인라인 쌍 모드에서 FTD 인터페이스 구성

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소
- 관련 제품

배경 정보

FTD에서 인라인 쌍 인터페이스 구성

- 네트워크 다이어그램

다음을 확인합니다.

FTD 인라인 쌍 인터페이스 작업 확인

- 기본 이론
- 확인 1. Packet-Tracer 사용 시
- 확인 2. 인라인 쌍을 통해 TCP SYN/ACK 패킷 전송
- 확인 3. 허용되는 트래픽에 대한 방화벽 엔진 디버그
- 확인 4. 링크 상태 전파 확인
- 확인 5. 고정 NAT 구성

인라인 쌍 인터페이스 모드에서 패킷 차단

Tap를 사용하여 인라인 쌍 모드 구성

탭 인터페이스 작업으로 FTD 인라인 쌍 확인

인라인 쌍 및 Etherchannel

- Etherchannel이 FTD에서 종료됨
- FTD를 통한 Etherchannel

문제 해결

비교: Inline Pair vs Inline Pair with Tap

요약

관련 정보

소개

이 문서에서는 FTD(Firepower Threat Defense) 어플라이언스에서 Inline Pair Interface의 컨피그레이션, 확인 및 작동에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요구 사항은 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Firepower 4150 FTD(코드 6.1.0.x 및 6.3.x)
- FMC(firepower 관리 센터)(코드 6.1.0.x 및 6.3.x)

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.

관련 제품

이 문서는 다음과 같은 하드웨어 및 소프트웨어 버전에서도 사용할 수 있습니다.

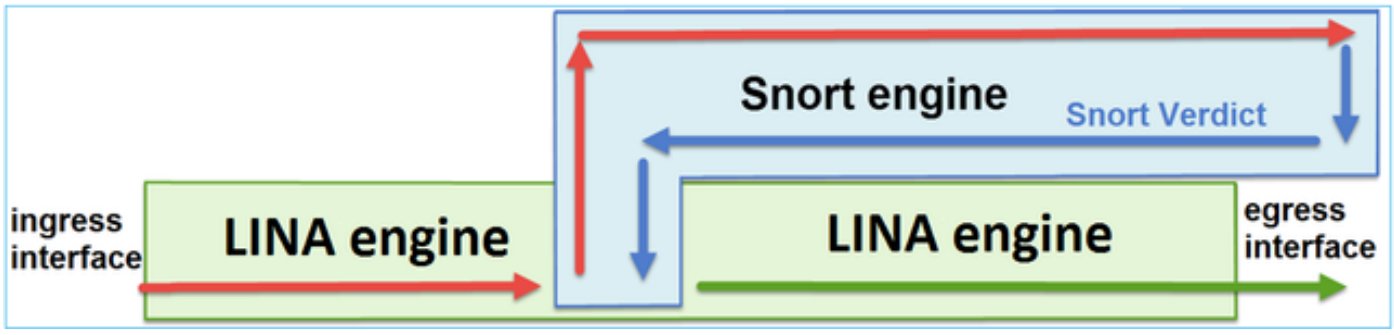
- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR2100, FPR4100, FPR9300
- VMware(ESXi), Amazon Web Services(AWS), Kernel-based Virtual Machine(KVM)
- FTD 소프트웨어 코드 6.2.x 이상

배경 정보

FTD는 2개의 주 엔진으로 구성된 통합 소프트웨어 이미지입니다.

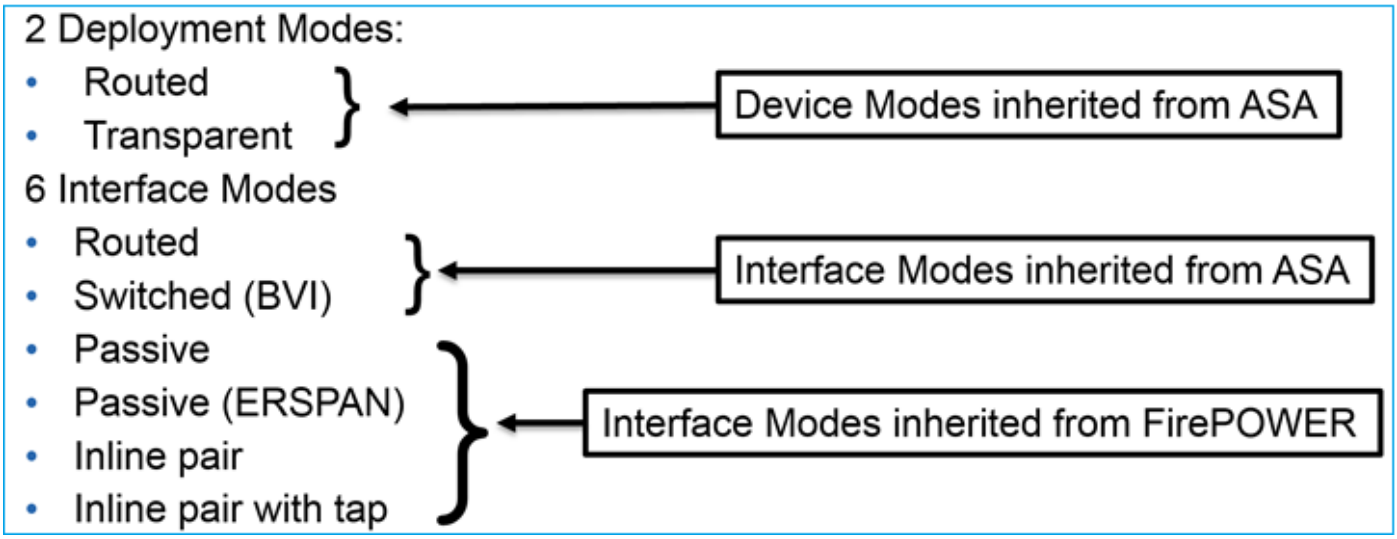
- LINA 엔진
- Snort 엔진

이 그림은 2개의 엔진이 상호 작용하는 방식을 보여줍니다.



- 패킷이 인그레스 인터페이스로 들어가고 LINA 엔진에 의해 처리됩니다.
- FTD 정책에 필요한 경우 Snort 엔진에서 패킷을 검사합니다.
- Snort 엔진이 패킷에 대한 판정을 반환합니다
- LINA 엔진은 Snort의 판정에 따라 패킷을 삭제 또는 포워딩합니다.

FTD는 그림과 같이 2가지 구축 모드와 6가지 인터페이스 모드를 제공합니다.



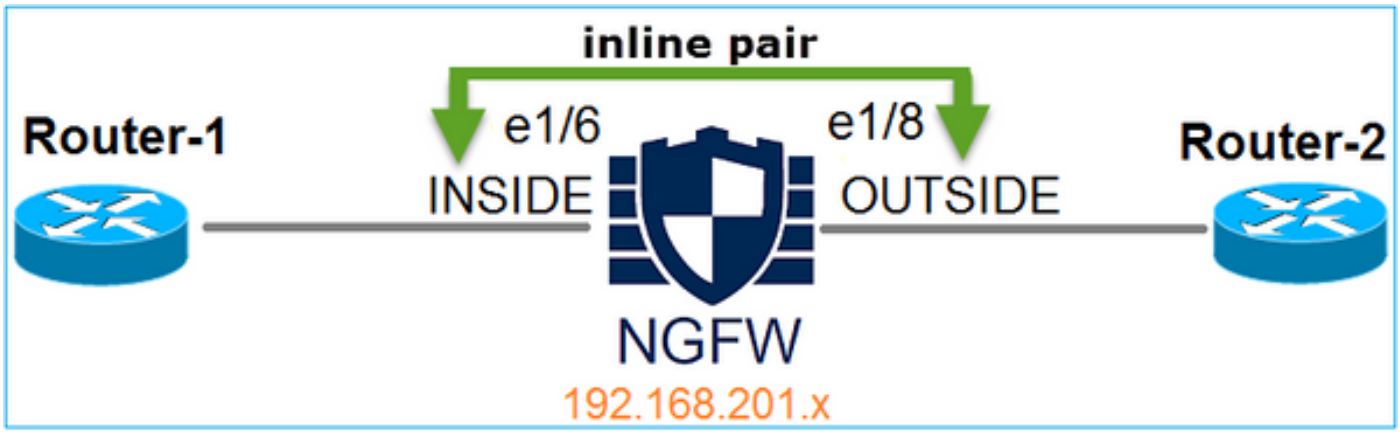
참고: 단일 FTD 어플라이언스에서 인터페이스 모드를 혼합할 수 있습니다.

다음은 다양한 FTD 구축 및 인터페이스 모드에 대한 개괄적인 개요입니다.

