FTD의 LINA 프로토콜 검사로 인한 트래픽 삭제 트러블슈팅

목차

소개

이 문서에서는 MPF(Modular Policy Framework)에 대한 LINA 프로토콜 검사가 Cisco Secure FTD에서 트래픽을 삭제하는지 여부를 식별하는 방법에 대해 설명합니다.

사전 요구 사항

Cisco에서는 다음 항목에 대한 지식이 있는 것을 권장합니다.

- Cisco FTD(Secure Firewall Threat Defense).
- Cisco FMC(Secure Firewall Manager Center).

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Virtual Cisco FTD(Secure Firewall Threat Defense) 버전 7.4.2
- Virtual Cisco FMC(Secure Firewall Manager Center) 버전 7.4.2

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

배경 정보

검사 엔진은 사용자 데이터 패킷에 IP 주소 지정 정보를 포함하거나 동적으로 할당된 포트에서 보조 채널을 여는 서비스에 대해 방화벽에 필요합니다.

프로토콜 검사는 네트워크 패킷의 내용을 검사하고 사용되는 애플리케이션 또는 프로토콜을 기준으로 트래픽을 차단 또는 수정하여 악성 트래픽이 네트워크에 유입되는 것을 방지할 수 있습니다. 따라서 검사 엔진은 전체 처리량에 영향을 미칠 수 있습니다. 방화벽에서는 기본적으로 몇 가지 일반적인 검사 엔진이 활성화되어 있으며, 네트워크에 따라 다른 엔진을 활성화해야 할 수도 있습니다.

기본 컨피그레이션

기본적으로 FTD LINA 컨피그레이션에는 모든 기본 애플리케이션 검사 트래픽과 일치하는 정책이 포함됩니다.

검사는 모든 인터페이스의 트래픽에 적용됩니다(전역 정책).

기본 애플리케이션 검사 트래픽에는 각 프로토콜의 기본 포트에 대한 트래픽이 포함됩니다. 글로벌 정책은 하나만 적용할 수 있으므로, 예를 들어 검사를 비표준 포트에 적용하거나 기본적으로 활성화되지 않은 검사를 추가하려면 기본 정책을 수정하거나 비활성화하고 새 정책을 적용해야 합니다.

LINA에서 show running-config policy-map, system support diagnostic-cli를 통해 FTD Command Line Interface(CLI) 명령을 실행하여 정보를 얻습니다.

```
firepower# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 parameters
  eool action allow
  nop action allow
  router-alert action allow
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
```

```
  inspect skinny
  inspect sunrpc
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
  inspect icmp error
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 class class_snmp
  inspect snmp
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
!
```

MPF 프로토콜 검사로 인한 패킷 삭제 식별

트래픽이 방화벽에 할당된 ACP(Access Control Policy)와 일치하는 경우에도 특정 시나리오에서 검사 프로세스는 방화벽에 수신된 특정 트래픽 동작, 지원되지 않는 설계, 애플리케이션 표준 또는 검사 제한으로 인해 연결을 종료합니다.

트래픽 트러블슈팅 중에 유용한 프로세스는 다음과 같습니다.

- 트래픽이 흐르는 인터페이스(인그레스 및 이그레스 인터페이스)에 실시간 캡처 로그를 설정합니다. 다음 명령을 사용합니다.

```
firepower# capture

        [interface

        ][match


           [port

           ]


             [port

             ]]
```

캡처를 사용하면 패킷 번호 X 추적 세부 정보를 포함할 수 있으며, 패킷 추적기 명령처럼 연결을 수행할 때 단계별로 결과 단계를 제공해야 하지만, 이 옵션을 사용하면 실시간 트래픽임을 확인할 수 있습니다.

```
firepower# show capture

        packet number X trace detail
```

- 실시간 ASP(Accelerated Security Path) 삭제를 설정합니다. 캡처 유형 asp-drop은 ASP에서 삭제한 패킷 또는 연결을 표시합니다. 문서의 관련 링크에서 찾을 수 있는 이유 목록이 있습니다.

```
firepower# capture

        [type

        ] [interface

         ][match

            [port

            ]
```

```
[port

]]
```

패킷-추적기 단계에서 허용 결과를 관찰할 수 있으므로 프로토콜 검사 삭제를 무시할 수 있습니다. 따라서 실시간 캡처 로그를 사용하여 삭제 이유를 항상 확인하는 것이 중요합니다.

일반 삭제 오류 메시지

ASP(Accelerated Security Path) 드롭은 네트워크 문제를 해결하는 데 도움이 되는 디버깅 목적으로 자주 사용됩니다. show asp drop 명령을 사용하여 이러한 삭제된 패킷 또는 연결을 표시함으로써 NAT 실패, 검사 실패 또는 액세스 규칙 거부와 같은 문제를 비롯한 삭제 이유에 대한 통찰력을 제공합니다.

ASP 삭제에 대한 핵심 사항:

- 프레임 삭제: 이는 잘못된 캡슐화 또는 호스트로 향하는 경로 없음과 같은 개별 패킷과 관련된 삭제입니다.
- 플로우 삭제: 이는 액세스 규칙 또는 NAT 실패에 의해 거부된 흐름과 같은 연결과 관련된 것입니다.
- 사용: 이 명령은 주로 디버깅을 위한 것이며 출력이 변경될 수 있습니다.

