사항을 수정할 수 있는 Override Configuration(구성 재정의) 팝업 창이 나타납니다.

참고

- 재정의하려는 설정만 유지해야 합니다. 동일한 값을 사용하여 설정을 유지하면 해당 필드가 고정으로 설정됩니다. 따라서 이후에 Talos에서 해당 설정을 변경할 경우 현재 값이 유지됩니다.
- 사용자 지정 인스턴스를 추가하거나 삭제하는 경우 바인더 검사기에서도 해당 인스턴스에 대한 바인더 규칙을 추가하거나 삭제해야 합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

JSON 표준에 의거하여 오류가 있는 경우 오류 메시지가 표시됩니다.

단계 **6** **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

변경 사항이 OpenAPI 스키마 사양을 준수하는 경우 management center에서 구성을 저장할 수 있습니다. 그렇지 않은 경우 **Error saving overridden configuration(**재정의 구성 저장 오류**)** 팝업 창에 오류가 표시됩니다. 오류가 포함된 파일을 다운로드할 수도 있습니다.

관련 항목

네트워크 분석 정책 사용자 정의, 13 페이지
인라인 수정 시 저장하지 않은 변경 사항 되돌리기 , 17 페이지
재정의된 구성을 기본 구성으로 되돌리기, 18 페이지
사용자 지정 네트워크 분석 정책 구성의 예, 21 페이지

인라인 수정 시 저장하지 않은 변경 사항 되돌리기

검사기의 구성을 재정의하기 위해 인라인 수정을 수행하거나 저장하지 않은 변경 사항을 되돌릴 수 있습니다. 이 작업은 저장하지 않은 모든 변경 사항을 가장 최근에 저장된 값으로 되돌리지만, 구성을 검사기의 기본 구성으로 되돌리는 것은 아닙니다.

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 **2** 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**으로 이동합니다.

단계 3 **Inspectors(**검사기**)**에서 저장되지 않은 변경 사항을 되돌릴 필수 검사기를 확장합니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다.

단계 4 오른쪽 열의 **Overridden Configuration(**재정의된 구성**)** 아래에서 **Cross(**십자**)**(X) 아이콘을 클릭하여 검사기의 저장하지 않은 변경 사항을 되돌립니다.

또는 변경을 취소하려면 **Cancel(**취소**)**을 클릭합니다.

검사기 컨피그레이션에 대한 저장하지 않은 변경 사항이 없는 경우 이 옵션이 표시되지 않습니다.

관련 항목

재정의된 구성을 기본 구성으로 되돌리기, 18 페이지
검사기에 대한 인라인 수정으로 구성 재정의, 16 페이지

재정의 항목이 있는 검사기 목록 보기

재정의된 모든 검사기 목록을 볼 수 있습니다.

단계 1 **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 2 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**으로 이동합니다.

단계 3 Search(검색) 표시줄 옆에 있는 **Show Overrides Only(**재정의 항목만 표시**)** 체크 박스를 선택하여 재정의된 검사기 목록을 봅니다.

재정의된 모든 검사기는 이름 옆에 주황색 아이콘이 표시되어 쉽게 식별할 수 있습니다.

관련 항목

네트워크 분석 정책 페이지에서 검사기 검색, 12 페이지
검사기에 대한 인라인 수정으로 구성 재정의, 16 페이지
네트워크 분석 정책 사용자 정의, 13 페이지

재정의된 구성을 기본 구성으로 되돌리기

검사기의 기본 구성을 재정의하기 위해 수행한 변경 사항을 되돌릴 수 있습니다. 다음 작업을 수행하면 재정의된 구성이 검사기의 기본 구성으로 되돌려집니다.

단계 1 **Policies(**정책**)** > **Intrusion(**침입**)** > **Network Analysis Policies(**네트워크 분석 정책**)**로 이동합니다.

단계 2 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**으로 이동합니다.

단계 3 **Inspectors(**검사기**)**에서 재정의된 구성을 되돌릴 필수 검사기를 확장합니다.

재정의된 검사기는 이름 옆에 주황색 아이콘이 표시됩니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다. 오른쪽 열의 **Overridden Configuration(**재정의된 구성**)**에서 **Revert to default configuration(**기본 구성으로 되돌리기**)**(뒤로 화살표) 아이콘을 클릭하여 검사기의 재정의된 구성을 기본 구성으로 되돌립니다.