FTD 인터페이스 모드	FTD 구축 모드	설명	트래픽 삭제 가능
라우팅됨	라우팅됨	전체 LINA 엔진 및 Snort 엔진 검사	예
전환됨	투명	전체 LINA 엔진 및 Snort 엔진 검사	예
인라인 쌍	라우팅 또는 투명	부분 LINA 엔진 및 전체 Snort 엔진 검사	예
Tap가 있는 인라인 쌍	라우팅 또는 투명	부분 LINA 엔진 및 전체 Snort 엔진 검사	아니요
수동	라우팅 또는 투명	부분 LINA 엔진 및 전체 Snort 엔진 검사	아니요
수동(ERSPAN)	라우팅됨	부분 LINA 엔진 및 전체 Snort 엔진 검사	아니요

FTD에서 인라인 쌍 인터페이스 구성

네트워크 다이어그램



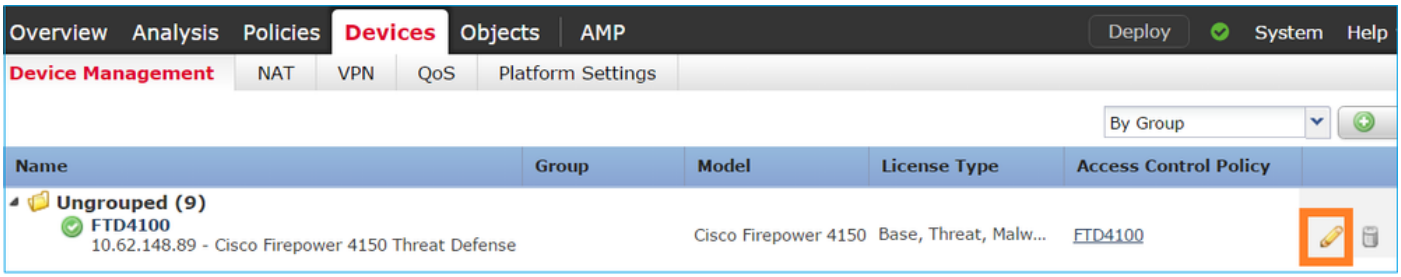
요건

다음 요구 사항에 따라 인라인 쌍 모드에서 물리적 인터페이스 e1/6 및 e1/8을 구성합니다.

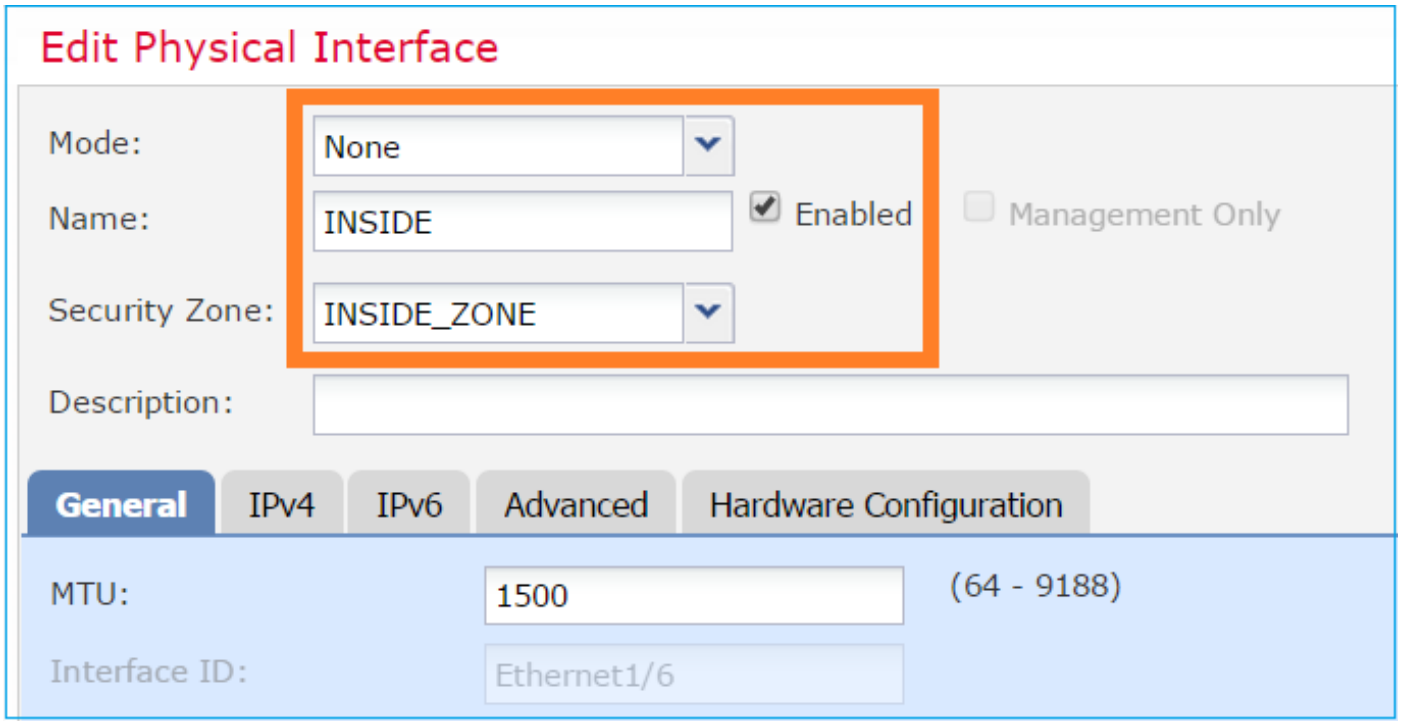
인터페이스	e1/6	e1/8
이름	내부	외부
보안 영역	내부 영역(_Z)	외부 영역(_Z)
인라인 집합 이름	인라인 쌍 1	
인라인 집합 MTU	1500	
고장 안전	사용	
링크 상태 전파	사용	

솔루션

1단계. 개별 인터페이스에 대해 구성하려면 Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 적절한 디바이스를 선택하고 이미지에 표시된 대로 Edit(수정)를 선택합니다.

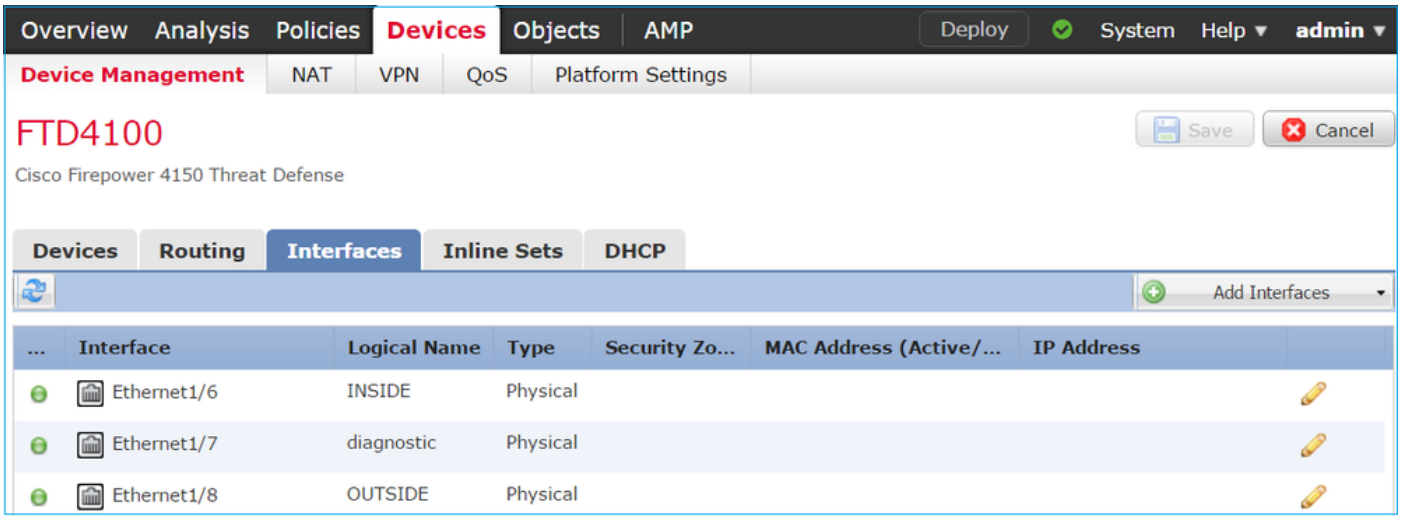


그런 다음 이미지에 표시된 대로 인터페이스에 대해 Name(이름) 및 Tick Enabled(틱 활성화)를 지정합니다.



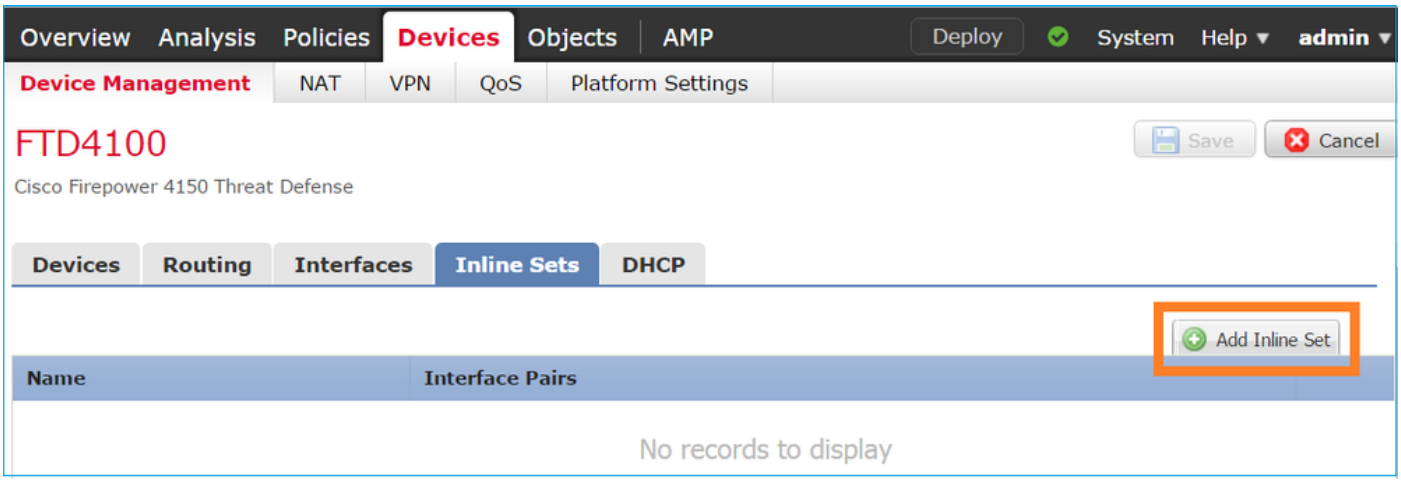
참고: Name(이름)은 인터페이스의 nameif입니다.