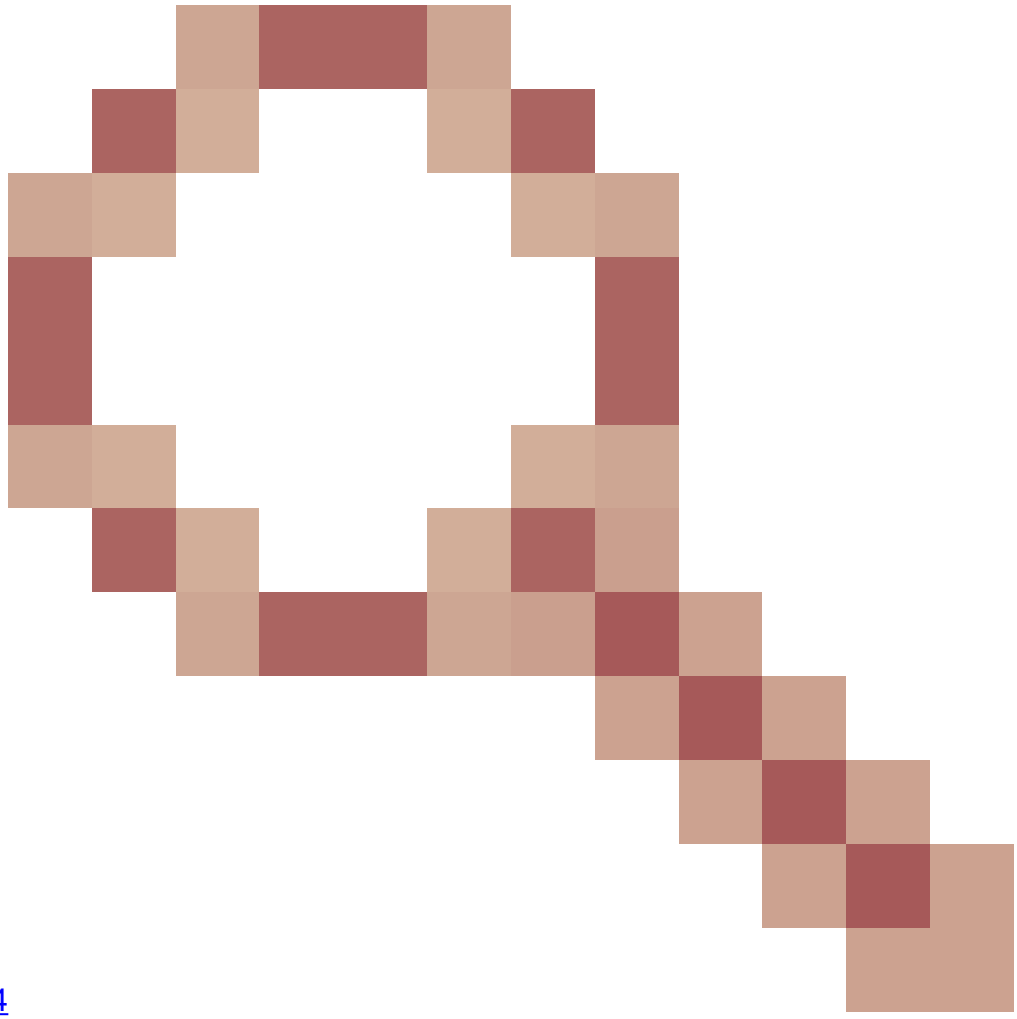
이러한 오류 메시지 또는 삭제 이유는 문제 해결 중에 발생할 수 있는 예입니다. 사용 중인 검사 프로토콜에 따라 지연할 수 있습니다.

SUN RPC 검사 삭제 예

이 시나리오는 AWS 구축의 단일 암 프록시 FTDv에 대한 것으로, Sun Rpc 검사가 활성화된 경우 연결이 삭제되는 경우 Geneve에서 캡슐화한 RPC 트래픽입니다.

이 출력은 Sun Rpc 검사에 대한 ASP 삭제를 보여줍니다. Sun Rcp는 포트 111을 대상으로 사용합니다. 마지막 패킷은 6081을 대상으로 사용하는 Geneve 캡슐화 포트입니다. 관찰할 수 있는 출력의 삭제 사유는 "유효한 인접성 없음"입니다.

```
firepower# show capture asp-drop
...
8: 16:23:02.462958 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency)
9: 16:23:09.769338 10.0.0.5.780 > 172.16.0.3.111: P 1795131583:1795131679(96) ack 526534108 win 29200 D
10: 16:23:10.148658 172.16.0.3.111 > 10.0.0.5.780: . ack 4026726685 win 26880 Drop-reason: (no-adjacenc
11: 16:23:10.463004 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency
12: 16:23:26.462729 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency
13: 16:23:27.548692 10.79.67.11.60855 > 10.79.67.4.6081: udp 176 [GENEVE segment-id 0 payload-length 13
```



Cisco 버그 ID CSCwj00074

FTDv 단일 암 프록시는 inspect sunrpc가 활성화된 상태에서 인접성이 없는 트래픽을 삭제합니다.

3방향 핸드셰이크의 두 번째 패킷(SYN/ACK) 이후 소스 및 대상 mac 주소가 갑자기 모두 0으로 채워지기 때문에 트래픽은 LINA 엔진의 ASP에서 'no-valid adjacency'로 삭제됩니다.

ASP 삭제 이유:

이름: 인접하지 않음

유효한 인접성 없음:
　이 카운터는 보안 어플라이언스가 더 이상 유효한 출력 인접성이 없는 기존 흐름에서 패킷을 수신할 때 증가합니다. 이는 다음 홉에 더 이상 연결할 수 없거나 일반적으로 동적 라우팅 환경에서 라우팅 변경이 발생한 경우에 발생할 수 있습니다.

해결책: sunrpc 검사를 비활성화합니다.

SQL*NET 검사 삭제 예

이 시나리오는 AWS 구축의 단일 암 프록시 FTDv에 대한 것으로, Sql*Nel 검사가 활성화된 경우 Geneve가 캡슐화한 트래픽이 삭제됩니다.

출력은 병합된 패킷 캡처에 대한 것입니다(동일한 패킷 번호를 관찰할 수 있음).
첫 줄: asp-drop 패킷 캡처는 캡슐화되지 않으며, Sql*Net은 1521 포트를 대상으로 사용합니다.
두 번째 줄: LINA의 VNI 인터페이스 asp-drop, Geneve는 캡슐화 포트 6081을 대상으로 사용합니다
.

출력에 두 가지 다른 삭제 이유가 있습니다. "tcp-buffer-timeout"과 "tcp-not-syn"이 확인될 수 있습니다

```
95    2024-12-14 07:55:58.771764    172.16.0.14    10.0.8.2    TCP    251    53905 → 1521 [PSH, ACK] Seq=
95: 07:55:58.771764       10.7.0.3.64056 > 10.7.2.5.6081:  udp 209 [GENEVE segment-id 0 payload-length 169] Drop-

96    2024-12-14 07:55:58.771780    172.16.0.14    10.0.8.2    TCP    1514    [TCP Out-Of-Order] 53905 → 1521 [AC
96: 07:55:58.771780       10.7.0.3.64056 > 10.7.2.5.6081:  udp 1472 [GENEVE segment-id 0 payload-length 1432] Dro

99    2024-12-14 07:55:58.997049    172.16.0.14    10.0.8.2    TCP    308    53903 → 1521 [PSH, ACK] Seq=1 Ack=1
99: 07:55:58.997049       10.7.0.3.64056 > 10.7.2.5.6081:  udp 266 [GENEVE segment-id 0 payload-length 226] Drop-

100    2024-12-14 07:55:58.997079    172.16.0.14    10.0.8.2    TCP    1514    [TCP Out-Of-Order] 53903 → 1521 [A
100: 07:55:58.997079       10.7.0.3.64056 > 10.7.2.5.6081:  udp 1472 [GENEVE segment-id 0 payload-length 1432] Dr
```

ASP 삭제 이유:

이름: tcp-buffer-timeout
TCP 무순서 패킷 버퍼 시간 초과:
　대기열에서 벗어난 TCP 패킷이 너무 오래 버퍼에 보관되면 이 카운터가 증가하고 패킷이 삭제됩니다.일반적으로 TCP 패킷은 보안 어플라이언스에서 검사하는 연결에서 순서가 지정되거나 검사를 위해 SSM으로 패킷이 전송될 때 삭제됩니다. 다음 예상 TCP 패킷이 특정 기간 내에 도착하지 않으면 대기열에서 벗어난 패킷이 삭제됩니다.

