인라인 페어 모드에서 Firepower Threat Defense 인터페이스 구성

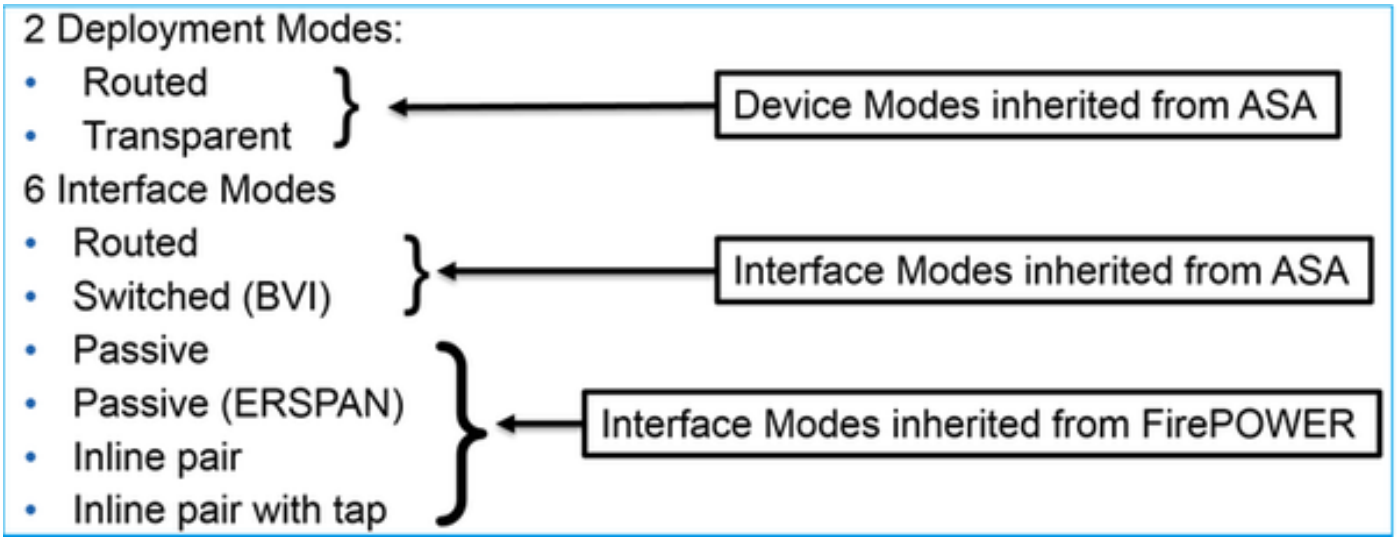
목차

소개

FTD(Firepower Threat Defense)는 다음 플랫폼에 설치할 수 있는 통합 소프트웨어 이미지입니다.

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR4100, FPR9300
- VMware(ESXi)
- AWS(Amazon Web Services)
- KVM
- ISR 라우터 모듈

FTD는 2개의 구축 모드와 6개의 인터페이스 모드를 제공합니다.



참고: 단일 FTD 어플라이언스에서 여러 인터페이스 모드를 함께 사용할 수 있습니다.

다음 표에는 다양한 FTD 구축 및 인터페이스 모드가 간략하게 요약되어 있습니다.

FTD 인터페이스 모드	FTD 구축 모드	설명	트래픽 삭제 가능 여부
라우팅 모드	라우팅 모드	전체 ASA 엔진 및 Snort 엔진 검사	예
전환됨	투명 모드	전체 ASA 엔진 및 Snort 엔진 검사	예
인라인 페어	라우팅 또는 투명 모드	부분 ASA 엔진 및 전체 Snort 엔진 검사	예
인라인 페어(탭 포함)	라우팅 또는 투명 모드	부분 ASA 엔진 및 전체 Snort 엔진 검사	아니요
수동	라우팅 또는 투명 모드	부분 ASA 엔진 및 전체 Snort 엔진 검사	아니요
수동(ERSPAN)	라우팅 모드	부분 ASA 엔진 및 전체 Snort 엔진 검사	아니요

목표

이 문서의 목표는 다음과 같습니다.

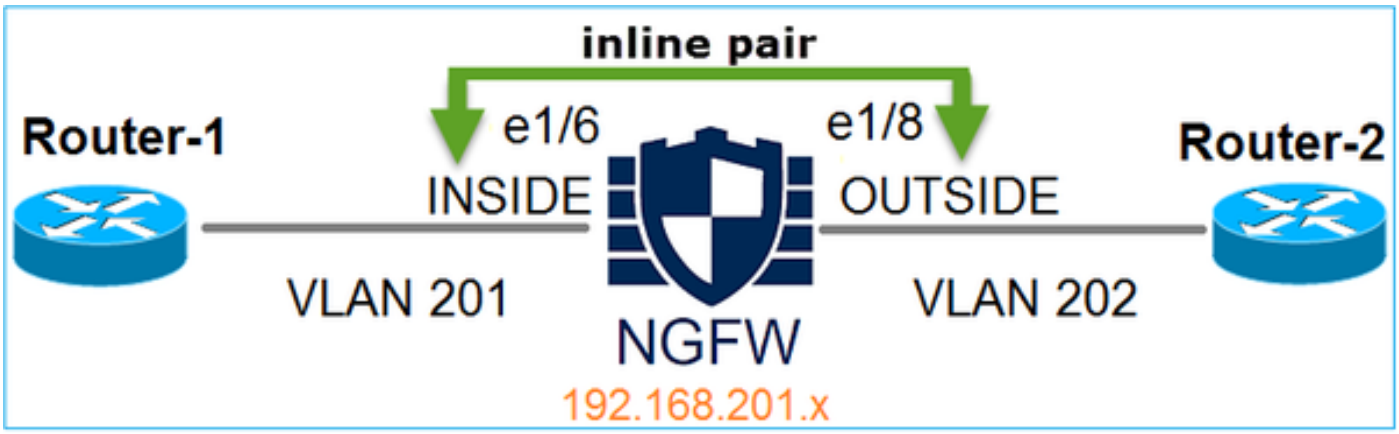
- FTD 인라인 페어 인터페이스의 컨피그레이션 및 작업 방식 제시

사용되는 구성 요소

- FTD 코드 6.1.0.x를 실행하는 Firepower 4150

- 6.1.0.x를 실행하는 FMC(Firepower Management Center)