검사기의 기본 구성을 변경하지 않은 경우 이 옵션은 비활성화됩니다.

단계 **4** **Revert(**되돌리기**)**를 클릭하여 결정을 확인합니다.

단계 **5** **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

변경 사항을 저장하지 않으려면 **Cancel(**취소**)** 또는 **Cross(**십자**)**(X) 아이콘을 클릭합니다.

관련 항목

인라인 수정 시 저장하지 않은 변경 사항 되돌리기 , 17 페이지
네트워크 분석 정책 사용자 정의, 13 페이지
검사기에 대한 인라인 수정으로 구성 재정의, 16 페이지
사용자 지정 네트워크 분석 정책 구성의 예, 21 페이지

Snort 3 정책 검증

다음은 Snort 3 정책을 검증하기 위해 사용자가 기록해 둘 수 있는 기본 정보 목록입니다.

- management center의 현재 버전은 여러 위협 방어 버전을 관리할 수 있습니다.
- management center의 현재 버전은 위협 방어 디바이스의 이전 버전에 적용할 수 없는 NAP 구성을 지원합니다.
- 현재 NAP 정책 및 검증은 현재 버전 지원에 따라 작동합니다.
- 변경 사항에 위협 방어의 이전 버전에 유효하지 않은 콘텐츠가 포함될 수 있습니다.
- 정책 구성 변경 사항은 현재 버전에 대해 유효한 구성이고 현재 Snort 3 바이너리 및 NAP 스키마를 사용하여 수행되는 경우 수락됩니다.
- 이전 버전 위협 방어의 경우 구축 중에 해당 특정 버전에 대한 NAP 스키마 및 Snort 3 바이너리를 사용하여 검증이 수행됩니다. 지정된 버전에 적용할 수 없는 구성이 있는 경우, 지정된 버전에서 지원되지 않는 구성은 구축되지 않으며 나머지 구성만 구축된다는 정보 또는 경고가 사용자에게 제공됩니다.

이 절차에서 NAP 정책을 액세스 제어 정책에 연결하고 이를 디바이스에 구축할 경우, 가령 Snort 3 정책을 검증하는 데 속도 필터 구성과 같은 모든 검사기가 적용됩니다.

단계 **1** **NAP** 정책 구성 재정의 단계**:** 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**의 **Inspectors(**검사기**)**에서 기본 설정을 재정의할 검사기를 확장합니다.

기본 구성은 왼쪽 열에 표시되고 재정의된 구성은 검사기의 오른쪽 열에 표시됩니다.

단계 **2** 오른쪽 열의 **Overridden Configuration(**재정의된 구성**)**에서 **Edit Inspector(**검사기 편집**)**(연필) 아이콘을 클릭하여 rate_filter와 같은 검사기를 변경합니다.

rate_filter 검사기에 필요한 편집을 수행할 수 있는 Override Configuration(구성 재정의) 팝업 창이 나타납니다.

단계 3 **OK(**확인**)**를 클릭합니다.

단계 4 **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.

또는 **Actions(**작업**)** 드롭다운 메뉴를 사용하여 재정의된 구성 파일을 업로드할 수도 있습니다.

단계 5 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**에서 **Actions(**작업**)** 드롭다운 메뉴를 클릭합니다.

단계 6 **Upload(**업로드**)**에서 **Overrideden Configuration(**재정의된 구성**)**을 클릭하여 재정의된 구성이 포함된 JSON 파일을 업로드할 수 있습니다.

주의 필요한 변경 사항만 업로드합니다. 전체 구성을 업로드해서는 안 됩니다. 이렇게 하면 재정의가 고정되어 이후에 LSP 업데이트의 일부로 포함되는 기본 구성 변경 사항이 적용되지 않습니다.

파일을 끌어다 놓거나 클릭하여 시스템에 저장된 재정의된 검사기 구성이 포함된 JSON 파일을 찾아 볼 수 있습니다.

- **Merge inspector overrides(**검사기 재정의 병합**)** - 공용 검사기가 없는 경우 업로드된 파일의 콘텐츠가 기존 구성과 병합됩니다. 공용 검사기가 있는 경우 업로드된 파일의 콘텐츠(공용 검사기 사용 대상)가 이전 콘텐츠보다 우선하며 해당 검사기의 이전 구성을 대체합니다.
- **Replace inspector overrides(**검사기 재정의 교체**)** - 이전의 모든 재정의를 제거하고 업로드된 파일의 새 콘텐츠로 대체합니다.