권장 사항:
　다음으로 예상되는 TCP 패킷은 혼잡으로 인해 네트워크에 도착하지 않습니다. 이는 사용 중인 네트워크에서 정상입니다. 엔드 호스트의 TCP 재전송 메커니즘은 패킷을 재전송해야 하며 세션이 계속될 수 있습니다.

이름: tcp-not-syn

첫 번째 TCP 패킷이 SYN이 아님:
인터셉트되지 않은 고정 연결의 첫 번째 패킷으로 비 SYN 패킷을 받았습니다.

권장 사항:
정상적인 상황에서는 어플라이언스가 이미 연결을 닫은 상태에서 클라이언트 또는 서버가 여전히 연결이 열려 있다고 생각하고 데이터를 계속 전송할 때 이를 확인할 수 있습니다. 이러한 상황이 발생할 수 있는 몇 가지 예는 'clear local-host' 또는 'clear xlate'가 실행된 직후입니다. 또한 연결이 최근에 제거되지 않았는데 카운터가 빠르게 증가하는 경우 어플라이언스를 공격할 수 있습니다. 스니퍼 추적을 캡처하여 원인을 격리합니다.

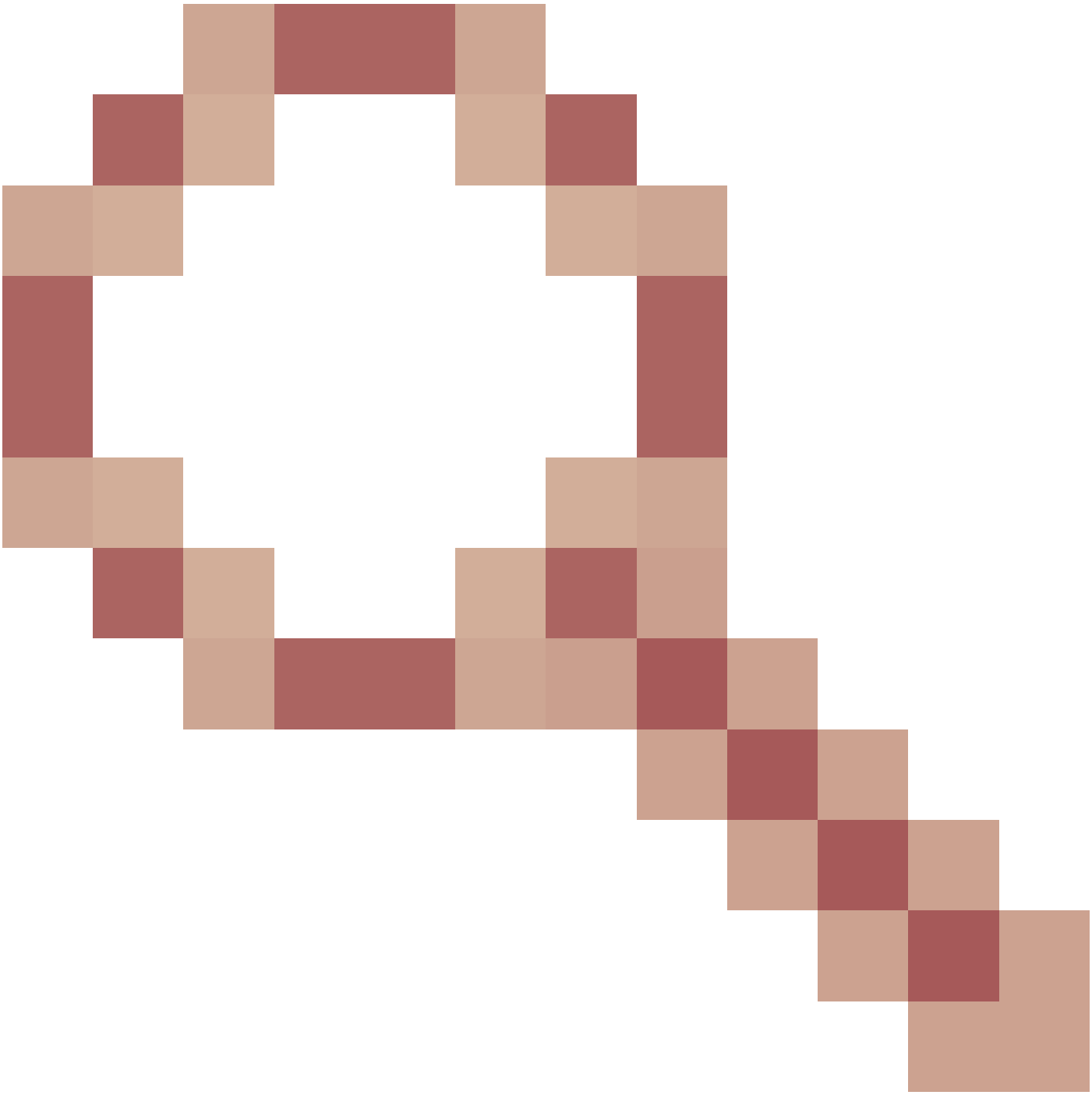
해결책: SQL 제어 TCP 포트 1521과 동일한 포트에서 SQL 데이터 전송이 발생하는 경우 SQL*Net 검사를 비활성화합니다. 보안 어플라이언스는 SQL*Net 검사가 활성화된 경우 프록시 역할을 하며 클라이언트 윈도우 크기를 65000에서 약 16000으로 줄여서 데이터 전송 문제를 일으킵니다.

ICMP 검사 삭제 예

이 시나리오는 FTD 클러스터 환경을 위한 것입니다.
ICMP 헤더의 ICMP 식별자는 플로우에서 5-튜플의 소스 포트로 사용될 수 있으므로 ping 패킷의 5-튜플은 모두 동일하며, 이 출력에서 관찰할 수 있는 것처럼 ASP 삭제 사유는 "inspect-icmp-seq-num-not-matched"입니다.

```
firepower#show cap asp-drop
 1: 19:47:09.293136 10.0.5.8 > 10.50.0.53 icmp: echo reply Drop-reason: (inspect-icmp-seq-num-not-match
```

Cisco 버그 ID CSCvb92417



Cluster ASA에서 To-the-box ICMP 회신을 "inspect-icmp-seq-num-not-matched" 사유로 삭제합니다.

ASP 삭제 이유:

이름: inspect-icmp-seq-num-not-matched
ICMP 검사 시퀀스 번호가 일치하지 않음:
ICMP 에코 응답 메시지의 시퀀스 번호가 동일한 연결에서 이전에 어플라이언스를 통해 전달된 ICMP 에코 메시지와 일치하지 않을 경우 이 카운터를 증가시켜야 합니다.