토폴로지



FTD에서 인라인 페어 인터페이스 구성

요건

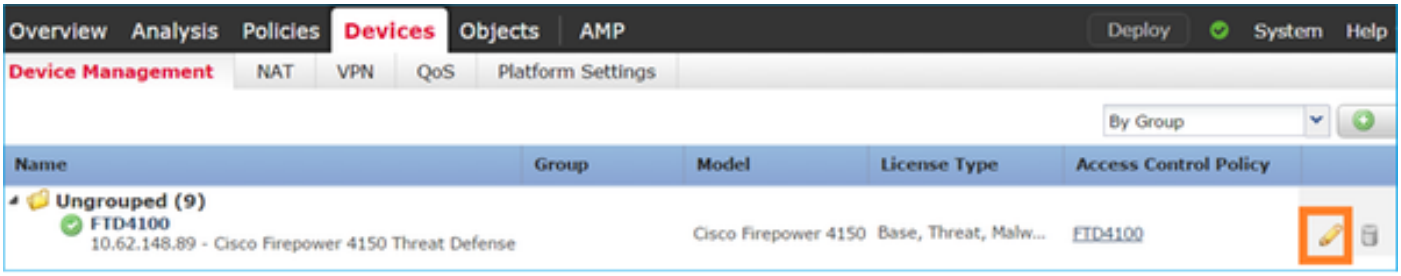
다음 요건에 따라 인라인 페어 모드에서 물리적 인터페이스 e1/6 및 e1/8을 구성합니다.

인터페이스	e1/6	e1/8
이름	내부	외부
Security Zone	INSIDE_ZONE	OUTSIDE_ZONE
인라인 세트 이름	Inline-Pair-1	
인라인 세트 MTU	1500	
페일세이프	활성화됨	
링크 상태 전파	활성화됨	

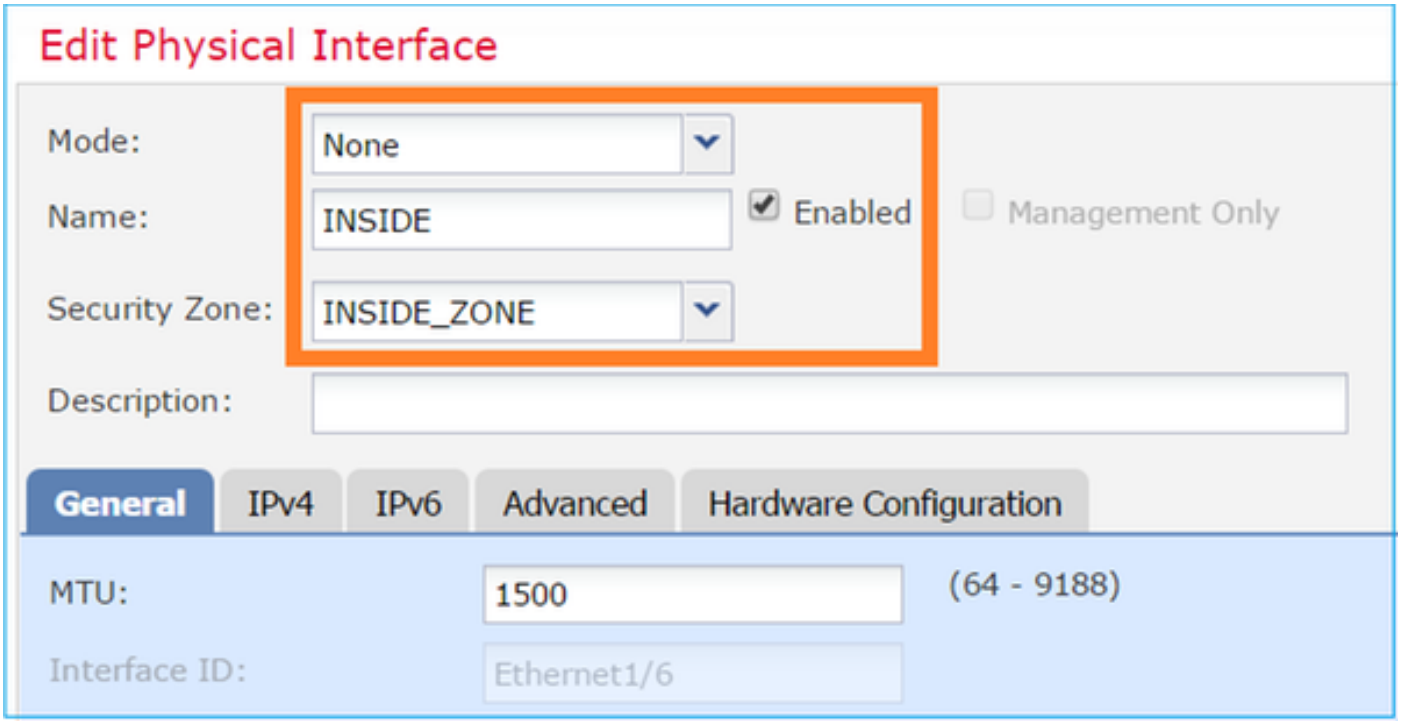
해결책

1단계 - 개별 인터페이스 구성

Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 적절한 디바이스를 선택하고 **Edit(수정)** 아이콘을 클릭합니다.