인터페이스 Ethernet1/8도 마찬가지입니다. 최종 결과는 그림과 같습니다.

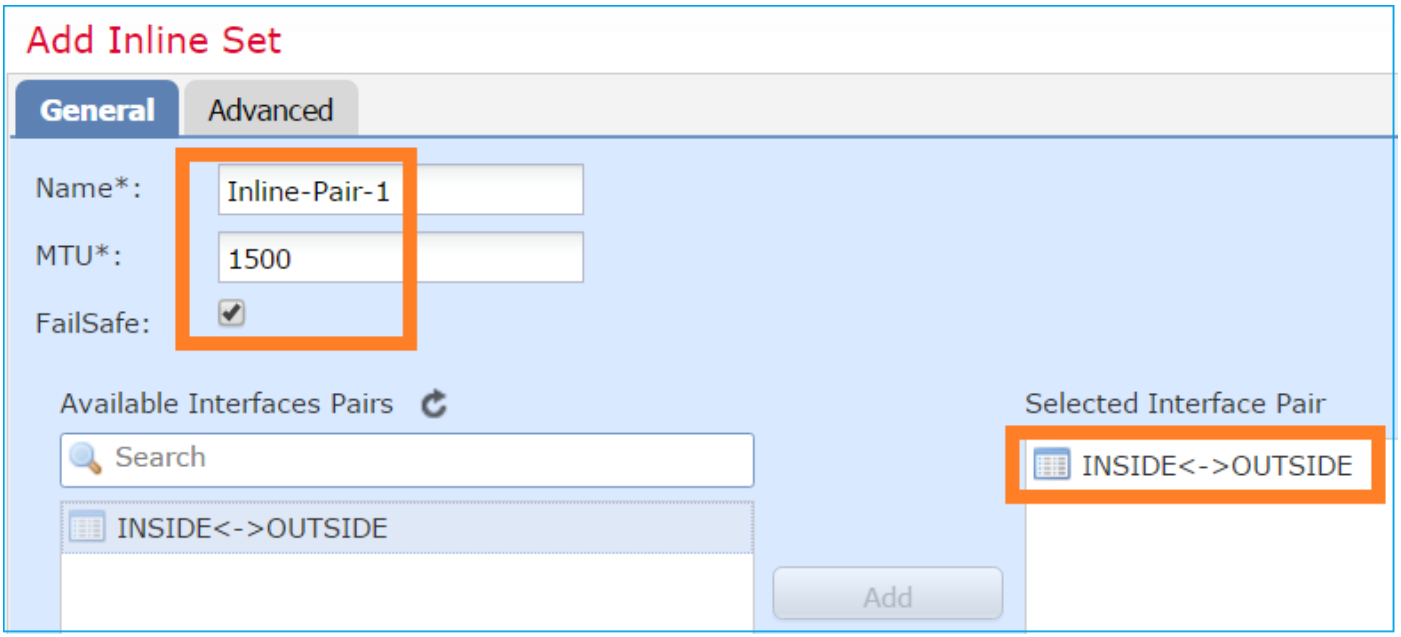


2단계. 인라인 쌍을 구성합니다.

이미지에 표시된 대로 Inline Sets(인라인 세트) > Add Inline Set(인라인 세트 추가)로 이동합니다.

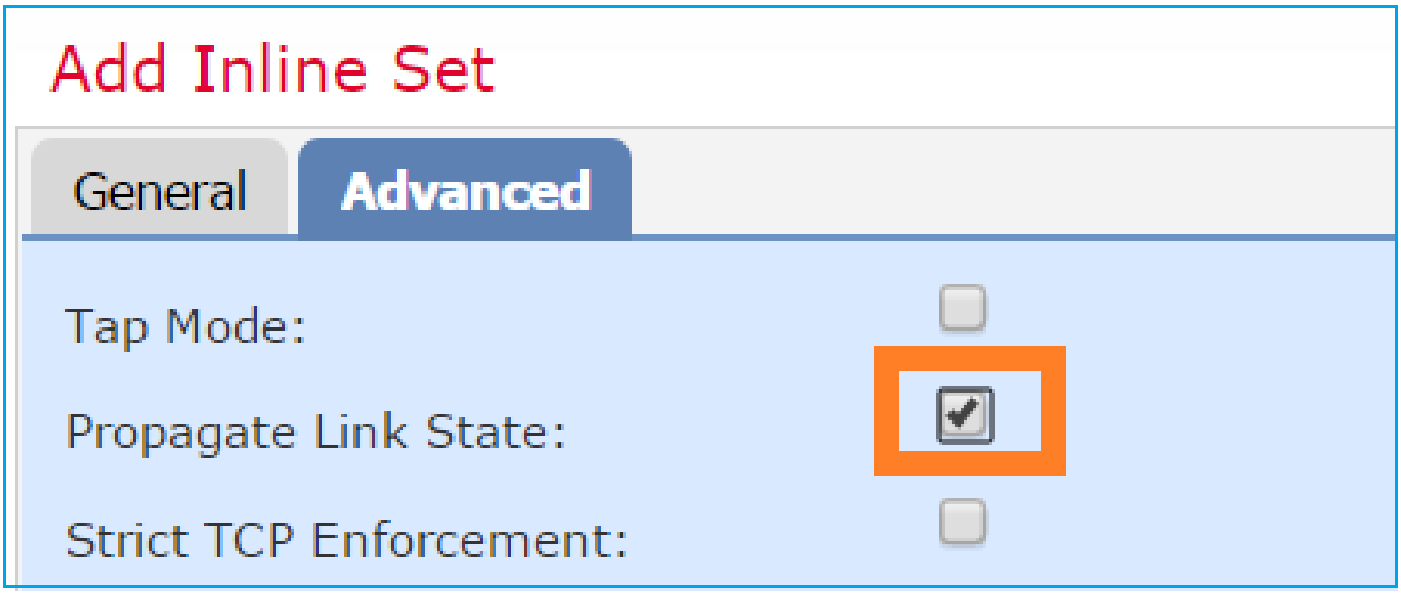


3단계. 이미지에 표시된 요구 사항에 따라 일반 설정을 구성합니다.



참고: Failsafe를 사용하면 인터페이스 버퍼가 가득 찬 경우(일반적으로 디바이스가 오버로드되거나 Snort 엔진이 오버로드될 때 표시됨) 트래픽이 검사되지 않은 인라인 쌍을 통과할 수 있습니다. 인터페이스 버퍼 크기가 동적으로 할당됩니다.

4단계. 이미지에 표시된 것처럼 Advanced Settings(고급 설정)에서 Propagate Link State(링크 상태 전파) 옵션을 활성화합니다.



링크 상태 전파는 인라인 집합의 인터페이스 중 하나가 다운될 때 인라인 인터페이스 쌍에서 두 번째 인터페이스를 자동으로 다운시킵니다.

5단계. 변경 사항을 저장하고 구축합니다.

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

FTD CLI에서 인라인 쌍 컨피그레이션을 확인합니다.

솔루션

FTD CLI에 로그인하고 인라인 쌍 컨피그레이션을 확인합니다.

```
> show inline-set

Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Failsafe mode is on/activated
  Failsecure mode is off
  Tap mode is off
  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/6 "INSIDE"
      Current-Status: UP
    Interface: Ethernet1/8 "OUTSIDE"
      Current-Status: UP
    Bridge Group ID: 509
>
```

참고: 브리지 그룹 ID는 0과 다른 값입니다. 탭 모드가 켜져 있으면 0입니다.