해결책: ICMP 검사를 비활성화합니다. 클러스터 환경: 클러스터에 있는 둘 이상의 FTD 및 ICMP 트래픽은 비대칭적일 수 있습니다. ICMP 흐름 삭제에 대한 지연이 있는 것으로 관찰되며, 이전 ping 흐름이 정리되기 전에 후속 ping이 빠르게 전송됩니다. 이 경우 패킷 손실이 연속적으로 발생할 수

있습니다.

SIP 검사 삭제 예

이 시나리오에서는 통화가 5분 동안만 지속된 다음 연결이 끊어집니다. RTP를 사용하면 SIP 검사에서 연결을 삭제할 수 있습니다.
VoIP 트래픽에 대한 인터페이스의 패킷 캡처 출력에서 확인할 수 있듯이, SIP 트래픽의 BYE 플래그는 해당 시간에 전화가 닫혔음을 의미합니다.

```
1    2023-10-13 18:39:03.421456    10.6.6.66    172.16.3.77    SIP/SDP    1055    Request: INVITE sip:1
2    2023-10-13 18:39:03.448325    172.16.3.77    10.6.6.66    SIP    497    Status: 100 Trying |
3    2023-10-13 18:39:03.525424    172.16.3.77    10.6.6.66    SIP    687    Status: 401 Unauthorized |
4    2023-10-13 18:39:03.525943    10.6.6.66    172.16.3.77    SIP    425    Request: ACK sip:123456789
5    2023-10-13 18:39:03.527331    10.6.6.66    172.16.3.77    SIP/SDP    1343    Request: INVITE sip:1
6    2023-10-13 18:39:03.553544    172.16.3.77    10.6.6.66    SIP    497    Status: 100 Trying |
7    2023-10-13 18:39:05.902815    172.16.3.77    10.6.6.66    SIP/SDP    992    Status: 183 Session Pr
8    2023-10-13 18:39:06.091822    172.16.3.77    10.6.6.66    SIP/SDP    967    Status: 180 Ringing |
9    2023-10-13 18:39:13.114435    172.16.3.77    10.6.6.66    SIP/SDP    1063    Status: 200 OK (INVIT
10    2023-10-13 18:39:13.115899    10.6.6.66    172.16.3.77    SIP    560    Request: ACK sip:55663399
11    2023-10-13 18:40:29.206593    172.16.3.77    10.6.6.66    SIP    642    Request: UPDATE sip:FD3a5
12    2023-10-13 18:40:29.207630    10.6.6.66    172.16.3.77    SIP    659    Status: 200 OK (UPDATE) |
13    2023-10-13 18:41:09.940854    10.6.6.66    172.16.3.77    SIP    684    Request: BYE sip:33445566
14    2023-10-13 18:41:10.003066    172.16.3.77    10.6.6.66    SIP    659    Status: 200 OK (BYE) |
```

이 다른 예에서 syslog는 PAT를 사용하는 매핑된 IP를 표시합니다. IP는 사용 가능한 포트가 하나뿐이며 SIP 세션은 동일한 포트에 연결되었습니다. 포트 할당으로 인해 SIP가 실패했습니다. PAT가 사용 중인 경우 SIP 검사는 연결을 끊을 수 있습니다.

ASP 삭제 이유는 다음과 같습니다. "호스트별 PAT 포트 차단 제한인 X에 도달하여 IP/포트에서 IP/포트로의 UDP 연결을 만들 수 없습니다." 및 "검사 엔진에서 종료됨, 이유 - '서비스 재설정' 컨피그레이션에 따라 재설정됨"

```
Nov 18 2019 10:19:34: %FTD-6-607001: Pre-allocate SIP Via UDP secondary channel for 3111:10.11.0.13/506
Nov 18 2019 10:19:35: %FTD-6-302022: Built backup stub TCP connection for identity:172.16.2.20/2325 (17
Nov 18 2019 10:19:38: %FTD-3-305016: Unable to create UDP connection from 3111:10.11.0.12/50195 to 3121
Nov 18 2019 10:19:38: %FTD-4-507003: udp flow from 3111:10.11.0.12/5060 to 3121:10.21.0.12/5060 termina
Nov 18 2019 10:19:39: %FTD-3-305016: Unable to create UDP connection from 3111:10.11.0.12/50195 to 3121
Nov 18 2019 10:19:39: %FTD-4-507003: udp flow from 3111:10.11.0.12/5060 to 3121:10.21.0.12/5060 termina
```

ASP 삭제 이유:

이름: 비동기 잠금 큐 제한
비동기 잠금 큐 제한 초과:
　각 비동기 잠금 작업 대기열의 제한은 1000입니다. 더 많은 SIP 패킷을 작업 대기열로 디스패치하려는 경우 패킷을 삭제해야 합니다.
권장 사항:

SIP 트래픽만 삭제할 수 있습니다. SIP 패킷에 동일한 상위 잠금이 있고 동일한 비동기 잠금 큐에 대기시킬 수 있는 경우, 단일 코어만 모든 미디어를 처리하므로 블록이 고갈될 수 있습니다. 비동기 잠금 대기열의 크기가 제한을 초과할 때 SIP 패킷이 대기열을 시도하려면 패킷을 삭제해야 합니다.

이름: sp-looping-address
루프 주소:
이 카운터는 흐름의 소스 주소와 대상 주소가 같을 때 증가합니다. 주소 프라이버시가 활성화된 SIP 플로우는 제외됩니다. 이러한 플로우는 동일한 소스 및 대상 주소를 갖는 것이 일반적입니다.

권장 사항:
이 카운터가 증가할 수 있는 조건은 두 가지입니다. 하나는 어플라이언스가 소스 주소가 목적지와 동일한 패킷을 수신하는 경우입니다. DoS 공격의 유형을 나타냅니다. 두 번째는 어플라이언스의 NAT 컨피그레이션이 목적지의 소스 주소와 동일한 경우 입니다.

이름: 부모-닫힘
상위 흐름이 닫혔습니다.
종속 흐름의 상위 흐름이 닫히면 종속 흐름도 닫힙니다. 예를 들어 FTP 데이터 흐름(종속 흐름)은 제어 흐름(상위 흐름)이 종료될 때 이 특정 이유로 종료될 수 있습니다. 이러한 이유는 또한 그 제어 애플리케이션에 의해 2차 유동(핀-홀)이 폐쇄될 때 주어진다. 예를 들어, BYE 메시지가 수신되면 SIP 검사 엔진(제어 애플리케이션)이 해당 SIP RTP 플로우(보조 플로우)를 닫아야 합니다.