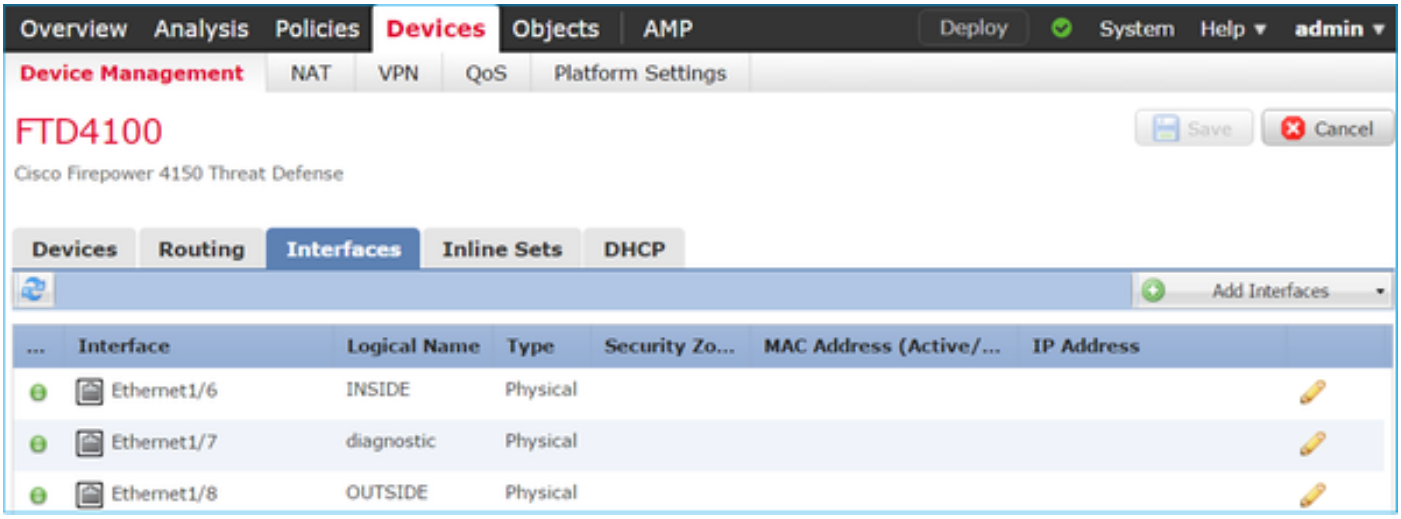


인터페이스의 이름을 지정하고 인터페이스를 활성화합니다.



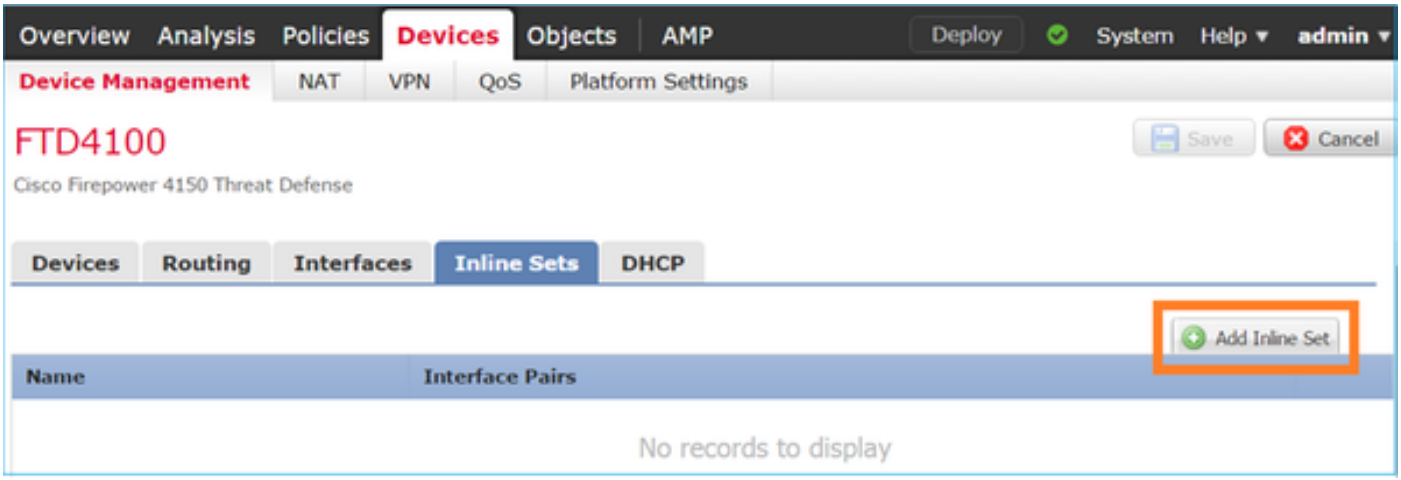
Name(이름)은 인터페이스의 **nameif**가 됩니다.

인터페이스 Ethernet1/8의 경우에도 마찬가지입니다. 최종 결과는 다음 그림과 같습니다.