  주의 이 옵션을 선택하면 이전의 모든 재정의가 삭제되므로 이 옵션으로 구성을 재정의하기 전에 정보에 입각하여 올바른 결정을 내려야 합니다.

재정의된 검사기를 업로드하는 동안 오류가 발생할 경우 **Upload Overriden Configuration File(**재정의된 구성 파일 업로드**)** 팝업 창에 오류가 표시됩니다. 오류가 있는 파일을 다운로드한 다음 오류를 해결하고 파일을 다시 업로드할 수도 있습니다.

단계 7 액세스 제어 정책에 **NAP** 정책을 연결하는 단계**:** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭하고 Network Analysis(네트워크 분석) 및 Intrusion Policies(침입 정책) 섹션 옆에 있는 **Edit(**편집**)**을 클릭합니다.

단계 8 **Default Network Analysis Policy(**기본 네트워크 분석 정책**)** 드롭다운 목록에서 기본 네트워크 분석 정책을 선택합니다.

사용자가 생성한 정책을 선택할 경우, **Edit(**편집**)**을 클릭하여 새 창에서 정책을 편집할 수 있습니다. 시스템에서 제공하는 정책은 편집할 수 없습니다.

단계 9 **OK(**확인**)**를 클릭합니다.

단계 10 **Save(**저장**)**를 클릭하여 정책을 저장합니다.

단계 11 아니면 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭하고 Network Analysis(네트워크 분석) 및 Intrusion Policies(침입 정책) 섹션 옆에 있는 **Edit(**편집**)**을 클릭합니다.

단계 12 **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 13 추가할 조건을 클릭하여 규칙 조건을 구성합니다.

단계 14 **Network Analysis(**네트워크 분석**)**을 클릭하고 이 규칙과 일치하는 트래픽을 전처리하는 데 사용할 **Network Analysis Policy(**네트워크 분석 정책**)**를 선택합니다.

단계 15 **Add(**추가**)**를 클릭합니다.

단계 16 **Deployment(구축):** management center 메뉴 모음에서 **Deploy(구축)**를 클릭한 다음 **Deployment(구축)**를 선택합니다.

단계 17 구성 변경 사항을 구축할 디바이스를 식별하여 선택합니다.

- Search(검색)-검색 상자에서 디바이스 이름, 유형, 도메인, 그룹 또는 상태를 검색합니다.
- Expand(확장)-구축할 디바이스별 구성 변경 사항을 보려면 **Expand Arrow(확장 화살표)**를 클릭합니다.

  디바이스 체크 박스를 선택하면 디바이스 아래에 나열된 디바이스에 대한 모든 변경 사항이 푸시되어 구축됩니다. 그러나 **Policy Selection(정책 선택)**을 사용하면 나머지 변경 사항을 구축하지 않고 보류하면서 구축할 개별 정책 또는 구성을 선택할 수 있습니다.

  필요에 따라, 수정되지 않은 관련 정책을 선택적으로 보거나 숨기는 데 **Show or Hide Policy(정책 표시 또는 숨기기)**를 사용할 수 있습니다.

단계 18 **Deploy(구축)**를 클릭합니다.

단계 19 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(검증 메시지)** 창에 이를 표시합니다. 전체 세부 사항을 보려면 경고 또는 오류 앞에 있는 화살표 아이콘을 클릭합니다.

참고 Snort 3 네트워크 분석 정책에 이 위협 방어 버전에 대해 유효하지 않은 검사기 또는 속성이 포함되어 있으며 구축 시 잘못된 설정이 생략된다는 경고가 표시됩니다. 잘못된 검사기는 7.1 버전 이하의 디바이스에 대해서만 ["rate_filter"]입니다.

사용자 지정 네트워크 분석 정책 구성의 예

이것은 Snort 3의 네트워크 분석 정책을 사용자 지정할 수 있는 방법을 설명하는 JSON 스니펫이 포함된 샘플 파일입니다. 다음과 같은 방법으로 검사기 구성을 재정의하도록 선택할 수 있습니다.