해결책: SIP 검사를 비활성화합니다. 프로토콜의 제한 때문에:

- SIP 검사는 채팅 기능만 지원합니다. 화이트보드, 파일 전송 및 애플리케이션 공유는 지원되지 않습니다. RTC Client 5.0은 지원되지 않습니다.
- PAT를 사용하는 경우 포트 없이 내부 IP 주소가 포함된 SIP 헤더 필드를 변환할 수 없으므로 내부 IP 주소가 외부로 유출될 수 있습니다. 이 유출을 방지하려면 PAT 대신 NAT를 구성합니다.
- SIP 검사는 다음과 같은 기본 검사 맵을 사용하여 기본적으로 활성화됩니다.
  * SIP IM(인스턴트 메시징) 확장: 활성화됨.
  * SIP 포트의 비 SIP 트래픽: 삭제됨.
  * 서버 및 엔드포인트 IP 주소 숨기기: 비활성화됨.
  * 마스크 소프트웨어 버전 및 비 SIP URI: 비활성화됨.
  * 대상으로의 홉(hop) 수가 0보다 큰지 확인하십시오. 활성화됨.
  * RTP 적합성: 적용되지 않습니다.
  * SIP 적합성: 상태 검사 및 헤더 검증을 수행하지 마십시오.

문제 해결

다음은 LINA MPF 프로토콜 검사와 관련된 트래픽 문제를 해결하기 위해 제안된 명령 중 일부입니다.

- Show service-policy는 활성화된 LINA MPF 검사에 대한 서비스 정책 통계를 표시합니다.

```
firepower# show service-policy
```

```
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/s
      Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-clo
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-clo
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-
      Inspect: skinny, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: netbios, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
      Inspect: icmp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
      Inspect: icmp error, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-f
      Inspect: ip-options UM_STATIC_IP_OPTIONS_MAP, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-
    Class-map: class_snmp
      Inspect: snmp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
    Class-map: class-default

      Default Queueing      Set connection policy:         drop 0
      Set connection advanced-options: UM_STATIC_TCP_MAP
        Retransmission drops: 0                   TCP checksum drops : 0
        Exceeded MSS drops  : 0                   SYN with data drops: 0
        Invalid ACK drops   : 0                   SYN-ACK with data drops: 0
        Out-of-order (OoO) packets : 0            OoO no buffer drops: 0
        OoO buffer timeout drops : 0              SEQ past window drops: 0
        Reserved bit cleared: 0                   Reserved bit drops : 0
        IP TTL modified     : 0                   Urgent flag cleared: 0
        Window varied resets: 0
        TCP-options:
          Selective ACK cleared: 0                Timestamp cleared  : 0
          Window scale cleared : 0
          Other options cleared: 0
          Other options drops: 0
```

show service-policy inspect http 명령의 이 샘플 출력에서는 http 통계를 보여줍니다.

```
firepower# show service-policy inspect http
    Global policy:
      Service-policy: global_policy
        Class-map: inspection_default
          Inspect: http http, packet 1916, drop 0, reset-drop 0
            protocol violations
              packet 0
            class http_any (match-any)
              Match: request method get, 638 packets
              Match: request method put, 10 packets
              Match: request method post, 0 packets
              Match: request method connect, 0 packets
              log, packet 648
```

- 검사할 인터페이스에서 asp-drop 캡처를 설정합니다.

```
Syntax
#Capture


        type asp-drop


         match
```

```
for example
#Capture asp type asp-drop all match ip any any
#Capture asp type asp-drop all match ip any host x.x.x.x
#Capture asp type asp-drop all match ip host x.x.x.x host x.x.x.x
```

특정 LINA MPF 애플리케이션 검사를 활성화 또는 비활성화하는 방법

Cisco Secure Firewall Threat Defense에서 MPF LINA 애플리케이션 검사를 활성화하거나 비활성화할 수 있는 옵션입니다.

- FlexConfig를 통한 구성: FMC UI에 대한 관리자 액세스 권한이 필요합니다. 이 변경 사항은 컨피그레이션에 영구적입니다.
- FTD CLI를 통한 구성: FTD CLI에 대한 관리자 액세스 권한이 필요합니다. 이 변경 사항은 영구적이지 않습니다. 재부팅 또는 새 구축이 이루어지면 컨피그레이션이 제거됩니다.

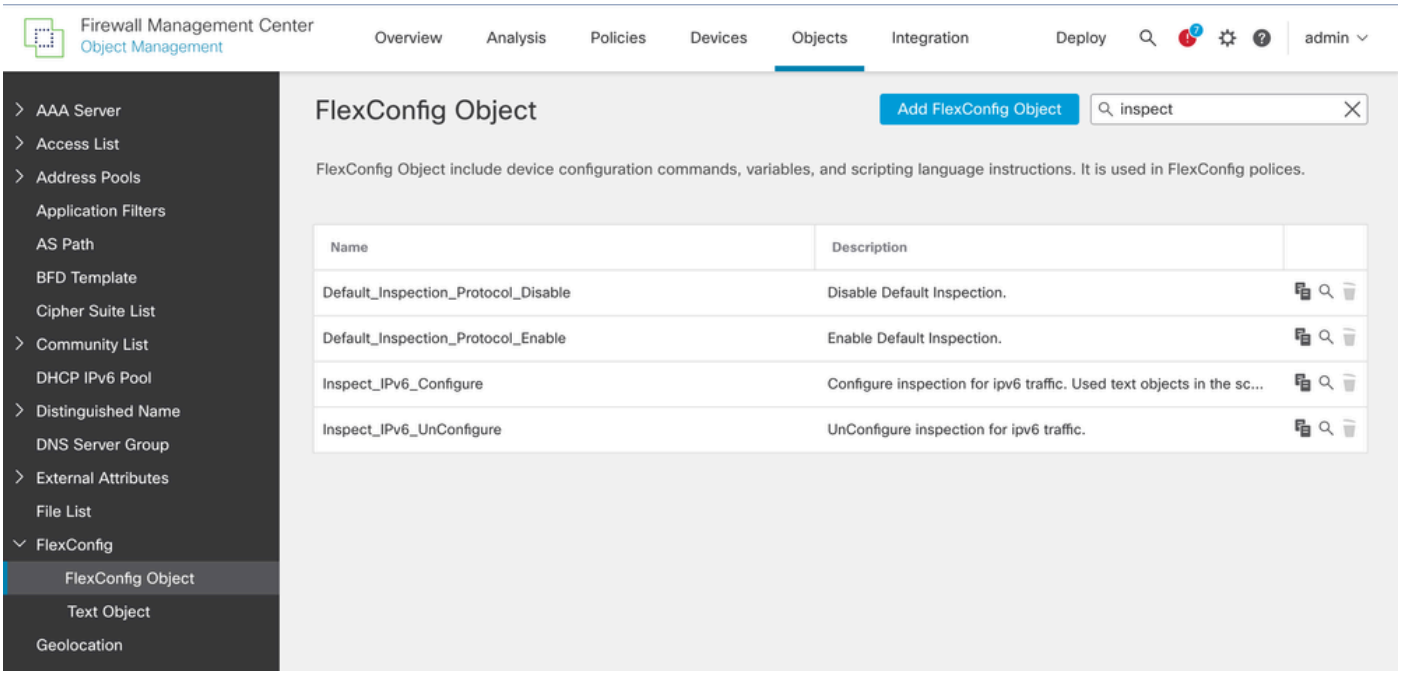
FlexConfig를 통한 컨피그레이션

FlexConfig는 위협 방어와 호환되지만 관리 센터에서 구성할 수 없는 ASA 기반 기능을 구성하는 마지막 방법입니다.