인터페이스 및 이름 정보:

```
<#root>

>

show nameif

Interface                   Name                        Security

Ethernet1/6                 INSIDE                        0

Ethernet1/7                 diagnostic                    0

Ethernet1/8                 OUTSIDE                       0

>
```

인터페이스 상태를 확인합니다.

```
<#root>

> show interface ip brief

Interface                  IP-Address      OK? Method Status                Protocol
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           unassigned      YES unset  up                    up
Internal-Data0/2           169.254.1.1     YES unset  up                    up

Ethernet1/6                unassigned      YES unset  up                    up

Ethernet1/7                unassigned      YES unset  up                    up

Ethernet1/8                unassigned      YES unset  up                    up
```

물리적 인터페이스 정보를 확인합니다.

```
<#root>

>

show interface e1/6

Interface Ethernet1/6 "INSIDE", is up, line protocol is up
```

```
  Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.770e, MTU 1500


IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1


        IP address unassigned
  Traffic Statistics for "INSIDE":
        468 packets input, 47627 bytes
        12 packets output, 4750 bytes
        1 packets dropped
      1 minute input rate 0 pkts/sec,  200 bytes/sec
      1 minute output rate 0 pkts/sec,  7 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  96 bytes/sec
      5 minute output rate 0 pkts/sec,  8 bytes/sec
      5 minute drop rate, 0 pkts/sec
>

show interface e1/8


Interface Ethernet1/8 "OUTSIDE", is up, line protocol is up


  Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.774d, MTU 1500


IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1


        IP address unassigned
  Traffic Statistics for "OUTSIDE":
        12 packets input, 4486 bytes
        470 packets output, 54089 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  7 bytes/sec
      1 minute output rate 0 pkts/sec,  212 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  7 bytes/sec
      5 minute output rate 0 pkts/sec,  106 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

FTD 인라인 쌍 인터페이스 작업 확인

이 섹션에서는 인라인 쌍 작업을 확인하기 위한 다음 확인 검사에 대해 설명합니다.

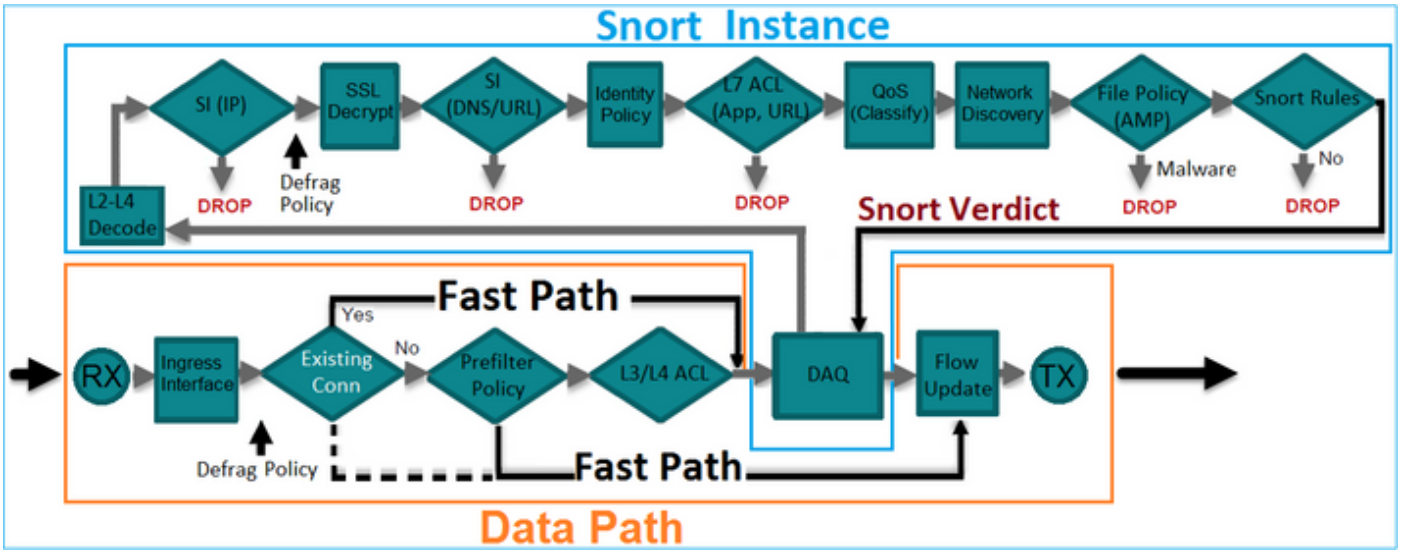
- 확인 1. Packet-tracer를 사용하여
- 확인 2. 추적을 사용하여 캡처를 활성화하고 인라인 쌍을 통해 TCP 동기화/승인(SYN/ACK)

패킷을 보냅니다.
- 확인 3. 방화벽 엔진 디버그를 사용하여 FTD 트래픽 모니터링
- 확인 4. 링크 상태 전파 기능 확인
- 확인 5. 고정 NAT(네트워크 주소 변환) 구성

솔루션

아키텍처 개요

FTD 인터페이스 2개가 인라인 쌍 모드에서 작동하는 경우 이미지에 표시된 대로 패킷이 처리됩니다.

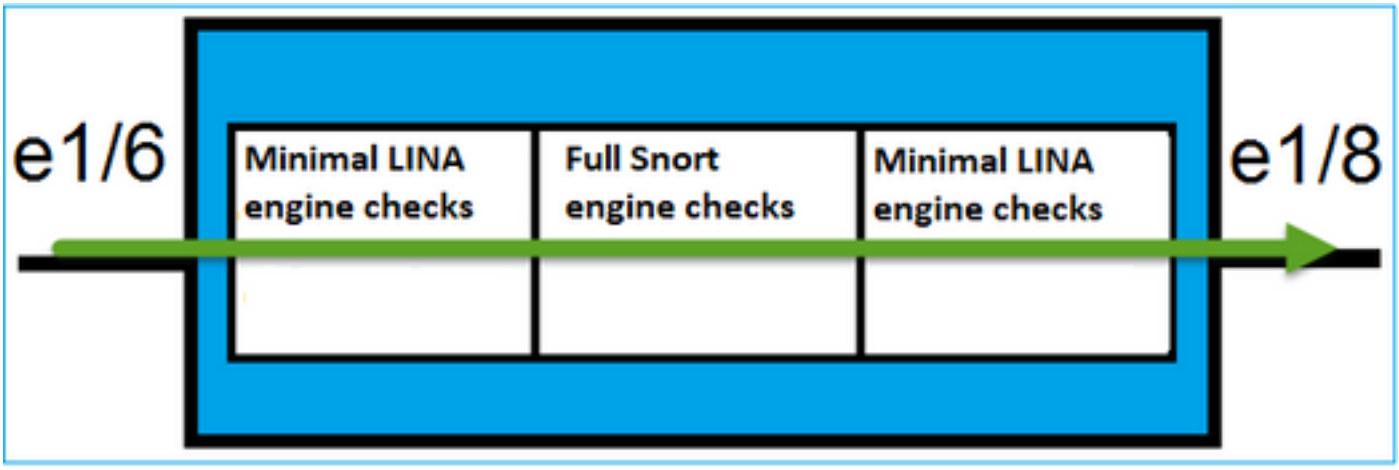


참고: 물리적 인터페이스만 인라인 쌍 집합의 멤버가 될 수 있습니다

기본 이론

- 인라인 쌍을 구성할 때 2 물리적 인터페이스는 내부적으로 브리지됩니다
- 기존 인라인 IPS(Intrusion Prevention System)와 매우 유사함
- 라우팅 또는 투명 구축 모드에서 사용 가능
- LINA 엔진 기능(NAT, 라우팅 등)의 대부분은 인라인 쌍을 통과하는 흐름에 사용할 수 없습니다
- 통과 트래픽을 삭제할 수 있음
- 전체 Snort 엔진 검사와 함께 몇 가지 LINA 엔진 검사가 적용됩니다

마지막 점은 그림과 같이 시각화할 수 있습니다.



확인 1. Packet-Tracer 사용 시

중요 포인트가 강조 표시된 상태로 인라인 쌍을 통과하는 패킷을 에뮬레이트하는 패킷 추적기 출력입니다.

<#root>

>

packet-tracer input INSIDE tcp 192.168.201.50 1111 192.168.202.50 80

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2

Type: NGIPS-MODE

Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services is be applied

Phase: 3

Type: ACCESS-LIST

Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet is sent to snort for additional processing where a verdict is reached

Phase: 4

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface
Result: ALLOW
Config:

Additional Information:

Ingress interface INSIDE is in NGIPS inline mode.

Egress interface OUTSIDE is determined by inline-set configuration

Phase: 5

Type: FLOW-CREATION

Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 106, packet dispatched to next module

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: allow

>

확인 2. 인라인 쌍을 통해 TCP SYN/ACK 패킷 전송

Scapy와 같은 유틸리티를 제공하는 패킷을 사용하여 TCP SYN/ACK 패킷을 생성할 수 있습니다. 이 구문은 SYN/ACK 플래그가 활성화된 3개의 패킷을 생성합니다.

```
<#root>

root@KALI:~#

scapy

INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>>

conf.iface='eth0'

>>>

packet = IP(dst="192.168.201.60")/TCP(flags="SA",dport=80)

>>>

syn_ack=[]

>>>

for i in range(0,3): # Send 3 packets

...

syn_ack.extend(packet)

...
>>>

send(syn_ack)
```

FTD CLI에서 이 캡처를 활성화하고 몇 가지 TCP SYN/ACK 패킷을 전송합니다.

```
<#root>

>

capture CAPI interface INSIDE trace match ip host 192.168.201.60 any


>

capture CAPO interface OUTSIDE match ip host 192.168.201.60 any


>
```

FTD를 통해 패킷을 전송한 후 생성된 연결을 볼 수 있습니다.