- management center에서 직접 검사기에 대해 인라인 수정을 수행합니다. 검사기에 대한 인라인 수정으로 구성 재정의, 16 페이지의 내용을 참조하십시오.
- **Actions(작업)** 드롭다운 메뉴를 사용하여 재정의된 구성 파일을 업로드합니다. 네트워크 분석 정책 사용자 정의, 13 페이지의 내용을 참조하십시오.

이러한 옵션을 선택하기 전에 네트워크 분석 정책 재정의를 성공적으로 정의하는 데 도움이 되는 다음과 같은 세부 정보와 예를 모두 검토하십시오. 위험과 오류를 방지하기 위해 여기에 설명된 다양한 시나리오의 예를 읽고 이해해야 합니다.

Actions(작업) 드롭다운 메뉴에서 검사기 구성을 재정의하도록 선택하는 경우 네트워크 분석 정책 재정의를 위한 JSON 파일을 생성하고 업로드해야 합니다.

네트워크 분석 정책에서 검사기 구성을 재정의하려면 필요한 변경 사항만 업로드해야 합니다. 전체 구성을 업로드해서는 안 됩니다. 이렇게 하면 재정의가 고정되어 이후에 LSP 업데이트의 일부로 포함되는 기본값 또는 구성 변경 사항이 적용되지 않습니다.

다음은 다양한 시나리오의 예입니다.

기본 정책의 기본 상태가 비활성화된 경우 싱글톤 검사기 활성화

```
{
  "rate_filter": {
    "enabled": true,
    "type": "singleton",
    "data": []
  }
}
```

기본 정책의 기본 상태가 활성화된 경우 싱글톤 검사기 비활성화

```
{
  "rate_filter": {
    "enabled": false,
    "type": "singleton",
    "data": []
  }
}
```

기본 정책의 기본 상태가 비활성화된 경우 멀티톤 검사기 활성화

```
{
  "ssh": {
    "enabled": true,
    "type": "multiton",
    "instances": []
  }
}
```

기본 정책의 기본 상태가 활성화된 경우 멀티톤 검사기 비활성화

```
{
  "ssh": {
    "enabled": false,
    "type": "multiton",
    "instances": []
  },
  "iec104": {
    "type": "multiton",
    "enabled": false,
    "instances": []
  }
}
```

싱글톤 검사기에 대한 특정 설정의 기본값 재정의

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  }
}
```

멀티톤 검사기에서 기본 인스턴스(인스턴스 이름이 검사기 유형과 일치)의 특정 설정 재정의

```
{
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false
        },
        "name": "http_inspect"
      }
    ]
  }
}
```

필요한 변경 사항이 있는 기본 인스턴스에 대한 바인더 규칙 추가

참고 기본 바인더 규칙은 수정할 수 없으며 항상 끝에 추가됩니다.

```
{
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

새 사용자 지정 인스턴스 추가

참고 해당하는 바인더 규칙 항목을 바인더 검사기에서 정의해야 합니다.

```
{
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
```

```
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      }
    ]
  }
}
```

싱글톤 인스턴스 및 멀티톤 기본 인스턴스 재정의, 단일 **JSON** 재정의에서 새 멀티톤 인스턴스 생성

단일 JSON 재정의에서 다음 사항을 보여주는 예:

- 싱글톤 인스턴스 재정의(**normalizer** 검사기)
- 멀티톤 기본 인스턴스 재정의(**http_inspect** 검사기)
- 새 멀티톤 인스턴스 생성(**telnet** 검사기)

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  },
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false,
          "xff_headers": "x-forwarded-for true-client-ip x-another-forwarding-header"
        },
        "name": "http_inspect"
      }
    ]
  },
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
```

```
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      },
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

참고 바인더 규칙에서 기본 인스턴스의 **name** 속성은 지정할 필요가 없습니다.