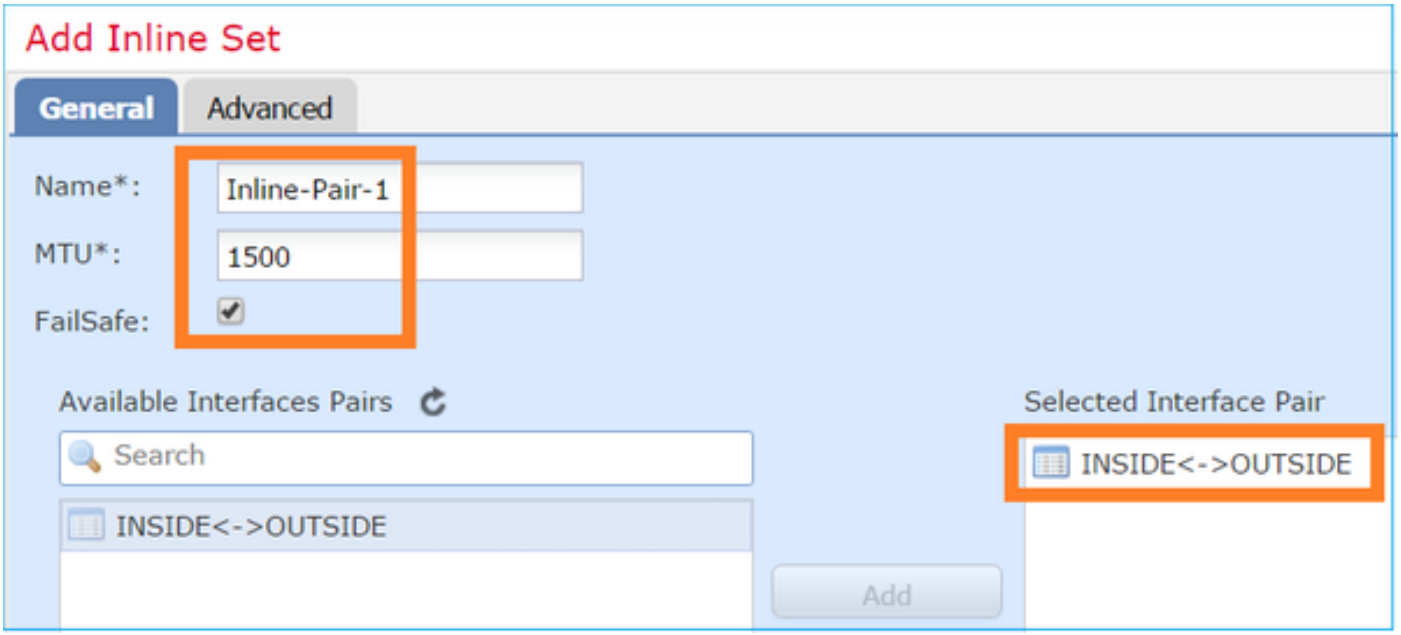


2단계 - 인라인 페어 구성

Inline Sets(인라인 세트) 탭으로 이동하여 **Add Inline Set(인라인 세트 추가)**를 클릭합니다.

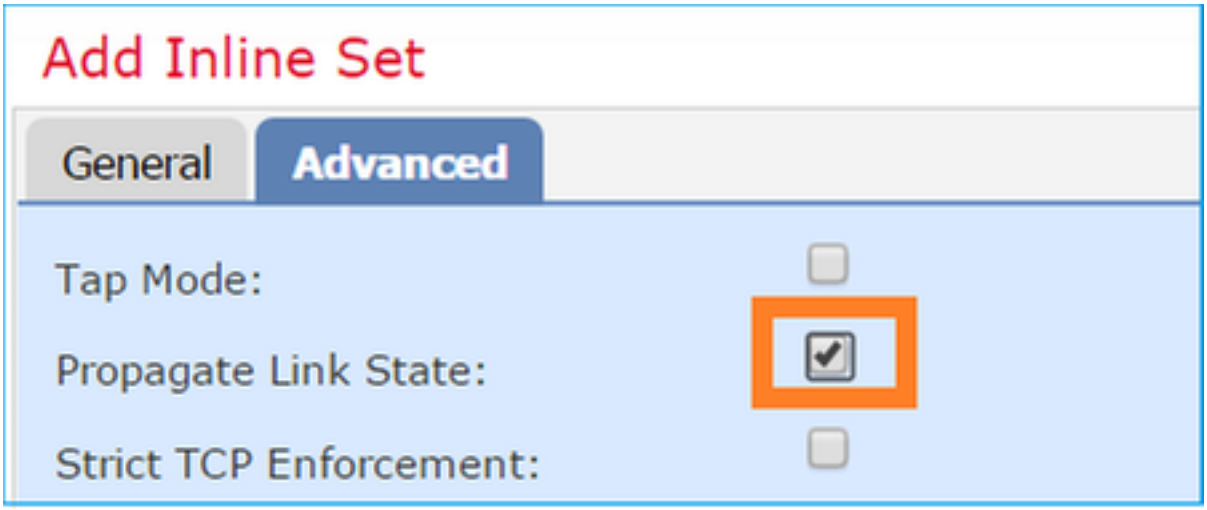


요건에 따라 설정을 구성합니다.



Failsafe(페일세이프)를 선택하면 인터페이스 버퍼가 가득 차는 경우 트래픽이 검사 없이 인라인 페어를 통과할 수 있습니다. 일반적으로는 디바이스나 Snort 엔진이 오버로드되면 인터페이스 버퍼가 가득 차는 현상이 나타납니다. 인터페이스 버퍼 크기는 동적으로 할당됩니다.

'**Propagate Link State(링크 상태 전파)**' 옵션을 활성화합니다.



링크 상태 전파는 인라인 세트의 인터페이스 중 하나가 다운될 때 인라인 인터페이스 페어에서 두 번째 인터페이스를 자동으로 불러옵니다.

변경 사항을 **Save(저장)**하고 **Deploy(구축)**합니다.

인라인 페어 인터페이스 컨피그레이션 확인

FTD CLI에서 인라인 페어 컨피그레이션을 확인합니다.

해결책

FTD CLI에 로그인하여 인라인 페어 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 0이 아닌 값입니다. 탭 모드의 경우에는 ID가 0입니다.