```
<#root>

>

show conn detail


1 in use, 34 most used
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,


 b - TCP state-bypass or nailed,


       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media,

N - inspected by Snort

, n - GUP
       O - responder data, P - inside back connection,
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow


TCP Inline-Pair-1:OUTSIDE(OUTSIDE): 192.168.201.60/80 Inline-Pair-1:INSIDE(INSIDE): 192.168.201.50/20,



flags b N

, idle 13s, uptime 13s, timeout 1h0m, bytes 0

>
```

참고: b 플래그 - TCP 상태 우회가 활성화되지 않은 경우 기존 ASA는 원치 않는 SYN/ACK 패킷을 삭제합니다. 인라인 쌍 모드의 FTD 인터페이스는 TCP 상태 우회 모드에서 TCP 연결을 처리하며, 이미 존재하는 연결에 속하지 않는 TCP 패킷을 삭제하지 않습니다.

참고: N 플래그 - FTD Snort 엔진에서 패킷을 검사합니다.

에서는 FTD를 통과하는 3개의 패킷을 확인할 수 있으므로 이를 입증합니다.

<#root>

>

show capture CAPI

3 packets captured

   1: 15:27:54.327146   192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
   2: 15:27:54.330000   192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
   3: 15:27:54.332517   192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
3 packets shown
>

3 패킷은 FTD 디바이스를 종료합니다.

<#root>

>

show capture CAPO

3 packets captured

   1: 15:27:54.327299   192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

```
 0 win 8192
   2: 15:27:54.330030       192.168.201.50.20 > 192.168.201.60.80:
S
 0:0(0)
ack
 0 win 8192
   3: 15:27:54.332548       192.168.201.50.20 > 192.168.201.60.80:
S
 0:0(0)
ack
 0 win 8192
3 packets shown
>
```

첫 번째 캡처 패킷의 Trace(추적)를 사용하면 Snort 엔진 판정과 같은 몇 가지 추가 정보가 표시됩니다.

```
<#root>
>
show capture CAPI packet-number 1 trace

3 packets captured

   1: 15:27:54.327146       192.168.201.50.20 > 192.168.201.60.80:
S
 0:0(0)
ack
 0 win 8192
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services is applied

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: DEFAULT ACTION RULE

Additional Information:
This packet is sent to snort for additional processing where a verdict is reached

Phase: 5
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface

Result: ALLOW
Config:
Additional Information:

Ingress interface INSIDE is in NGIPS inline mode.
Egress interface OUTSIDE is determined by inline-set configuration

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 282, packet dispatched to next module

Phase: 7
Type: EXTERNAL-INSPECT

Subtype:
Result: ALLOW
Config:
Additional Information:

Application: 'SNORT Inspect'

Phase: 8
Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:
Snort Verdict: (pass-packet) allow this packet

```
Phase: 9
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
Action: allow


1 packet shown
>
```

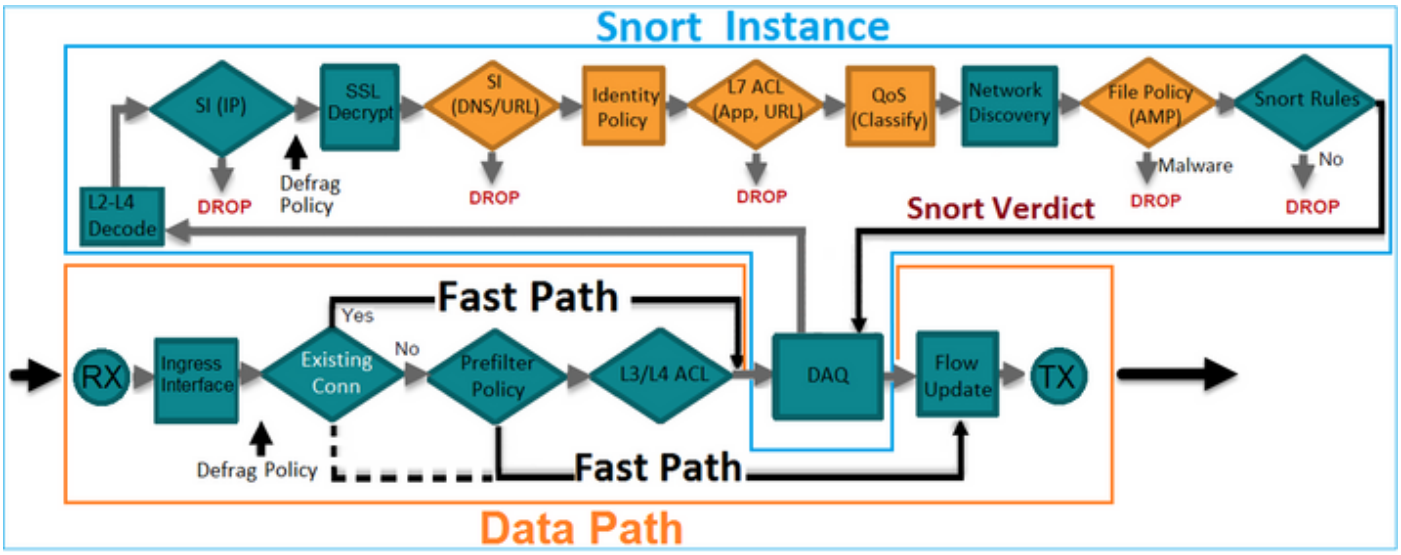
두 번째 캡처된 패킷의 Trace(추적)를 사용하면 패킷이 현재 연결과 일치하므로 ACL 검사를 우회하지만 Snort 엔진에서 계속 검사됨을 알 수 있습니다.

```
<#root>

>

show capture CAPI packet-number 2 trace


3 packets captured

   2: 15:27:54.330000       192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 3
Type: FLOW-LOOKUP
Subtype:ing
Result: ALLOW
Config:
Additional Information:
Found flow with id 282, using current flow


Phase: 4
Type: EXTERNAL-INSPECT

Subtype:
Result: ALLOW
Config:

Additional Information:
Application: 'SNORT Inspect'


Phase: 5
Type: SNORT

Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet


Phase: 6
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
Action: allow


1 packet shown
>
```

확인 3. 허용되는 트래픽에 대한 방화벽 엔진 디버그

방화벽 엔진 디버그는 그림에 표시된 액세스 제어 정책과 같은 FTD Snort 엔진의 특정 구성 요소에 대해 실행됩니다.



Inline Pair를 통해 TCP SYN/ACK 패킷을 전송할 때 디버그 출력에서 확인할 수 있습니다.

<#root>

>

system support firewall-engine-debug

Please specify an IP protocol:

tcp

Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:

192.168.201.60

Please specify a server port:

80

Monitoring firewall engine debug messages

192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 New session

192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 using HW or preset rule order 3, id 268438528 action A

192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 allow action

192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 Deleting session

확인 4. 링크 상태 전파 확인

FTD에서 버퍼 로그를 활성화하고 e1/6 인터페이스에 연결된 switchport를 종료합니다. FTD CLI에서 두 인터페이스가 모두 다운되었음을 확인해야 합니다.

```
<#root>

>

show interface ip brief


Interface                  IP-Address      OK? Method Status                Protocol
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           unassigned      YES unset  up                    up
Internal-Data0/2           169.254.1.1     YES unset  up                    up

Ethernet1/6                unassigned      YES unset  down                  down


Ethernet1/7                unassigned      YES unset  up                    up

Ethernet1/8                unassigned      YES unset  administratively down up


>
```

FTD 로그에는 다음이 표시됩니다.

```
<#root>

>

show log


Jan 03 2017 15:53:19: %ASA-4-411002:

Line protocol on Interface Ethernet1/6, changed state to down


Jan 03 2017 15:53:19: %ASA-4-411004:

Interface OUTSIDE, changed state to administratively down


Jan 03 2017 15:53:19: %ASA-4-411004:

Interface Ethernet1/8, changed state to administratively down


Jan 03 2017 15:53:19: %ASA-4-812005:

Link-State-Propagation activated on inline-pair due to failure of interface Ethernet1/6(INSIDE) bringing

>
```

inline-set 상태는 2개 인터페이스 멤버의 상태를 표시합니다.

```
<#root>

>

show inline-set



Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Failsafe mode is on/activated
  Failsecure mode is off
  Tap mode is off

 Propagate-link-state option is on


  hardware-bypass mode is disabled

Interface-Pair[1]:


    Interface: Ethernet1/6 "INSIDE"


      Current-Status: Down(Propagate-Link-State-Activated)


    Interface: Ethernet1/8 "OUTSIDE"


      Current-Status: Down(Down-By-Propagate-Link-State)

    Bridge Group ID: 509
>
```

2개 인터페이스의 상태 차이를 확인합니다.

```
<#root>

>

show interface e1/6



Interface Ethernet1/6 "INSIDE", is down, line protocol is down


  Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.770e, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1
```

```
  Propagate-Link-State-Activated


        IP address unassigned
  Traffic Statistics for "INSIDE":
        3393 packets input, 234923 bytes
        120 packets output, 49174 bytes
        1 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  6 bytes/sec
      5 minute output rate 0 pkts/sec,  3 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

Ethernet1/8 인터페이스의 경우:

```
<#root>

>

show interface e1/8


Interface Ethernet1/8 "OUTSIDE", is administratively down, line protocol is up


  Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.774d, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1


Down-By-Propagate-Link-State


        IP address unassigned
  Traffic Statistics for "OUTSIDE":
        120 packets input, 46664 bytes
        3391 packets output, 298455 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  3 bytes/sec
      5 minute output rate 0 pkts/sec,  8 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

switchport를 다시 활성화하면 FTD 로그에 다음이 표시됩니다.

```
<#root>

>
```

```
show log

...
Jan 03 2017 15:59:35: %ASA-4-411001:
Line protocol on Interface Ethernet1/6, changed state to up

Jan 03 2017 15:59:35: %ASA-4-411003:
Interface Ethernet1/8, changed state to administratively up

Jan 03 2017 15:59:35: %ASA-4-411003:
Interface OUTSIDE, changed state to administratively up

Jan 03 2017 15:59:35: %ASA-4-812006:
Link-State-Propagation de-activated on inline-pair due to recovery of interface Ethernet1/6(INSIDE) brir

>
```

