네트워크 분석 정책 시작하기

다음 주제에서는 네트워크 분석 정책을 바탕으로 시작하는 방법을 설명합니다.

네트워크 분석 정책 기본 사항

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 Talos 인텔리전스 그룹이(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 작동해 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.

네트워크 분석 정책에 대한 라이선스 요건

FTD 라이선스

위협

기본 라이선스

보호

네트워크 분석 정책 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

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.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

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

단계 **2** 네트워크 분석 정책 관리:

- 비교 - **Compare Policies(**정책 비교**)**를 클릭합니다. 정책 비교를 참조하십시오.
- 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 Snort 2에 대한 맞춤형 네트워크 분석 정책 생성, 12 페이지에 설명된 대로 진행합니다.
  - Snort 3 버전의 경우 네트워크 분석 정책 생성, 8 페이지에 설명된 대로 진행합니다.

- Delete(삭제) - 네트워크 분석 정책을 삭제하려면 **Delete(**삭제**)** ( )를 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.

- 구축 - **Deploy(**구축**)** > **Deployment(**구축**)**를 선택합니다. 구성 변경 사항 구축의 내용을 참조하십시오.
- Edit(편집) - 기존 네트워크 분석 정책을 편집하려면 **Edit(**수정**)** ( )을 클릭하고 네트워크 분석 정책 설정 및 캐시된 변경 사항, 14 페이지에서 설명하는 지침을 따릅니다.

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

- 보고서 - **Report(**보고서**)** ( )을(를) 클릭합니다. 현재 정책 보고서 생성의 내용을 참조하십시오.

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 않아도됩니다. 그러나 특정 네트워크 요구 사항이 있거나 성능 문제가 발생할 경우 기본 네트워크 분석 정책을 사용자 지정할 수 있습니다. 네트워크 분석 정책을 사용자 정의하는 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 확인할 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 FMC에서 사용할 수 있습니다. Snort 3에 대한 자세한 내용은 https://snort.org/snort3 항목을 참조하십시오. FMC에서 사용 가능한 검사기에 대한 자세한 내용은 https://www.cisco.com/go/snort3-inspectors 항목을 참조하십시오.

참고

- FMC를 7.0 릴리스로 업그레이드하는 동안 네트워크 분석 정책의 Snort 2 버전에서 수행된 변경 사항은 업그레이드 후에 Snort 3으로 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.