인터페이스 및 이름 정보:

```
> show nameif
Interface               Name                    Security
Ethernet1/6             INSIDE                  0
Ethernet1/7             diagnostic              0
Ethernet1/8             OUTSIDE                 0
>
```

인터페이스 상태 확인:

```
> 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 정보 확인:

```
> 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 페어 인터페이스 작업 확인

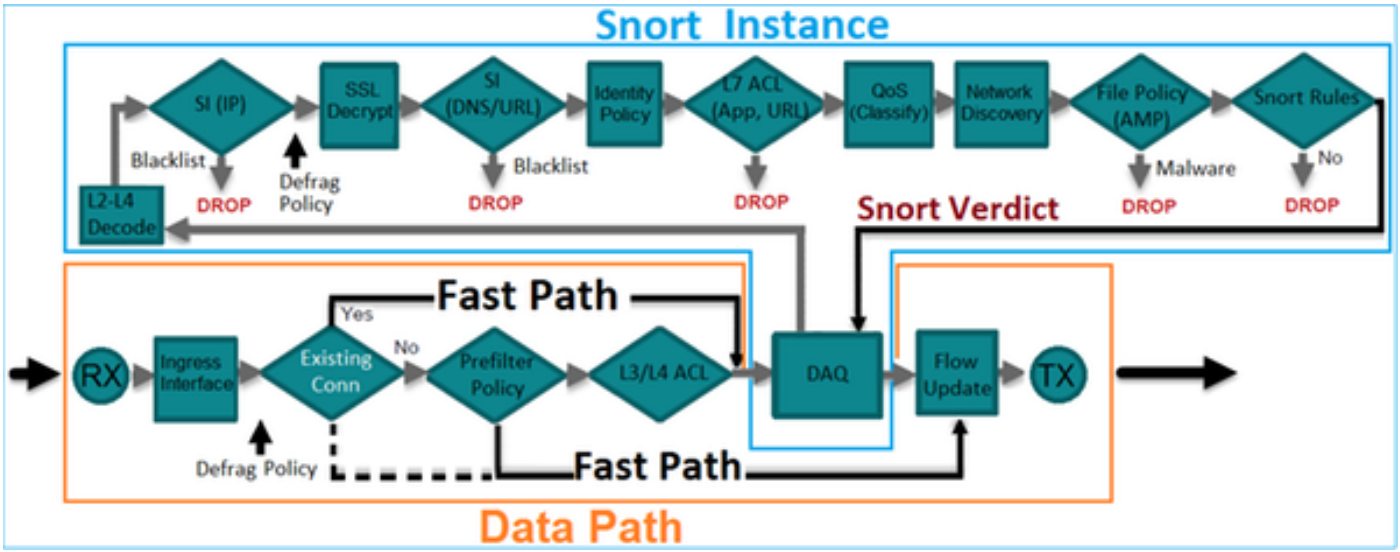
이 섹션에서는 인라인 페어 작업 확인을 위한 다음과 같은 확인 검사에 대해 설명합니다.

- 확인 1 - 패킷 트레이서 사용
- 확인 2 - 추적을 통한 캡처를 활성화하고 인라인 페어를 통해 TCP SYN/ACK 패킷 전송
- 확인 3 - 방화벽 엔진 디버그를 사용하여 FTD 트래픽 모니터링
- 확인 4 - 링크 상태 전파 기능 확인
- 확인 5 - 고정 NAT 구성

해결책

아키텍처 개요

FTD 인터페이스 2개가 인라인 페어 모드로 작동할 때는 패킷이 다음과 같이 처리됩니다.



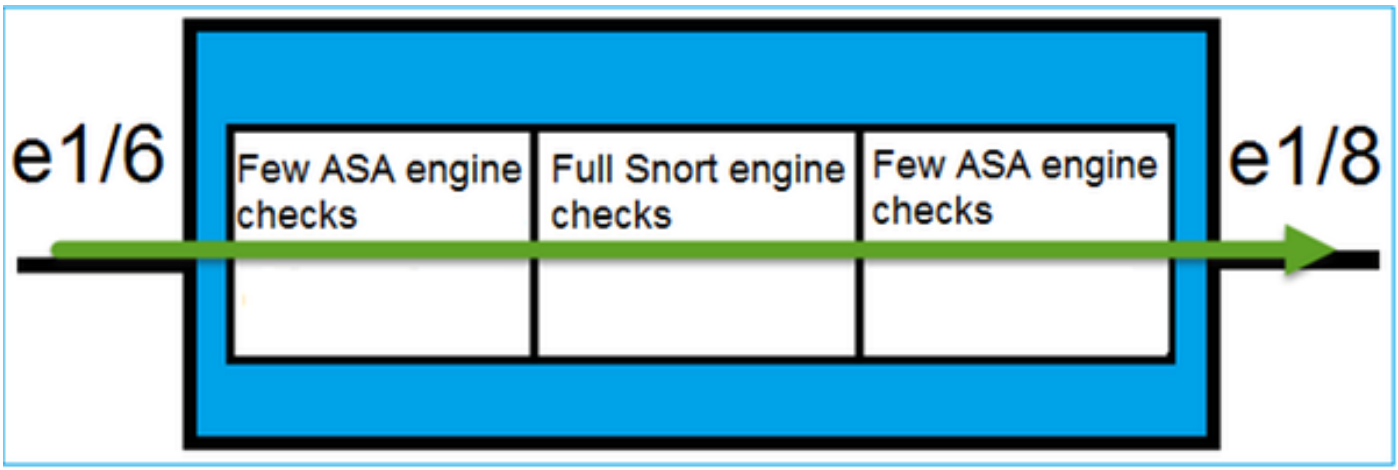
참고: 물리적 인터페이스만 인라인 페어 세트의 멤버로 포함될 수 있습니다.

기본 이론

- 인라인 페어를 구성할 때는 물리적 인터페이스 2개가 내부에서 브리지됨
- **클래식 인라인 IPS**와 매우 비슷함
- **라우팅** 또는 **투명 구축** 모드에서 사용 가능
- NAT, 라우팅, L3/L4 ACL 등 대부분의 ASA 엔진 기능은 인라인 페어를 통과하는 플로우에 **사용할 수 없음**

- 통과 트래픽을 **삭제할 수 있음**
- **소수의 ASA 엔진** 검사가 **전체 Snort 엔진** 검사와 함께 적용됨

마지막 항목은 다음 그림과 같이 표시할 수 있습니다.



확인 1 - 패킷 트레이서 사용

아래에는 인라인 페어를 통과하는 패킷을 에뮬레이트하는 패킷 트레이서 출력이 나와 있습니다. 출력에서 주목할 만한 부분은 굵은 글꼴로 강조 표시되어 있습니다.

```
> 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 will 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 will be sent to snort for additional processing where a verdict will be 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 페어를 통해 TCP SYN/ACK 패킷 전송

Scapy와 같은 패킷 제작 유틸리티를 사용하여 TCP SYN/ACK 패킷을 생성할 수 있습니다. 다음 구문은 SYN/ACK 플래그가 활성화된 3개 패킷을 생성합니다.