확인 5. 고정 NAT 구성

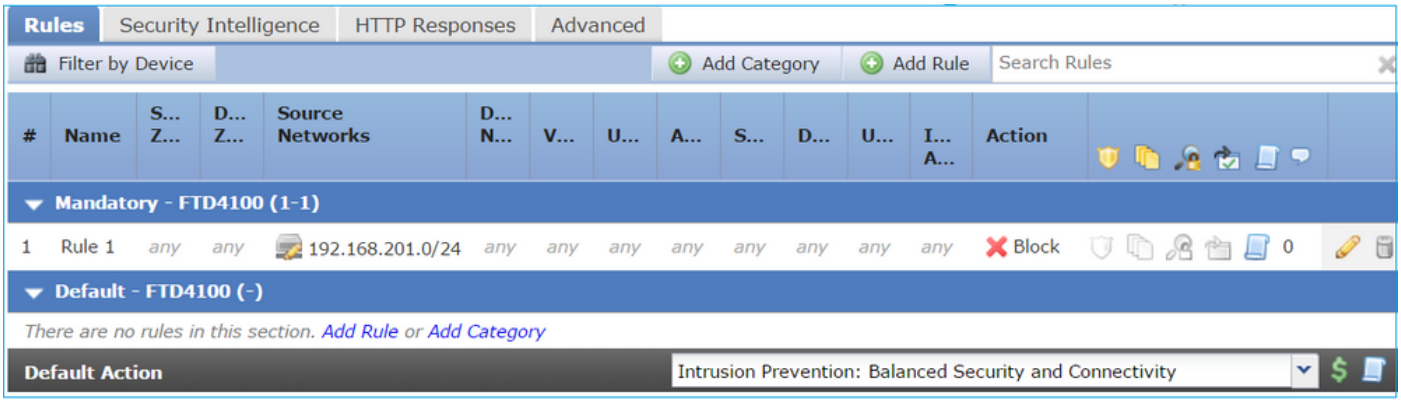
솔루션

인라인, 인라인 탭 또는 패시브 모드에서 작동하는 인터페이스에는 NAT가 지원되지 않습니다.

https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Network_Address_Translation__NAT__for_Threat_Defense.html

인라인 쌍 인터페이스 모드에서 패킷 차단

Block 규칙을 생성하고, FTD 인라인 쌍을 통해 트래픽을 전송하고, 이미지에 표시된 것처럼 동작을 관찰합니다.



솔루션

추적을 통한 캡처를 활성화하고 FTD 인라인 쌍을 통해 SYN/ACK 패킷을 전송합니다. 트래픽이 차

단됩니다.

<#root>

>

show capture

capture CAPI type raw-data trace interface INSIDE

[Capturing - 210 bytes]

  match ip host 192.168.201.60 any
capture CAPO type raw-data interface OUTSIDE

[Capturing - 0 bytes]

  match ip host 192.168.201.60 any

추적하면 패킷이 다음과 같이 표시됩니다.

<#root>

>

show capture CAPI packet-number 1 trace

3 packets captured

   1: 16:12:55.785085

192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3

Type: NGIPS-MODE

Subtype: ngips-mode

Result: ALLOW
Config:

Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services is applied

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: DROP

Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log fl
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD4100 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Rule 1

Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up

Action: drop

Drop-reason: (acl-drop) Flow is denied by configured rule

1 packet shown

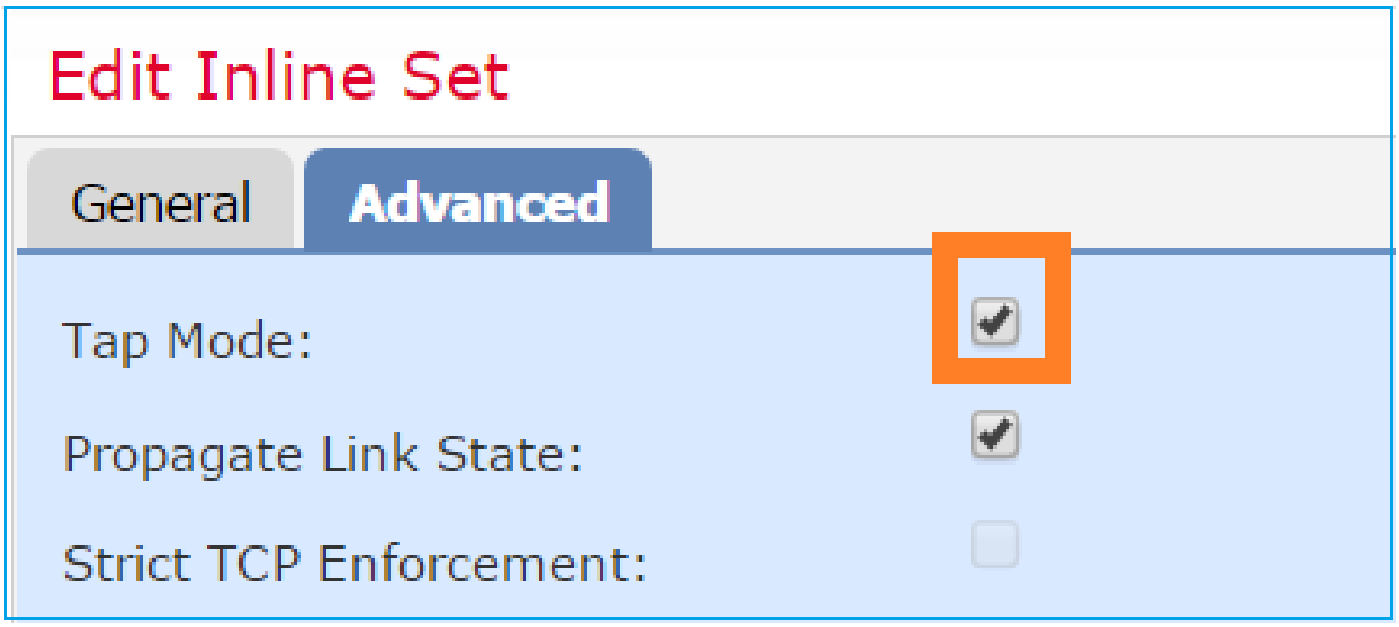
이 추적에서는 패킷이 FTD LINA 엔진에 의해 삭제되었고 FTD Snort 엔진에 전달되지 않았음을 알 수 있습니다.

Tap를 사용하여 인라인 쌍 모드 구성

인라인 쌍에서 탭 모드를 활성화합니다.

솔루션

이미지에 표시된 대로 Devices > Device Management > Inline Sets > Edit Inline Set > Advanced로 이동하여 Tap Mode를 활성화합니다.



확인

<#root>

>

show inline-set

```
Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Failsafe mode is on/activated
  Failsecure mode is off
```

Tap mode is on

```
  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/6 "INSIDE"
      Current-Status: UP
    Interface: Ethernet1/8 "OUTSIDE"
```

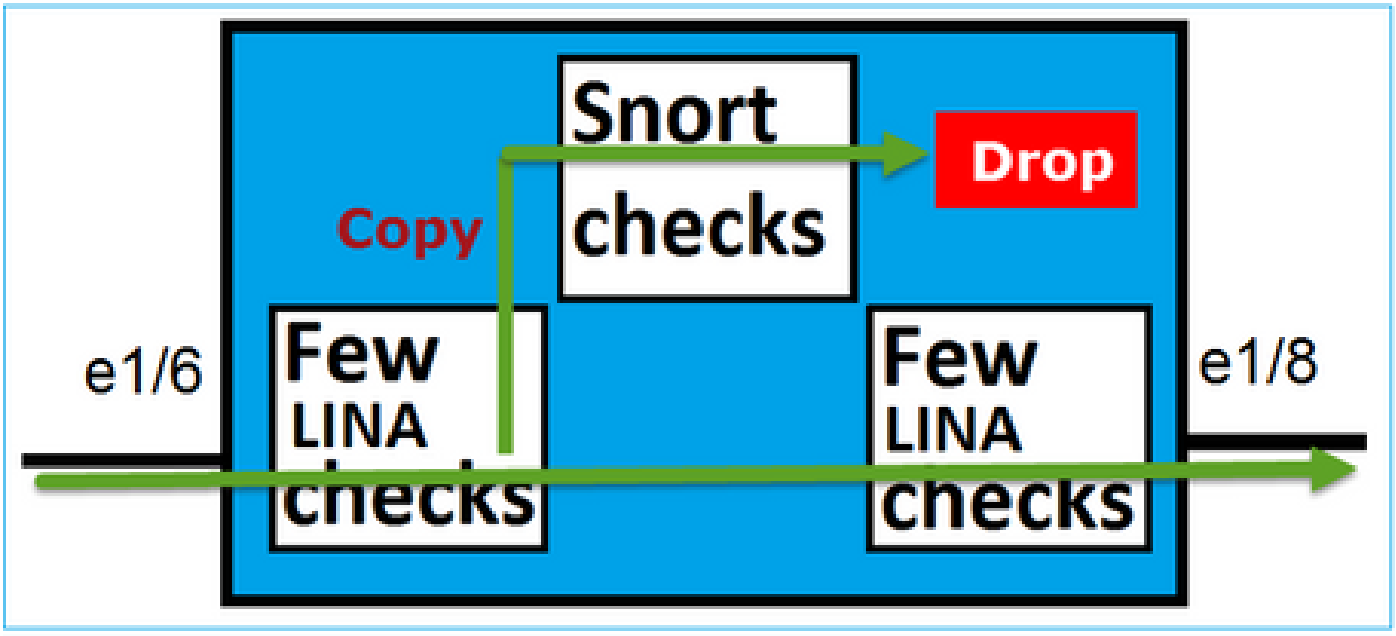
```
      Current-Status: UP
    Bridge Group ID: 0
>
```