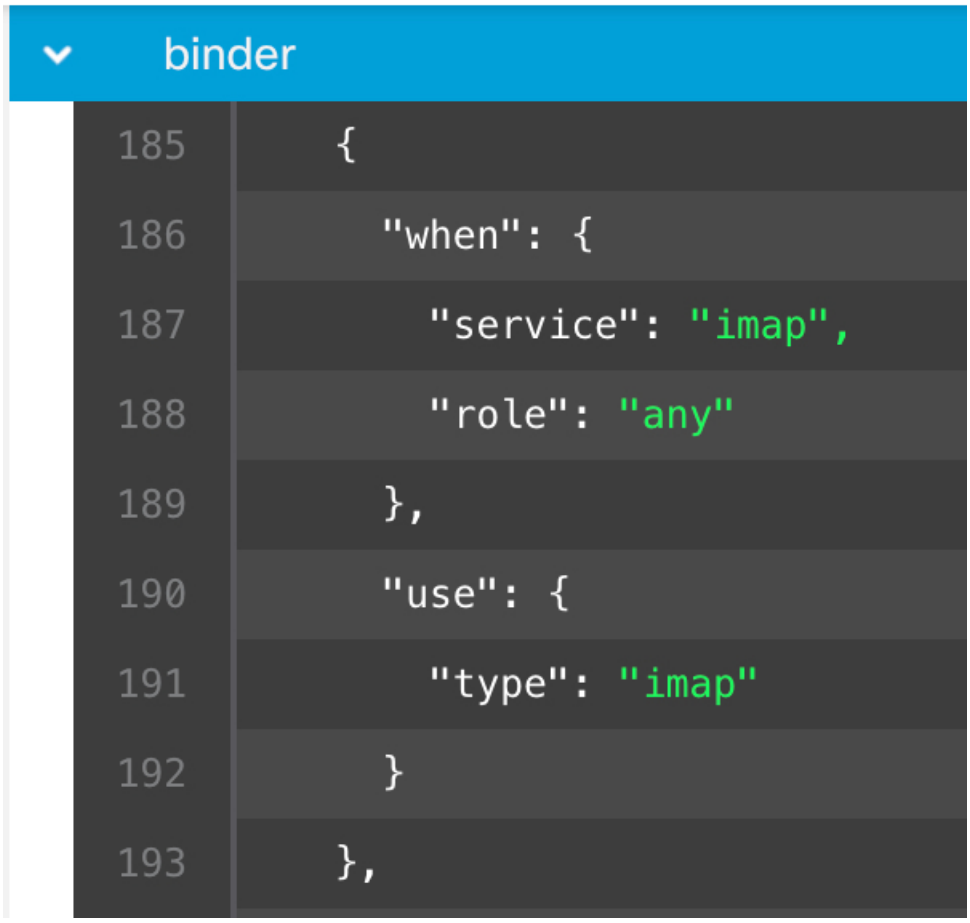
바인더 검사기

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. 조건:

- 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"
            }
         }
      ]
   }
}
```

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

프로시저

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 FMC에서 사용할 수 있습니다. 새 네트워크 분석 정책을 생성하면 정책이 Snort 2 버전과 Snort 3 버전 모두로 생성됩니다.

프로시저

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** 사용 가능한 선택 항목 중에서 **Inspection Mode(**검사 모드**)**를 선택합니다.

- 감지
- 방지

단계 **5** **Base Policy(**기본 정책**)**을 선택하고 **Save(**저장**)**를 클릭합니다.

참고 Snort 3 및 SSL 암호 해독 또는 TLS 서버 ID를 사용하는 경우 방지 모드에서 NAP(Network Analysis Policy)를 구성합니다.

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.

프로시저

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

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

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 사용자 정의

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

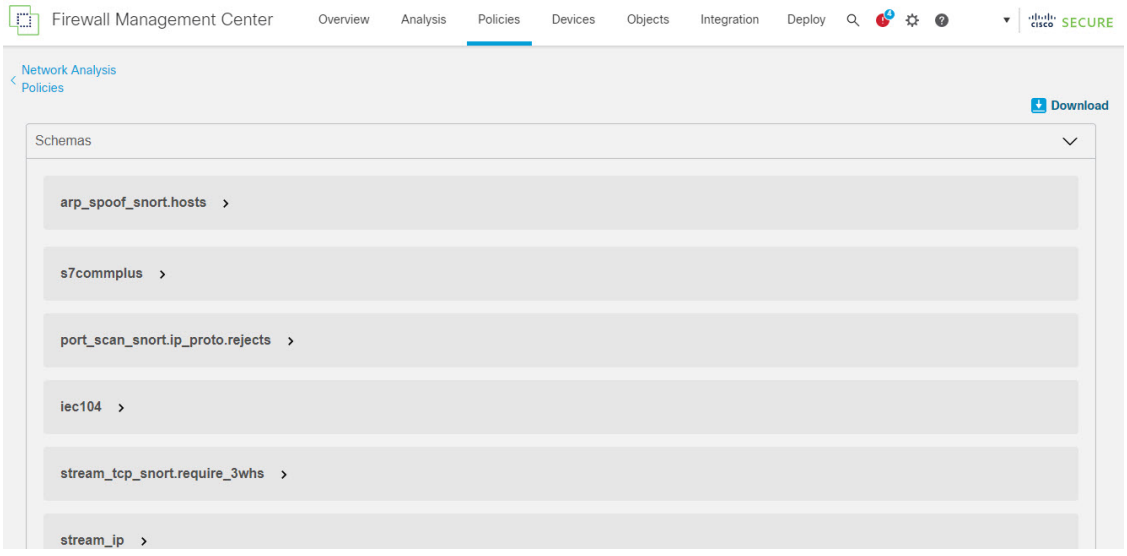
프로시저

단계 **1** 네트워크 분석 정책의 **Snort 3 Version(Snort 3** 버전**)**에서 **Actions(**작업**)** 드롭다운 메뉴를 클릭합니다.

다음 옵션이 표시됩니다.

- 스키마 보기
- 다운로드
  - Schema(스키마)
  - 샘플 파일/템플릿
  - 전체 설정
  - 재정의된 설정
- 업로드
  - 재정의된 설정

단계 **2** 브라우저에서 스키마 파일을 직접 열려면 **View Schema(**스키마 보기**)**를 클릭합니다.



단계 **3** **Download(**다운로드**)**에서 다음 옵션을 사용하여 필요에 따라 스키마 파일, 샘플 파일, 전체 구성 또는 재정의된 구성을 다운로드할 수 있습니다.

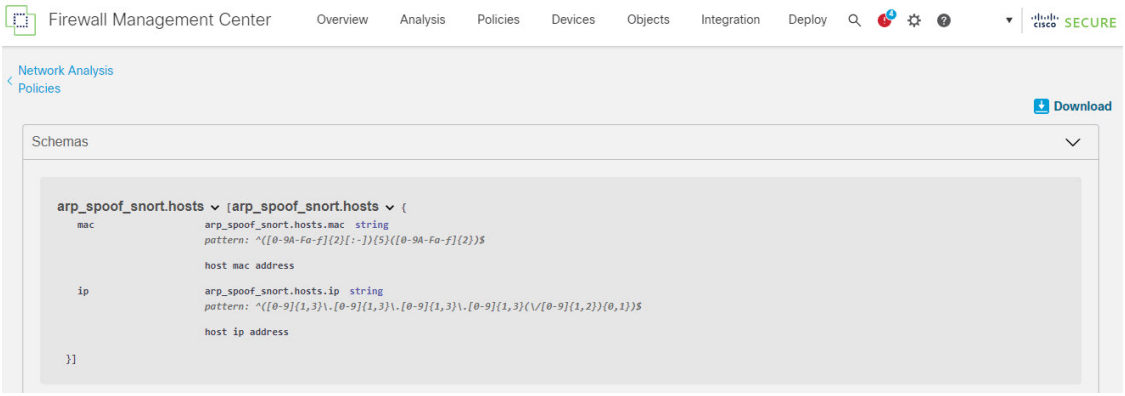
이러한 옵션은 허용되는 값, 범위 및 패턴, 기존 및 기본 검사기 구성, 재정의된 검사기 구성에 대한 통찰력을 제공합니다.

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

스키마 파일은 업로드하거나 다운로드하는 콘텐츠를 검증합니다. 스키마 파일을 다운로드하여 서드 파티 JSON 편집기를 사용하여 열 수 있습니다. 스키마 파일은 사용할 수 있는 허용되는 값, 범위 및 허용되는 패턴을 사용하여 검사기에 대해 구성할 수 있는 매개 변수를 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 제공해야합니다. 그렇지 않으면 오류 메시지가 표시됩니다.

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

샘플 파일에 포함된 예제 구성을 참조하여 필요에 따라 변경할 수 있습니다. 자세한 내용은 를 참고하십시오.

c) 전체 검사기 구성을 단일 파일로 다운로드하려면 **Full Configuration(**전체 구성**)**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) **Overrideden Configuration(**재정의된 구성**)**을 클릭하여 재정의된 관리자 구성을 다운로드합니다.

검사기 구성을 재정의하지 않은 경우 이 옵션은 비활성화됩니다. 검사기 구성을 재정의하면 이 옵션이 자동으로 활성화되어 다운로드할 수 있습니다.

단계 **4** 기존 구성을 재정의하려면 다음 단계를 수행합니다.

다음과 같은 방법으로 검사기 구성을 재정의하도록 선택할 수 있습니다.

- FMC에서 직접 검사기에 대해 인라인 수정을 수행합니다. 인라인 수정을 수행하는 단계는 항목을 참조하십시오.

- 계속해서 현재 절차를 따라 **Actions(**작업**)** 드롭다운 메뉴를 사용하여 재정의된 구성 파일을 업로드합니다.

FMC에서 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. 자세한 내용은 항목을 참조하십시오.

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 Snort 3에 대한 맞춤형 네트워크 분석 정책 생성, 3 페이지의 멀티톤 검사기를 참조하십시오.

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.

h) 다음 단계에 설명된 대로 재정의된 구성을 FMC에 업로드합니다.