```
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 다음 캡처를 활성화하고 TCP SYN/ACK 패킷을 몇 개 전송해 보십시오.

```
> 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 전송하고 나면 생성된 연결을 확인할 수 있습니다.

```
> 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

>
```

- **b 플래그:** TCP 상태 건너뛰기를 활성화한 경우가 아니면 클래식 ASA는 요청하지 않은 SYN/ACK 패킷을 삭제합니다. 인라인 모드 페어의 FTD 인터페이스는 TCP 상태 건너뛰기 모드에서 TCP 연결을 처리하며 기존 연결에 속하지 않는 TCP 패킷을 삭제하지 않습니다.
- **N 플래그:** FTD Snort 엔진이 패킷을 검사합니다.

캡처를 수행하면 위의 설명과 같이 FTD를 통과하는 패킷 3개를 확인할 수 있습니다.

```
> 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
>
```

FTD 디바이스에서 나가는 3개 패킷:

```
> 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 패킷을 추적하면 Snort 엔진 판정과 같은 몇 가지 추가 정보를 확인할 수 있습니다.

```
> 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 will be 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:
```

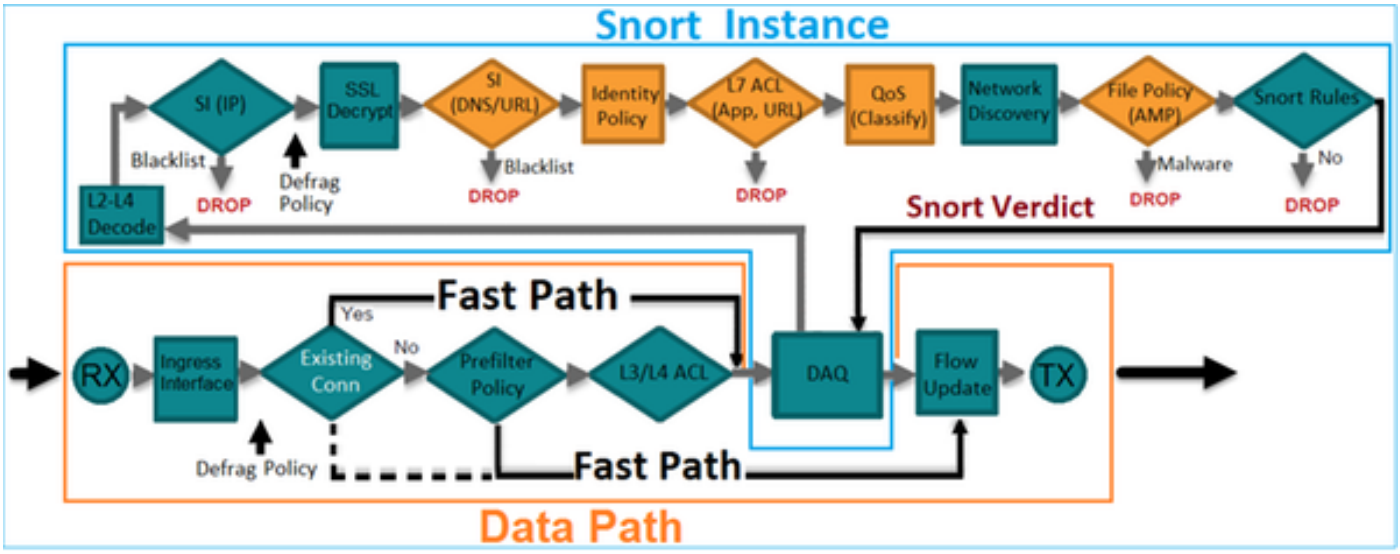
L4 RULE: DEFAULT ACTION RULE **Additional Information: This packet will be sent to snort for additional processing where a verdict will be reached Phase: 5 Type: NGIPS-EGRESS-INTERFACE-LOOKUP Subtype: Resolve Egress Interface Result: ALLOW Config: Additional Information: Ingress interface INSIDE is in 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 번째로 캡처된 패킷을 추적하면 패킷이 기존 연결과 일치하므로 ACL 검사를 건너뛰지만 Snort 엔진에서는 검사된다는 내용이 표시됩니다.

> **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: Result: ALLOW Config: Additional Information: Found flow with id 282, using existing 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 - 허용된 트래픽에 대한 방화벽 엔진 디버그

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



인라인 페어를 통해 TCP SYN/ACK 패킷을 전송하면 디버그 출력에서 다음과 같은 정보를 확인할 수 있습니다.

```
> 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 Allow and prefilter rule 0
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 로깅을 활성화하고 e1/6 인터페이스에 연결된 스위치 포트를 종료합니다. FTD CLI에서 두 인터페이스가 모두 다운되었음이 표시됩니다.

```
> 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 다음과 같은 내용이 표시됩니다.

```
> show logging

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 down pair interface Ethernet1/8(OUTSIDE)
>
```

인라인 세트 상태에는 2개 인터페이스 멤버의 상태가 표시됩니다.

```
> 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 상태는 서로 다릅니다.