arp_spoof 구성

arp_spoof를 구성하는 예:

arp_spoof 검사기에는 속성에 대한 기본 구성이 없습니다. 다음은 재정의를 제공할 수 있는 경우를 보여줍니다.

```
{
  "arp_spoof": {
    "type": "singleton",
    "data": {
      "hosts": [
        {
          "ip": "1.1.1.1",
          "mac": "ff:0f:f1:0f:0f:ff"
        },
        {
          "ip": "2.2.2.2",
          "mac": "ff:0f:f2:0f:0f:ff"
        }
      ]
    },
    "enabled": true
  }
}
```

rate_filter 구성

```
{
  "rate_filter": {
    "data": [
      {
        "apply_to": "[10.1.2.100, 10.1.2.101]",
        "count": 5,
        "gid": 135,
        "new_action": "alert",
        "seconds": 1,
        "sid": 1,
        "timeout": 5,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

다중 계층 네트워크 분석 정책이 사용되는 경우 바인더 규칙 구성

이 예에서는 하위 정책에 새 사용자 지정 인스턴스를 추가하는 방법과 바인더 규칙을 작성하는 방법을 보여줍니다. 바인더 규칙은 목록으로 정의되므로 규칙이 자동으로 병합되지 않아 상위 정책에 정의된 규칙을 선택하고 이를 기반으로 새 규칙을 작성하는 것이 중요합니다. 하위 정책에서 사용 가능한 바인더 규칙은 전체적으로 적용됩니다.

위협 방어에서는 기본 Cisco Talos 정책 규칙이 이러한 사용자 정의 재정의에 추가됩니다.

상위 정책:

telnet_parent_instance라는 이름의 사용자 지정 인스턴스와 해당 바인더 규칙을 정의했습니다.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
```

```
      }
    ]
  }
}
```

하위 정책:

이 네트워크 분석 정책에는 위에서 언급한 정책이 기본 정책으로 포함되어 있습니다. **telnet_child_instance**라는 이름의 사용자 지정 인스턴스를 정의하고 이 인스턴스에 대한 바인더 규칙도 정의했습니다. 상위 정책의 바인더 규칙을 여기에 복사한 다음 규칙의 특성에 따라 하위 정책 바인더 규칙을 그 앞이나 뒤에 추가할 수 있습니다.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_child_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet",
          "nets": "10.2.2.0/24"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_child_instance"
        }
      },
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

일반적인 목록 검사기 속성 구성

목록 유형의 속성에 대한 재정의를 변경하는 동안에는 부분 재정의가 아니라 전체 콘텐츠를 전달하는 것이 중요합니다. 이는 기본 정책 속성이 다음과 같이 정의된 경우를 의미합니다.

```
{
  "list-attribute": [
```

```
    {
      "entry1": {
        "key1": "value1"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

value1을 **value1-new**로 수정하려는 경우 재정의 페이로드는 다음과 같아야 합니다.

올바른 방법:

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

잘못된 방법:

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    }
  ]
}
```

smtp 검사기에서 **alt_max_command_line_len** 속성의 잘린 값을 가져와서 이 구성을 이해할 수 있습니다. **smtp** 검사기의 기본 정책 구성이 다음과 같다고 가정해 보겠습니다.

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "decompress_zip": false,
          "normalize_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
           EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
           NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
           TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
           ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
           XSTA XTRN XUSR",
          "ignore_data": false,
          "max_command_line_len": 512,
          "max_header_line_len": 1000,
          "log_rcptto": false,
```

```
            "decompress_swf": false,
            "max_response_line_len": 512,
            "b64_decode_depth": -1,
            "max_auth_command_line_len": 1000,
            "log_email_hdrs": false,
            "xlink2state": "alert",
            "binary_data_cmds": "BDAT XEXCH50",
            "auth_cmds": "AUTH XAUTH X-EXPS",
            "log_filename": false,
            "uu_decode_depth": -1,
            "ignore_tls_data": false,
            "data_cmds": "DATA",
            "bitenc_decode_depth": -1,
            "alt_max_command_line_len": [
              {
                "length": 255,
                "command": "ATRN"
              },
              {
                "command": "AUTH",
                "length": 246
              },
              {
                "length": 255,
                "command": "BDAT"
              },
              {
                "length": 246,
                "command": "DATA"
              }
            ],
            "log_mailfrom": false,
            "decompress_pdf": false,
            "normalize": "none",
            "email_hdrs_log_depth": 1464,
            "valid_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
             EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
             NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
             TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
             ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
             XSTA XTRN XUSR",
            "qp_decode_depth": -1
          }
        }
    ],
    "enabled": true
  }
}
```

이제 다음과 같이 **alt_max_command_line_len** 목록에 두 개의 개체를 더 추가합니다.