단계 **5** **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 찾아볼 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 **6** **Upload Overridden Configuration File(**재정의된 구성 파일 업로드**)** 팝업 창에서 **Import(**가져오기**)** 버튼을 클릭하여 재정의된 검사기 구성을 업로드합니다.

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

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

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

참고 **Download(**다운로드**)** 아래에서 **Overrideden Configurations(**재정의된 구성**)**를 항상 다운로드한 다음 JSON 파일을 열고 이 파일의 검사기 구성에 새로운 변경/재정의를 추가합니다. 이 작업은 기존의 재정의된 구성을 잃지 않도록 하는 데 필요합니다.

단계 **7** (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
- 재정의 항목이 있는 검사기 목록 보기
- 사용자 지정 네트워크 분석 정책 구성의 예
- 네트워크 분석 정책 페이지에서 검사기 검색
- 검사기 구성 복사

Snort 2에 대한 맞춤형 네트워크 분석 정책 생성

새로운 네트워크 분석 정책을 생성하는 경우 고유한 이름 및 기본 정책을 지정하고 인라인 모드를 선택해야 합니다.

기본 정책은 네트워크 분석 정책의 기본 설정을 정의합니다. 새로운 정책에서 구성을 변경하면 기본 정책 설정을 대체하지만 변경하지는 않습니다. 기본 정책으로 시스템 제공 정책 또는 사용자 지정 정책을 사용할 수 있습니다.

네트워크 분석 정책의 인라인 모드에서는 전처리기가 트래픽을 수정(표준화)하고 삭제하여 공격자가 탐지를 회피할 가능성을 최소화할 수 있습니다. 수동 배포에서는 시스템이 인라인 모드와 관계없이 트래픽 흐름에 영향을 줄 수 없다는 점에 유의하십시오.

관련 항목

기본 레이어
인라인 구축의 전처리기 트래픽 수정, 17 페이지
사용자 지정 네트워크 분석 정책 만들기, 13 페이지
네트워크 분석 정책 수정, 15 페이지

사용자 지정 네트워크 분석 정책 만들기

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.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

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

단계 **2** **Create Policy(**정책 생성**)**를 클릭합니다. 다른 정책에 저장되지 않은 변경 사항이 있는 경우, **Network Analysis Policy(**네트워크 분석 정책**)** 페이지로 돌아가라는 메시지가 나타나면 **Cancel(**취소**)**을 클릭합니다.

단계 **3** 고유한 **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 정책 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 정책 이름과의 충돌을 식별할 수 있습니다.

단계 **4** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **5** 최초 **Base Policy(**기본 정책**)**를 선택합니다. 기본 정책으로 시스템 제공 정책 또는 사용자 지정 정책을 사용할 수 있습니다.

주의 맞춤형 NAP를 구성하는 동안 **Maximum Detection(**최대 탐지**)**을 **Base Policy(**기본 정책**)**로 선택하면 성능이 저하될 수 있습니다. 생산 환경에 구축하기 전에 이 설정을 검토하고 테스트하는 것이 좋습니다.

단계 **6** 인라인 구축에서 트래픽이 전처리기의 영향을 받게 하려면 **Inline Mode(**인라인 모드**)**를 활성화합니다.

단계 **7** 정책을 생성하려면:

- 새로운 정책을 만들고 **Network Analysis Policy(**네트워크 분석 정책**)**로 돌아가려면 **Create Policy(**정책 생성**)**를 클릭합니다. 새로운 정책의 설정은 기본 정책의 설정과 같습니다.

- **Create and Edit Policy(**정책 생성 및 편집**)**를 클릭하여 정책을 만들고 고급 네트워크 분석 정책 편집기에서 정책을 열어 편집합니다.

Snort 2에 대한 네트워크 분석 정책 관리

Network Analysis Policy(네트워크 분석 정책) 페이지(또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**(이)나 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**)에서 다음 정보와 함께 현재 맞춤형 네트워크 분석 정책을 볼 수 있습니다.