```
> 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 상태는 다음과 같습니다.

```
> 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
>
```

스위치 포트를 다시 활성화하고 나면 FTD 로그에는 다음과 같은 내용이 표시됩니다.

```
> show logging
...
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) bringing up pair interface Ethernet1/8(OUTSIDE)
```

>

확인 5 - 고정 NAT 구성

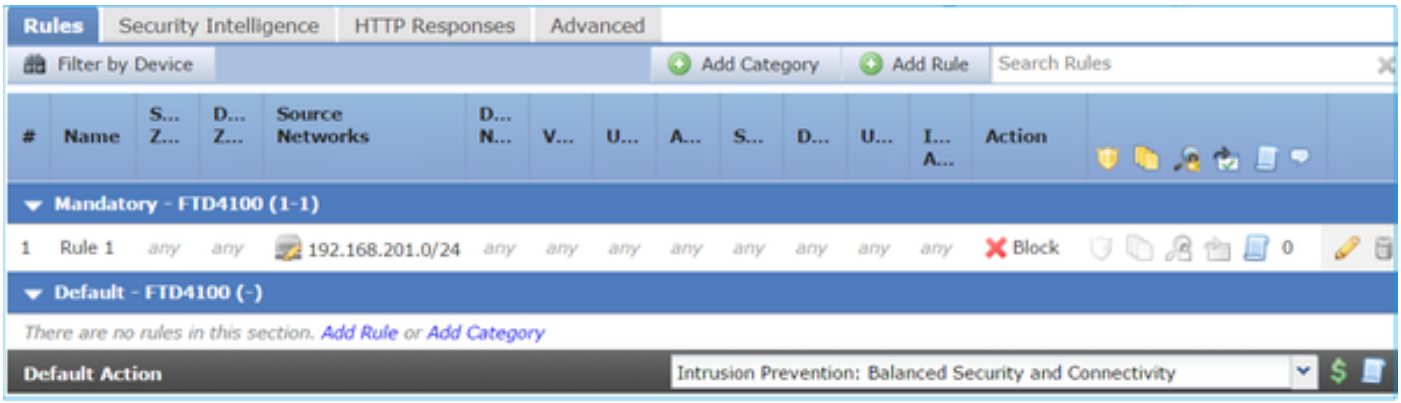
해결책

인라인, 인라인 탭 또는 수동 모드로 작동하는 인터페이스에 대해서는 NAT가 지원되지 않습니다.

http://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 페어 인터페이스 모드에서 패킷 차단

다음과 같은 차단 규칙을 생성하고 FTD 인라인 페어를 통해 트래픽을 전송한 후에 동작을 관찰합니다.



해결책

추적을 통한 캡처를 활성화하고 FTD 인라인 페어를 통해 SYN/ACK 패킷을 전송합니다. 트래픽이 차단됩니다.

```
> 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
```

패킷을 추적하면 다음 결과가 표시됩니다.

```
> 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 will be 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 flow-start
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
```

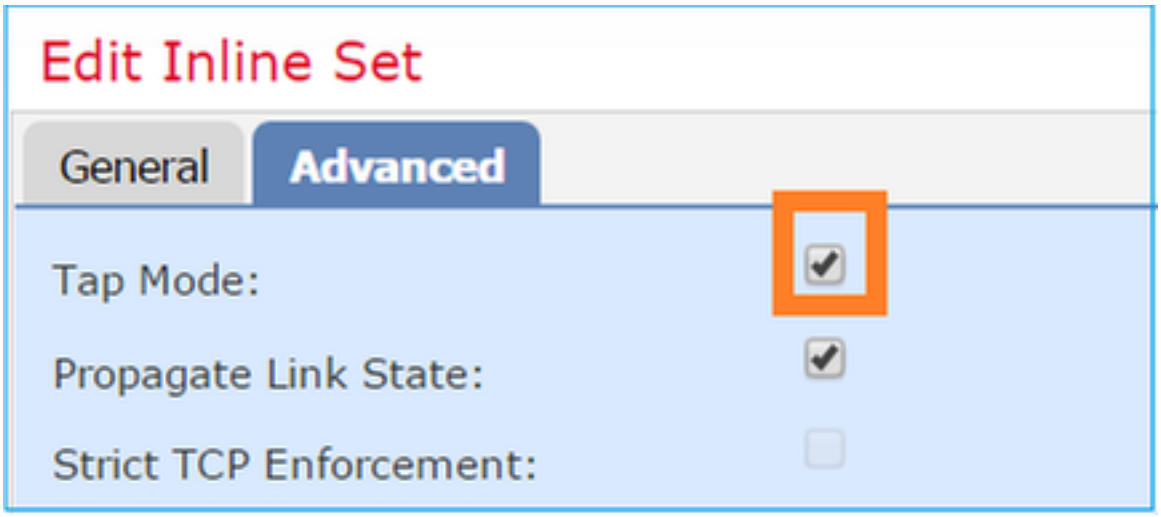
위의 추적에서는 패킷이 FTD ASA 엔진에 의해 삭제되어 FTD Snort 엔진으로 전달되지 않았음을 확인할 수 있습니다.

인라인 페어 모드(탭 포함) 구성

인라인 페어에서 탭 모드를 활성화합니다.

해결책

Devices(디바이스) > Device Management(디바이스 관리) > Inline Sets(인라인 세트)로 이동하여 인라인 페어를 수정하고 **Advanced(고급)** 탭을 클릭한 다음 **Tap Mode(탭 모드)**를 활성화합니다.