탭 인터페이스 작업으로 FTD 인라인 쌍 확인

기본 이론

- Inline Pair with Tap 2를 구성하면 물리적 인터페이스가 내부적으로 브리징됩니다
- 라우팅 또는 투명 구축 모드에서 사용할 수 있습니다
- LINA 엔진 기능(NAT, 라우팅 등)의 대부분은 인라인 쌍을 통과하는 흐름에 사용할 수 없습니다
- 실제 트래픽은 삭제할 수 없습니다.
- 실제 트래픽의 복사본에 대한 전체 Snort 엔진 검사와 함께 몇 가지 LINA 엔진 검사가 적용됩니다

마지막 점은 그림과 같습니다.



Inline Pair with Tap Mode(탭 모드의 인라인 쌍)는 트랜짓 트래픽을 삭제하지 않습니다. 패킷 추적을 통해 다음을 확인합니다.

<#root>

>

show capture CAPI packet-number 2 trace

```
3 packets captured
```

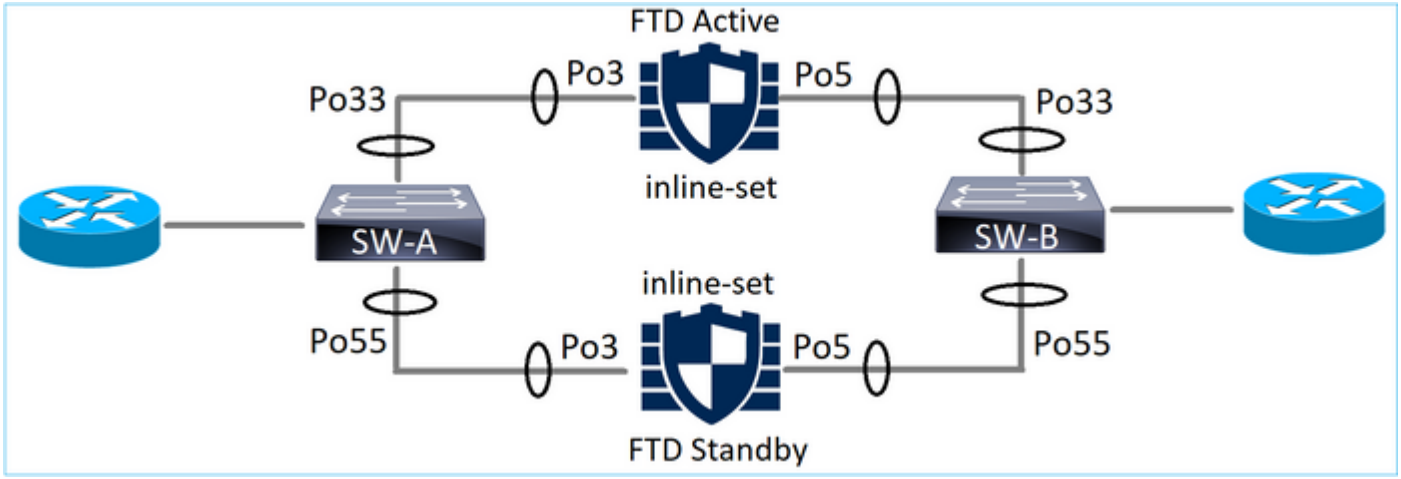
```
   2: 13:34:30.685084       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) win 8192
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list


Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode

Result: ALLOW
Config:
Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services is applied



Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: WOULD HAVE DROPPED

Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log fl
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD4100 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Rule 1
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up

Action: Access-list would have dropped, but packet forwarded due to inline-tap


1 packet shown
>
```

인라인 쌍 및 Etherchannel

다음 2가지 방법으로 etherchannel과 인라인 쌍을 구성할 수 있습니다.

1. Etherchannel이 FTD에서 종료됨
2. Etherchannel은 FTD를 거칩니다(FXOS 코드 2.3.1.3 이상 필요).

Etherchannel이 FTD에서 종료됨



SW-A의 Etherchannel:

<#root>

SW-A#

show etherchannel summary | i Po33|Po55

```
33     Po33(SU)         LACP      Gi3/11(P)
35     Po35(SU)         LACP      Gi2/33(P)
```

SW-B의 Etherchannel:

<#root>

SW-B#

show etherchannel summary | i Po33|Po55

```
33     Po33(SU)         LACP        Gi1/0/3(P)
55     Po55(SU)         LACP        Gi1/0/4(P)
```

트래픽은 MAC 주소 학습을 기반으로 활성 FTD를 통해 전달됩니다.

<#root>

```
SW-B#
 show mac address-table address 0017.dfd6.ec00

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0017.dfd6.ec00    DYNAMIC
Po33

Total Mac Addresses for this criterion: 1
```

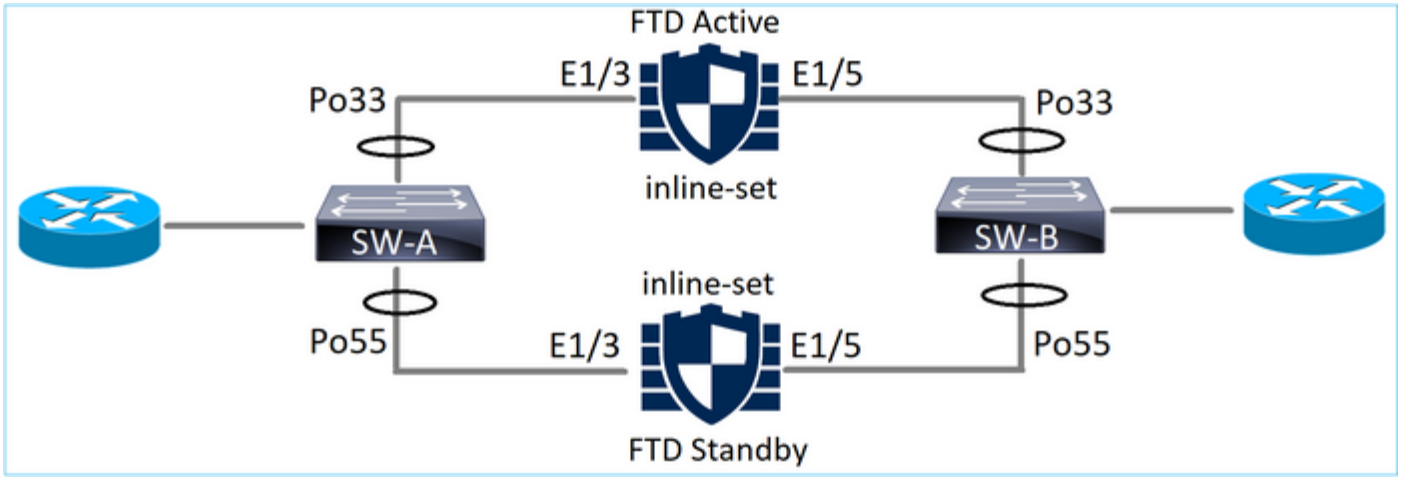
FTD의 인라인 집합:

<#root>

```
FTD#
show inline-set


Inline-set SET1
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled


Interface-Pair[1]:
    Interface: Port-channel3 "INSIDE"
      Current-Status: UP
    Interface: Port-channel5 "OUTSIDE"
      Current-Status: UP

    Bridge Group ID: 775
```

참고: FTD 장애 조치 이벤트의 경우 트래픽 중단은 주로 원격 피어의 MAC 주소를 학습하는 데 스위치에서 걸리는 시간에 따라 달라집니다.

FTD를 통한 Etherchannel



SW-A의 Etherchannel:

<#root>

SW-A#

show etherchannel summary | i Po33|Po55

33 Po33(SU) LACP Gi3/11(P)
55 Po55(SD) LACP Gi3/7

(I)

대기 FTD를 통한 LACP 패킷은 차단됩니다.

<#root>

FTD#

capture ASP type asp-drop fo-standby

FTD#

show capture ASP | i 0180.c200.0002

29: 15:28:32.658123 a0f8.4991.ba03 0180.c200.0002 0x8809 Length: 124
70: 15:28:47.248262 f0f7.556a.11e2 0180.c200.0002 0x8809 Length: 124

SW-B의 Etherchannel:

<#root>

SW-B#

show etherchannel summary | i Po33|Po55

33 Po33(SU) LACP Gi1/0/3(P)

```
55     Po55(SD)        LACP        Gi1/0/4
(s)
```

트래픽은 MAC 주소 학습을 기반으로 활성 FTD를 통해 전달됩니다.