- 정책이 최종 수정된 시간과 날짜(로컬 시간) 및 정책을 수정한 사용자
- **Inline Mode** 설정의 활성화 여부(프리프로세서가 트래픽에 영향을 미치도록 허용)
- 트래픽을 전처리하는 데 네트워크 분석 정책을 사용하는 액세스 제어 정책 및 디바이스
- 정책에 저장되지 않은 변경 사항이 있는지 여부 및 현재 정책을 수정하고 있는 사람에 관한 정보

사용자가 생성하는 맞춤형 정책 이외에도 시스템은 두 개의 맞춤형 정책인, Initial Inline Policy(초기 인라인 정책)와 Initial Passive Policy(초기 수동 정책)를 제공합니다. 이 두 가지 네트워크 분석 정책은 Balanced Security and Connectivity(균형 보안 및 연결) 네트워크 분석 정책을 기반으로 사용합니다. 이 둘의 유일한 차이점은 인라인 모드에서는 전처리기가 인라인 정책의 트래픽에 영향을 미치도록 허용하고, 패시브 정책에서는 이를 비활성화한다는 점입니다. 시스템이 제공하는 이러한 맞춤형 정책을 편집하고 사용할 수 있습니다

Firepower System 사용자 계정 역할이 Intrusion Policy(침입 정책) 또는 Modify Intrusion Policy(침입 정책 수정)로 제한된 경우에만 네트워크 분석과 침입 정책을 생성 및 수정할 수 있습니다.

관련 항목

사용자 지정 네트워크 분석 정책 만들기, 13 페이지
네트워크 분석 정책 수정, 15 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 전처리기를 비활성화할 경우, 일부 전처리기 및 침입 규칙은 트래픽이 먼저 특정 방법으로 디코딩되거나 전처리되어야 한다는 점에 유의하십시오. 필수 전처리기를 비활성화하는 경우, 네트워크 분석 정책 웹 인터페이스에서는 전처리기가 비활성화되어 있더라도 시스템은 자동으로 전처리기를 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.

관련 항목

정책이 트래픽에서 침입을 검토하는 방법
사용자 지정 정책의 한계

네트워크 분석 정책 수정

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.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**을(를) 선택합니다.

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

단계 **2** 편집하려는 정책 옆의 **Snort 2 Version(Snort 2** 버전**)**을 클릭합니다.

단계 **3** 구성하려는 네트워크 분석 정책 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

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

단계 **4** 네트워크 분석 정책 편집:

- 기본 정책 변경 - 기본 정책을 변경하려면 Policy Information(정책 정보) 페이지의 **Base Policy(**기본 정책**)** 드롭다운 목록에서 기본 정책을 선택합니다.
- 정책 레이어 관리 - 정책 레이어를 관리하려면 탐색 패널에서 **Policy Layers(**정책 레이어**)**를 클릭합니다.
- 전처리기 수정 - 전처리기를 활성화, 비활성화 또는 편집하려면 탐색 패널에서 **Settings(**설정**)**를 클릭합니다.
- 트래픽 수정 - 전처리기가 트래픽을 수정하거나 삭제하도록 허용하려면 Policy Information(정책 정보) 페이지에서 **Inline Mode(**인라인 모드**)** 확인란을 선택합니다.
- 설정 확인 - 기본 정책의 설정을 확인하려면 Policy Information(정책 정보) 페이지에서 **Manage Base Policy(**기본 정책 관리**)**를 클릭합니다.

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 선택한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다. 변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 전처리기가 이벤트를 생성하고, 인라인 구축에서 문제가 되는 패킷을 삭제합니다.하도록 허용하려면, 전처리기에 대한 규칙을 활성화합니다. 자세한 내용은 침입 규칙 상태 설정를 참고하십시오.
- Deploy configuration changes(구성 변경 사항 구축), Firepower Management Center 관리 가이드 참조.

관련 항목

기본 레이어
기반 정책 변경
Snort 2에 대한 네트워크 분석 정책의 전처리기 구성, 16 페이지
인라인 구축의 전처리기 트래픽 수정, 17 페이지
레이어 관리
충돌 및 변경: 네트워크 분석 및 침입 정책

Snort 2에 대한 네트워크 분석 정책의 전처리기 구성

전처리기는 트래픽을 정규화하고 프로토콜 이상 징후를 확인하여 트래픽의 추가 검사를 준비합니다. 전처리기는 패킷이 사용자가 구성한 전처리기 옵션을 트리거할 때 전처리기 이벤트를 생성합니다. 네트워크 분석 정책에 대한 기본 정책은 기본적으로 활성화되는 전처리기 및 각각에 대한 기본 구성을 결정합니다.