검사를 영구적으로 비활성화하거나 활성화하는 컨피그레이션은 FMC UI를 통해 FlexConfig에 있으며, 전역적으로 또는 특정 트래픽에만 적용할 수 있습니다.

1단계.

FMC UI에서 Objects(개체) > Object Management(개체 관리) > FlexConfig > FlexConfig Object(FlexConfig 개체)로 이동하면 기본 Protocol Inspection(프로토콜 검사) 개체 목록을 찾을 수 있습니다.



기본 FlexConfig 프로토콜 검사 개체

2단계.

특정 프로토콜 검사를 비활성화하려면 FlexConfig 개체를 만들 수 있습니다.

Objects(개체) > Object Management(개체 관리) > FlexConfig > FlexConfig Object(FlexConfig 개체) > Add FlexConfig Object(FlexConfig 개체 추가)로 이동합니다.

이 예에서 global_policy에서 SIP 검사를 비활성화하려면 다음 구문을 사용해야 합니다.

```
policy-map global_policy
 class inspection_default
  no inspect sip
```

FlexConfig 객체를 구성할 때 구축 빈도 및 유형을 선택할 수 있습니다.

구축

- FlexConfig 객체가 네트워크 또는 ACL 객체와 같은 시스템 관리 객체를 가리키는 경우

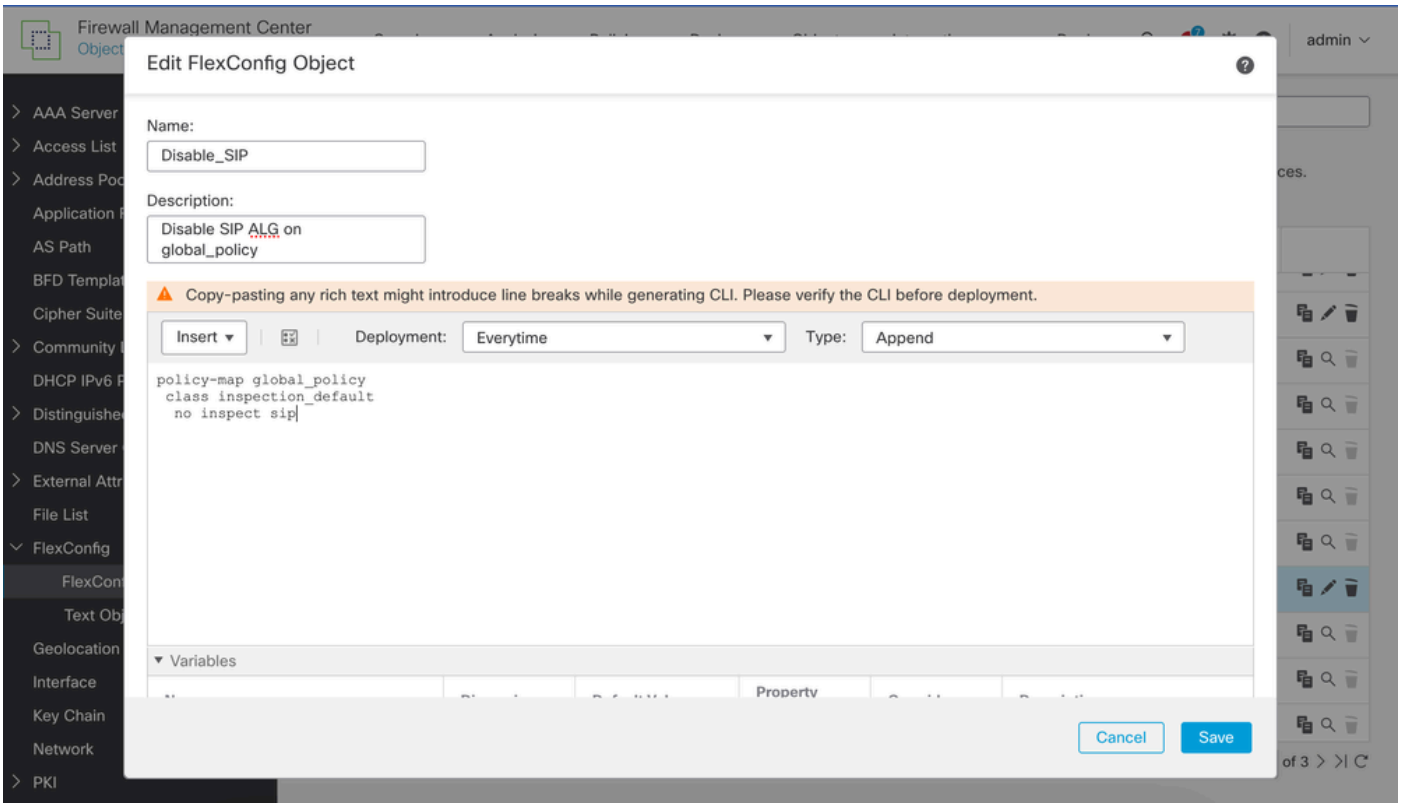
Everytime을 선택합니다. 그렇지 않으면 개체에 대한 업데이트를 배포할 수 없습니다.

- 개체에서 컨피그레이션을 지우는 작업만 수행하는 경우 한 번을 사용합니다. 그런 다음 다음 다음 구축 후 FlexConfig 정책에서 객체를 제거합니다.

유형

- Append(기본값) 객체의 명령은 관리 센터 정책에서 생성된 컨피그레이션의 끝에 배치됩니다. 관리 객체에서 생성된 객체를 가리키는 정책 객체 변수를 사용하는 경우 Append를 사용해야 합니다. 다른 정책에 대해 생성된 명령이 객체에 지정된 명령과 겹치는 경우 명령을 덮어쓰지 않도록 이 옵션을 선택해야 합니다. 이것이 가장 안전한 옵션입니다.

- 앞에 추가합니다. 개체의 명령은 관리 센터 정책에서 생성된 구성의 시작 부분에 배치됩니다. 일반적으로 컨피그레이션을 지우거나 부정하는 명령에 prepend를 사용합니다.