<#root>

```
SW-B#
 show mac address-table address 0017.dfd6.ec00

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0017.dfd6.ec00    DYNAMIC
Po33

Total Mac Addresses for this criterion: 1
```

FTD의 인라인 집합:

<#root>

```
FTD#
show inline-set


Inline-set SET1
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled

Interface-Pair[1]:

    Interface: Ethernet1/3 "INSIDE"

      Current-Status: UP

    Interface: Ethernet1/5 "OUTSIDE"
```

```
    Current-Status: UP

  Bridge Group ID: 519
```

⚠ 주의: 이 시나리오에서 FTD 장애 조치 이벤트의 경우 컨버전스 시간은 주로 Etherchannel LACP 협상에 따라 다르며, 중단 시간이 훨씬 더 길 수 있습니다. Etherchannel 모드가 ON(LACP 없음)인 경우 컨버전스 시간은 MAC 주소 학습에 따라 달라집니다.

문제 해결

현재 이 구성에 사용할 수 있는 특정 정보가 없습니다.

비교: Inline Pair vs Inline Pair with Tap

	인라인 쌍	Tap가 있는 인라인 쌍

인라인 집합 표시	> 인라인 집합 표시
	
	인라인 집합 Inline-Pair-1
	  Mtu는 1500바이트입니다.
	  Failsafe 모드가 설정/활성화됨
	  장애 조치(Failsecure) 모드가 해제됨
	  탭 모드가 꺼져 있습니다.
	  Propagate-link-state 옵션이 켜짐
	  하드웨어 바이패스 모드가 비활성화되었습니다.
	  인터페이스 쌍[1]:
	  인터페이스: Ethernet1/6 "INSIDE"
	  현재 상태: 작동
	  인터페이스: Ethernet1/8 "OUTSIDE"
	  현재 상태: 작동
	  브리지 그룹 ID: 509
	>
		> 인라인 집합 표시
		
		인라인 집합 Inline-Pair-1
		  Mtu는 1500바이트입니다.
		  Failsafe 모드가 설정/활성화됨
		  장애 조치(Failsecure) 모드가 해제됨
		  탭 모드가 켜져 있습니다.
		  Propagate-link-state 옵션이 켜짐
		  하드웨어 바이패스 모드가 비활성화되었습니다.
		  인터페이스 쌍[1]:
		  인터페이스: Ethernet1/6 "INSIDE"
		  현재 상태: 작동
		  인터페이스: Ethernet1/8 "OUTSIDE"
		  현재 상태: 작동
		  브리지 그룹 ID: 0
		
		>

인터페이스 표시	> show interface e1/6
	Interface Ethernet1/6 "INSIDE", 작동 중, 회선 프로토콜 작동 중
	  하드웨어는 EtherSVI, BW 1000Mbps,
		> show interface e1/6
		Interface Ethernet1/6 "INSIDE", 작동 중, 회선 프로토콜 작동 중
		  하드웨어는 EtherSVI, BW 1000Mbps,

	DLY 1000usec MAC 주소 5897.bdb9.770e, MTU 1500 IPS 인터페이스 모드: 인라인, 인라인 집합: 인라인-쌍-1 할당되지 않은 IP 주소 "내부"에 대한 트래픽 통계: 3957 패킷 입력, 264913바이트 144 패킷 출력, 58664바이트 4개 패킷 삭제 1분 입력 속도 0 pkts/초, 26바이트/초 1분 출력 속도 0 pkts/초, 7바이트/초 1분 삭제 속도, 0pkts/초 5분 입력 속도 0 pkts/초, 28바이트/초 5분 출력 속도 0 pkts/초, 9바이트/초 5분 삭제 속도, 0pkts/초 > show interface e1/8 Interface Ethernet1/8 "OUTSIDE", 작동 중, 회선 프로토콜 작동 중 하드웨어는 EtherSVI, BW 1000Mbps, DLY 1000usec MAC 주소 5897.bdb9.774d, MTU 1500 IPS 인터페이스 모드: 인라인, 인라인 집합: 인라인-쌍-1 할당되지 않은 IP 주소 "외부"에 대한 트래픽 통계: 144개 패킷 입력, 55634바이트 3954 패킷 출력, 339987바이트 0개 패킷 삭제 1분 입력 속도 0 pkts/초, 7바이트/초 1분 출력 속도 0 pkts/초, 37바이트/초 1분 삭제 속도, 0pkts/초 5분 입력 속도 0 pkts/초, 8바이트/초 5분 출력 속도 0 pkts/초, 39바이트/초 5분 삭제 속도, 0pkts/초 >	DLY 1000usec MAC 주소 5897.bdb9.770e, MTU 1500 IPS Interface-Mode: inline-tap, Inline-Set: Inline-Pair-1 할당되지 않은 IP 주소 "내부"에 대한 트래픽 통계: 24개 패킷 입력, 1378바이트 0 패킷 출력, 0 바이트 24개 패킷 삭제 1분 입력 속도 0 pkts/초, 0 바이트/초 1분 출력 속도 0 pkts/초, 0 bytes/초 1분 삭제 속도, 0pkts/초 5분 입력 속도 0 pkts/초, 0 bytes/초 5분 출력 속도 0 pkts/초, 0 bytes/초 5분 삭제 속도, 0pkts/초 > show interface e1/8 Interface Ethernet1/8 "OUTSIDE", 작동 중, 회선 프로토콜 작동 중 하드웨어는 EtherSVI, BW 1000Mbps, DLY 1000usec MAC 주소 5897.bdb9.774d, MTU 1500 IPS Interface-Mode: inline-tap, Inline-Set: Inline-Pair-1 할당되지 않은 IP 주소 "외부"에 대한 트래픽 통계: 1 패킷 입력, 441바이트 0 패킷 출력, 0 바이트 삭제된 패킷 1개 1분 입력 속도 0 pkts/초, 0 바이트/초 1분 출력 속도 0 pkts/초, 0 bytes/초 1분 삭제 속도, 0pkts/초 5분 입력 속도 0 pkts/초, 0 bytes/초 5분 출력 속도 0 pkts/초, 0 bytes/초 5분 삭제 속도, 0pkts/초 >
블록 규칙으로 패킷 처리하기	> show capture CAPI packet-number 1 trace 캡처된 패킷 3개 1: 16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win	> show capture CAPI packet-number 1 trace 캡처된 패킷 3개 1: 16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) win 8192

	8192 단계: 1 유형: CAPTURE 하위 유형: 결과: 허용 설정: 추가 정보: MAC 액세스 목록 단계: 2 유형: 액세스 목록 하위 유형: 결과: 허용 설정: 암시적 규칙 추가 정보: MAC 액세스 목록 단계: 3 유형: NGIPS-MODE 하위 유형: ngips-mode 결과: 허용 설정: 추가 정보: 흐름은 NGIPS 모드 및 NGIPS 서비스에 대해 구성된 인터페이스를 적용했습니다 단계: 4 유형: 액세스 목록 하위 유형: 로그 결과: DROP 설정: 액세스 그룹 CSM_FW_ACL_ 전역 access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log flow-start access-list CSM_FW_ACL_ remark rule-id 268441600: 액세스 정책: FTD4100 - 필수/1 access-list CSM_FW_ACL_ remark rule-id 268441600: L4 규칙: 규칙 1 추가 정보: 결과: 입력 인터페이스: 내부	단계: 1 유형: CAPTURE 하위 유형: 결과: 허용 설정: 추가 정보: MAC 액세스 목록 단계: 2 유형: 액세스 목록 하위 유형: 결과: 허용 설정: 암시적 규칙 추가 정보: MAC 액세스 목록 단계: 3 유형: NGIPS-MODE 하위 유형: ngips-mode 결과: 허용 설정: 추가 정보: 흐름은 NGIPS 모드 및 NGIPS 서비스에 대해 구성된 인터페이스를 적용했습니다 단계: 4 유형: 액세스 목록 하위 유형: 로그 결과: 삭제되었을 가능성 설정: 액세스 그룹 CSM_FW_ACL_ 전역 access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log flow-start access-list CSM_FW_ACL_ remark rule-id 268441600: 액세스 정책: FTD4100 - 필수/1 access-list CSM_FW_ACL_ remark rule-id 268441600: L4 규칙: 규칙 1 추가 정보: 결과: 입력 인터페이스: 내부 입력 상태: up

	입력 상태: up 입력 라인 상태: up 작업: 삭제 삭제 사유: 구성된 규칙에 의해 (acl-drop) 흐름이 거부됨 1개 패킷 표시 >	입력 라인 상태: up 작업: Access-list는 삭제되었지만 인라인 탭으로 인해 패킷이 전달되었습니다. 1개 패킷 표시 >

요약

- Inline Pair 모드를 사용할 경우 패킷은 주로 FTD Snort 엔진을 거칩니다
- TCP 연결은 TCP 상태 바이패스 모드에서 처리됩니다
- FTD LINA 엔진 관점에서 ACL 정책이 적용됩니다
- Inline Pair Mode(인라인 쌍 모드)가 사용 중인 경우 패킷이 인라인으로 처리되므로 패킷을 차단할 수 있습니다
- Tap Mode(탭 모드)가 활성화되면 실제 트래픽이 수정되지 않은 FTD를 통과하는 동안 패킷의 사본이 검사되고 내부에 삭제됩니다

관련 정보

- Cisco Firepower NGFW
- 기술 지원 및 문서 – Cisco Systems

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.