참고 대부분의 경우, 전처리기는 특정 전문가가 구성해야 하며 거의 수정이 필요하지 않습니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 고급 작업입니다. 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 반드시 서로 보완해야 합니다.

전처리 구성을 수정하려면 구성 및 네트워크에 미치는 잠재적 영향에 대한 이해가 필요합니다.

일부 고급 전송 및 네트워크 전처리기 설정은 액세스 컨트롤 정책을 구축하는 모든 네트워크, 영역 및 VLAN에 전역적으로 적용됩니다. 네트워크 분석 정책이 아닌 액세스 제어 정책에서 이 고급 설정을 구성합니다.

또한 침입 정책에서 ASCII 텍스트의 신용카드 번호 및 주민등록번호 같은 민감한 데이터를 탐지하는 민감한 데이터 전처리기를 구성할 수도 있습니다.

관련 항목

DCE/RPC 전처리기
DNP3 전처리기
DNS 전처리기
FTP/텔넷 디코더
GTP 전처리기

인라인 구축의 전처리기 트래픽 수정

인라인 구축(즉 관련 설정을 라우팅, 스위칭 또는 투명 인터페이스나 인라인 인터페이스 쌍을 이용해 디바이스에 적용함)의 경우 일부 전처리기가 트래픽을 수정하거나 차단할 수 있습니다. 예를 들면 다음과 같습니다.

- 인라인 표준화 전처리기는 패킷을 정규화하여 다른 전처리기와 침입 규칙 엔진에 의한 분석을 위해 준비합니다. 또한 전처리기의 **Allow These TCP Options(**이러한 **TCP** 옵션 허용**)**와 **Block Unresolvable TCP Header Anomalies(**복구 불능 **TCP** 헤더 이상 징후 차단**)** 옵션을 사용하여 특정 패킷을 차단할 수도 있습니다.
- 시스템은 잘못된 체크섬이 포함된 패킷을 삭제할 수 있습니다.
- 시스템은 속도 기반 공격 방지 설정과 일치하는 패킷을 삭제할 수 있습니다.

네트워크 분석 정책에서 트래픽에 영향을 주도록 구성된 전처리기의 경우, 전처리기를 활성화하고 올바르게 구성해야 하며 매니지드 디바이스도 인라인으로 올바르게 구축해야 합니다. 마지막으로, 네트워크 분석 정책의 **Inline Mode(**인라인 모드**)** 설정을 활성화해야 합니다.

네트워크 분석 정책 참고 사항의 전처리기 설정

네트워크 분석 정책의 탐색 패널에 있는 **Settings(**설정**)**를 선택하는 경우, 정책은 유형 별 전처리기를 나열합니다. Settings(설정) 페이지에서 네트워크 분석 정책의 전처리기를 활성화 또는 비활성화할 수 있으며, 전처리기 구성 페이지에 액세스할 수도 있습니다.

이를 구성하려면 전처리기를 활성화해야 합니다. 전처리기를 활성화하면, 전처리기 구성 페이지로 연결되는 하위 링크가 탐색 패널의 **Settings(**설정**)** 링크 아래에 나타나고, Settings(설정) 페이지의 전처리기 옆에 구성 페이지로 연결되는 **Edit(**수정**)** 링크가 나타납니다.

팁 전처리기의 구성을 기본 정책의 설정으로 되돌리려면, 전처리기 구성 페이지에서 **Revert to Defaults(**기본값으로 되돌리기**)**를 클릭합니다. 메시지가 표시되면 복원할 것인지 확인합니다.

프리프로세서를 비활성화하면 하위 링크와 **Edit** 링크가 더 이상 나타나지 않지만 컨피그레이션은 그대로 유지됩니다. 특정 분석을 수행하려면 많은 전처리기와 침입 규칙에서 트래픽이 특정 방법으로 먼저 디코딩되거나 전처리되어야 한다는 점에 유의하십시오. 전처리기를 비활성화한 경우, 전처리기가 네트워크 분석 정책 웹 인터페이스에서 비활성화된 상태로 남아 있다고 해도, 시스템은 자동으로 전처리기를 현재의 설정으로 사용합니다.

구성이 인라인 배포에서 실제로는 트래픽을 수정하지 않으면서 어떻게 작동하는지 평가하려는 경우 인라인 모드를 비활성화하면 됩니다. 수동 구축에서 또는 탭 모드의 인라인 구축에서, 시스템은 인라인 모드에 관계없이 트래픽에 영향을 줄 수 없습니다.

참고 인라인 모드 비활성화는 침입 이벤트 성능 통계 그래프에 영향을 줄 수 있습니다. 인라인 구축에서 인라인 모드가 활성화된 경우 Intrusion Event Performance(침입 이벤트 성능) 페이지(**Overview(**개요**)** > **Summary(**요약**)** > **Intrusion Event Performance(**침입 이벤트 성능**)**)에는 표준화 및 차단된 패킷을 나타내는 그래프가 표시됩니다. 인라인 모드를 비활성화하면(즉 패시브 구축에서는), 시스템이 표준화 또는 삭제했을 트래픽에 대한 데이터가 다수의 그래프에 표시됩니다.

참고 인라인 배포에서는 인라인 모드를 활성화하고 **Normalize TCP Payload(TCP** 페이로드 표준화**)** 옵션이 활성화된 인라인 표준화 전처리기를 구성할 것을 권장합니다. 수동 구축에서는 적응형 프로파일 업데이트을 사용하는 것이 좋습니다.

관련 항목

고급 전송/네트워크 전처리기 설정
체크섬 확인
인라인 정상화 전처리기

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.