```
{
    "length": 246,
    "command": "XEXCH50"
},
{
    "length": 246,
    "command": "X-EXPS"
}
```

그러면 사용자 지정 네트워크 분석 정책 재정의 JSON이 다음과 같이 표시됩니다.

```
{
  "smtp": {
    "type": "multiton",
```

```
    "instances": [
      {
        "name": "smtp",
        "data": {
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            },
            {
              "length": 246,
              "command": "XEXCH50"
            },
            {
              "length": 246,
              "command": "X-EXPS"
            }
          ]
        }
      }
    ],
    "enabled": true
  }
}
```

다중 계층 네트워크 분석 정책이 멀티톤 검사기에서 사용되는 경우 바인더 규칙 구성

이 예에서는 하위 정책의 속성을 재정의하는 방법과 병합된 구성이 인스턴스의 하위 정책에 사용되는 방식을 보여줍니다. 하위 정책에 정의된 모든 재정의는 상위 정책과 병합됩니다. 예를 들어 속성 1과 속성 2가 상위 정책에서 재정의되고 속성 2와 속성 3이 하위 정책에서 재정의되는 경우 병합된 구성이 하위 정책에 적용됩니다. 즉, 속성 1(상위 정책에 정의됨), 속성 2(하위 정책에 정의됨) 및 속성 3(하위 정책에 정의됨)이 디바이스에 구성됩니다.

상위 정책:

여기서는 **telnet_parent_instance**라는 이름의 사용자 지정 인스턴스를 정의하고 사용자 지정 인스턴스에서 **normalize**와 **encrypted_traffic**이라는 2개의 속성을 재정의했습니다.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_parent_instance"
      }
```

```
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

하위 정책:

이 네트워크 분석 정책에는 위에서 언급한 정책이 기본 정책으로 포함되어 있습니다. 상위 정책에서 **encrypted_traffic** 속성을 재정의했으며 새 속성 **ayt_attack_thresh**도 재정의했습니다.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  }
}
```

위의 정책 JSON을 사용하면 네트워크 분석 정책을 구축할 때 다음과 같이 병합된 JSON이 디바이스에 구성됩니다.

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
```

```
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

이 예에서는 사용자 지정 네트워크 분석 정책의 세부 사항을 보여줍니다. 기본 인스턴스에서도 동일한 동작이 나타납니다. 또한 싱글톤 검사기에서도 유사한 병합이 수행됩니다.

네트워크 분석 정책에 대한 모든 검사기 재정의 제거:

특정 네트워크 분석 정책에 대한 모든 재정의를 제거할 때마다 빈 JSON을 업로드할 수 있습니다. 재정의를 업로드하는 동안 **Replace inspector overrides(**검사기 재정의 교체**)** 옵션을 선택합니다.

```
{
}
```

관련 항목

네트워크 분석 정책에 사용되는 Snort 3 정의 및 용어, 3 페이지
네트워크 분석 정책 매핑, 11 페이지
Snort 3에 대한 맞춤형 네트워크 분석 정책 생성, 5 페이지
네트워크 분석 정책 페이지에서 검사기 검색, 12 페이지
검사기 구성 복사 , 13 페이지
네트워크 분석 정책 사용자 정의, 13 페이지
재정의 항목이 있는 검사기 목록 보기, 18 페이지

네트워크 분석 정책 설정 및 캐시된 변경 사항

새로운 네트워크 분석 정책을 생성하는 경우 해당 기본 정책의 설정과 동일합니다.

네트워크 분석 정책을 조정할 경우, 특히 검사기를 비활성화할 경우, 일부 검사기 및 침입 규칙은 트래픽이 먼저 특정 방법으로 디코딩되거나 전처리되어야 한다는 점에 유의하십시오. 검사기를 비활성화한 경우, 검사기가 네트워크 분석 정책 웹 사용자 인터페이스에서 비활성화된 상태로 남아 있다고 해도 시스템은 자동으로 검사기를 현재의 설정으로 사용합니다.

참고 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 반드시 서로 보완해야 합니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 고급 작업입니다.

시스템은 사용자당 1개의 네트워크 분석 정책을 캐시합니다. 네트워크 분석 정책을 수정하는 동안 모든 메뉴 또는 다른 페이지로 이동하는 다른 경로를 선택하는 경우, 해당 페이지를 벗어난다고 해도 변경 사항은 시스템 캐시에 유지됩니다.