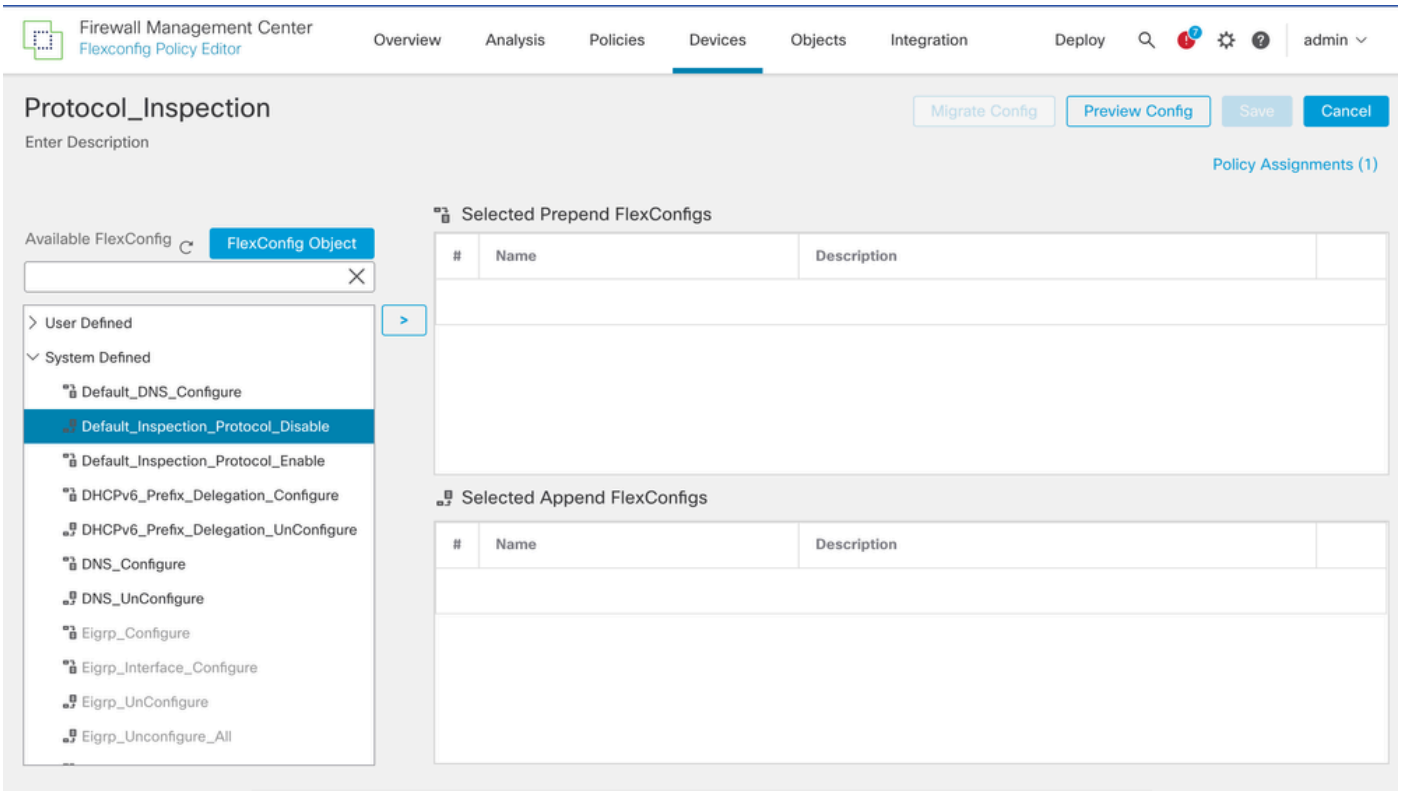
기본 global_policy에서 단일 프로토콜을 비활성화할 객체 생성

3단계.

LINA에 할당된 FlexConfig 정책에 개체를 추가합니다.

Devices(디바이스) > FlexConfig로 이동하여 삭제 문제가 있는 방화벽에 적용된 FlexConfig 정책을 선택합니다.

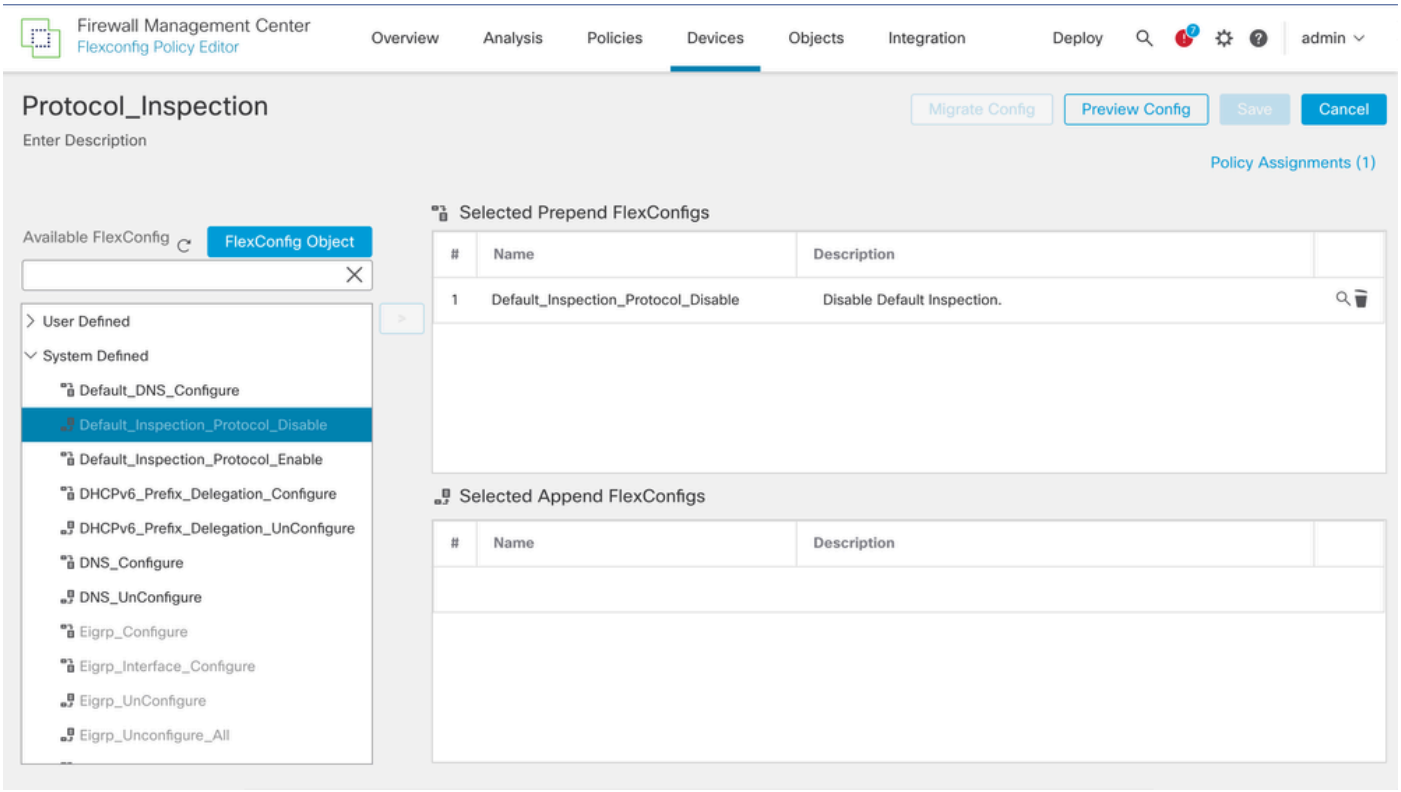
모든 검사를 전역적으로 비활성화하려면 System Defined FlexConfig Objects(시스템 정의 FlexConfig 개체)에서 Object Default_Inspection_Protocol_Disable(개체 Default_Inspection_Protocol_Disable)을 선택한 다음 그 사이의 파란색 화살표를 클릭하여 FlexConfig 정책에 추가합니다.



모든 프로토콜 검사를 비활성화하려면 시스템 정의 개체를 선택합니다

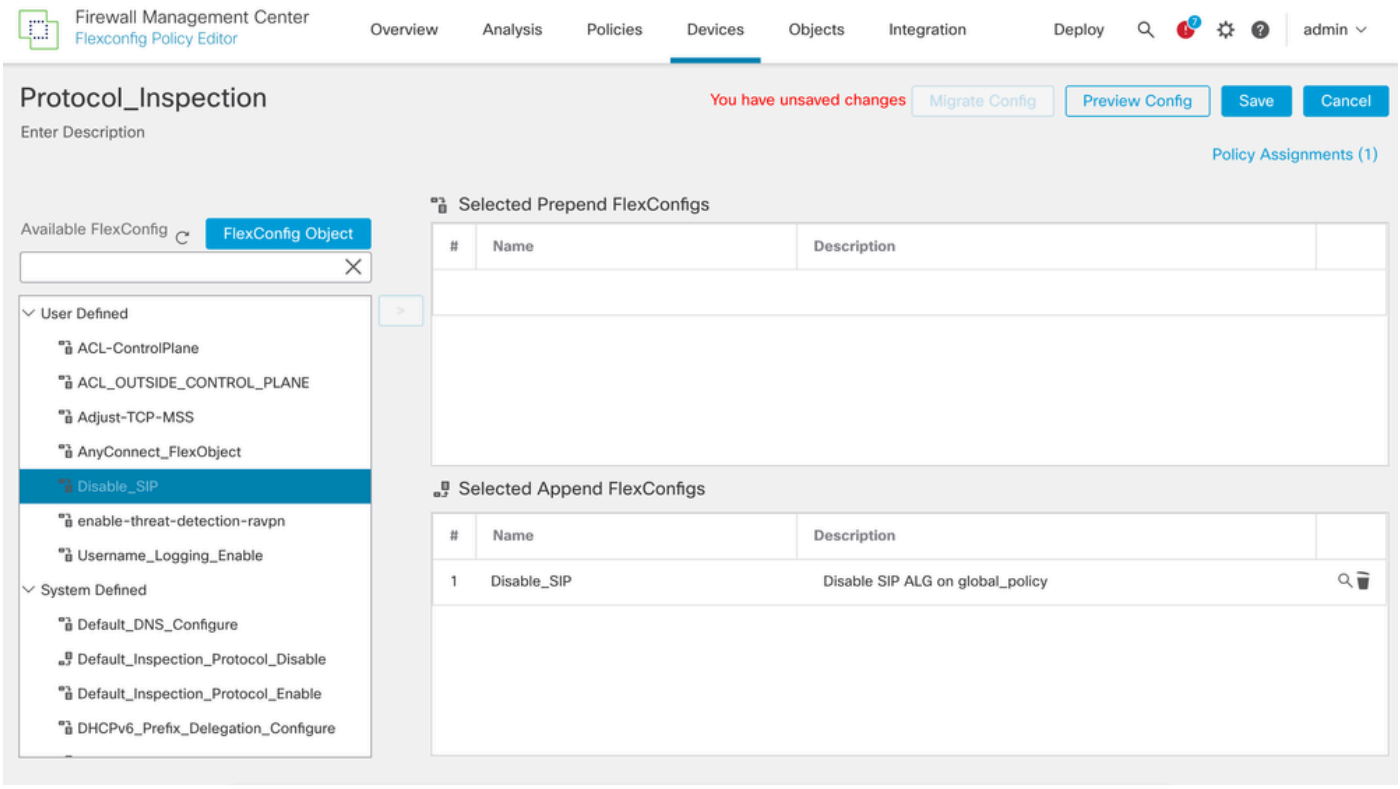
4단계.

선택한 후에는 오른쪽 상자에 해당 컨피그레이션이 표시되는지 확인합니다. 컨피그레이션을 저장하고 구축하는 것을 잊지 마십시오.



모든 프로토콜 검사를 비활성화하도록 선택한 개체

5단계.
단일 프로토콜 검사를 비활성화하려면 User defined(사용자 정의) 목록에서 이전에 생성한 객체를 선택하고 상자 사이의 화살표를 사용하여 정책에 추가합니다.



global_policy에서 단일 프로토콜 검사를 비활성화하려면 선택합니다.

6단계.

선택한 후에는 오른쪽 상자에 해당 컨피그레이션이 표시되는지 확인합니다. 컨피그레이션을 저장하고 구축하는 것을 잊지 마십시오.

FTD CLI를 사용한 컨피그레이션

이 솔루션은 FTD CLI에서 즉시 적용하여 검사가 트래픽에 영향을 미치는지 테스트할 수 있습니다. 그러나 재부팅 또는 새 구축이 발생할 경우 컨피그레이션 변경 사항은 저장되지 않습니다.

이 명령은 FTD CLI에서 클라이언트 모드로 실행해야 합니다.

```
> configure inspection


        disable

for example
> configure inspection SIP disable
```

다음을 확인합니다.

프로토콜 비활성화가 유효한지 확인하려면 show running-config policy-map 명령을 실행합니다. 이 예에서는 SIP 검사가 더 이상 기본 프로토콜 목록에 나타나지 않으므로 비활성화됩니다.

```
firepower# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 parameters
  eool action allow
  nop action allow
  router-alert action allow
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect netbios
  inspect tftp
  inspect icmp
  inspect icmp error
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 class class_snmp
  inspect snmp
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
!
firepower#
```

관련 정보

기술 지원 및 문서 – Cisco Systems

- 애플리케이션 레이어 프로토콜 검사 시작
- 기본 인터넷 프로토콜 검사
- ASP Drop 명령 사용 표시

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.