확인

```
> 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 >
```

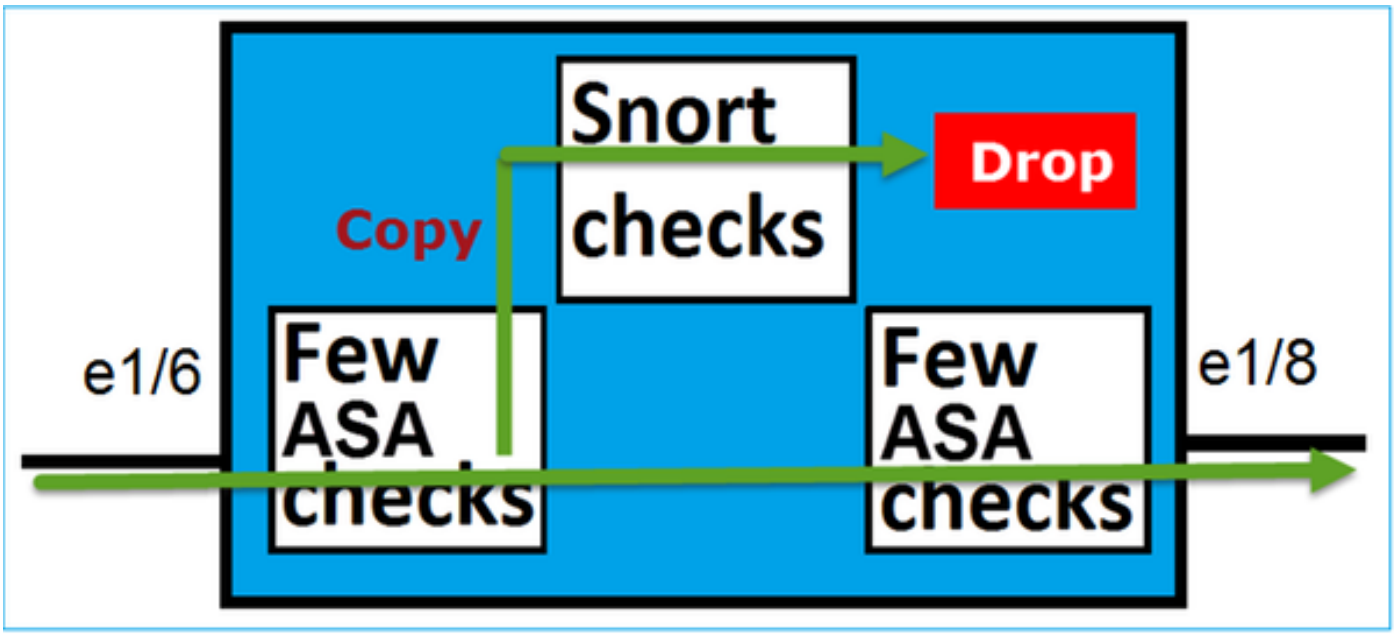
FTD 인라인 페어(탭 포함) 인터페이스 작업 확인

기본 이론

- 인라인 페어(탭 포함)을 구성할 때는 물리적 인터페이스 2개가 내부에서 브리지됨

- **라우팅** 또는 **투명 구축** 모드에서 사용 가능
- NAT, 라우팅, L3/L4 ACL 등 대부분의 **ASA 엔진 기능**은 인라인 페어를 통과하는 플로우에 **사용할 수 없음**
- 실제 트래픽을 **삭제할 수 없음**
- **소수의 ASA 엔진** 검사가 **전체 Snort 엔진** 검사와 함께 **실제 트래픽의 복사본에** 적용됨

마지막 항목은 다음 그림과 같이 표시할 수 있습니다.



인라인 페어(탭 포함) 모드에서는 통과 트래픽을 삭제하지 않습니다. 패킷을 추적하면 이를 확인할 수 있습니다.

```
> 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 will be 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 flow-
start 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
>
```

비교: 인라인 페어와 탭 포함한 인라인 페어

	인라인 페어 > show inline-set	인라인 페어(탭 포함) > show inline-set
인라인 세트 보기	Inline-set Inline-Pair-1 Mtu is 1500 bytes Failsafe mode is on/activated	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** **>**	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** **>**
인터페이스 보기	**> 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": 3957 packets input, 264913 bytes 144 packets output, 58664 bytes 4 packets dropped 1 minute input rate 0 pkts/sec, 26 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, 28 bytes/sec 5 minute output rate 0 pkts/sec, 9 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": 144 packets input, 55634 bytes 3954 packets output, 339987 bytes 0 packets dropped 1 minute input rate 0 pkts/sec, 7 bytes/sec 1 minute output rate 0 pkts/sec, 37 bytes/sec 1 minute drop rate, 0 pkts/sec 5 minute input rate 0 pkts/sec, 8 bytes/sec 5 minute output rate 0 pkts/sec, 39 bytes/sec 5 minute drop rate, 0 pkts/sec **>**	**> show interface e1/6** Interface Ethernet1/6 "INSIDE", is up, line protocol is up Hardware is EtherSVI, BW 1000 Mbps, D 1000 usec MAC address 5897.bdb9.770e, MTU IPS Interface-Mode: **inline-tap**, Inline- Inline-Pair-1 IP address unassigned Traffic Statistics for "INSIDE": 24 packets input, 1378 bytes 0 packets output, 0 bytes 24 packets dropped 1 minute input rate 0 pkts/sec, 0 bytes/ 1 minute output rate 0 pkts/sec, 0 byte 1 minute drop rate, 0 pkts/sec 5 minute input rate 0 pkts/sec, 0 bytes/ 5 minute output rate 0 pkts/sec, 0 byte 5 minute drop rate, 0 pkts/sec **>show interface e1/8** Interface Ethernet1/8 "OUTSIDE", is up, li protocol is up Hardware is EtherSVI, BW 1000 Mbps, D 1000 usec MAC address 5897.bdb9.774d, MTU IPS Interface-Mode: **inline-tap**, Inline- Inline-Pair-1 IP address unassigned Traffic Statistics for "OUTSIDE": 1 packets input, 441 bytes 0 packets output, 0 bytes 1 packets dropped 1 minute input rate 0 pkts/sec, 0 bytes/ 1 minute output rate 0 pkts/sec, 0 byte 1 minute drop rate, 0 pkts/sec 5 minute input rate 0 pkts/sec, 0 bytes/ 5 minute output rate 0 pkts/sec, 0 byte 5 minute drop rate, 0 pkts/sec **>**
차단 규칙을	**> show capture CAPI packet-number 1 trace**	**> show capture CAPI packet-number 1 tra**

사용한 패킷 처리	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 will be 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 flow-start 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	3 packets captured 1: 16:56:02.631437 192.168.201.50.2 192.168.201.60.80: 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 NGIPS mode and NGIPS services will be 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 den 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: 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,bu**

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

1 packet shown
>

packet forwarded due to inline-tap

1 packet shown
>

요약

- 인라인 페어 모드를 사용할 때 패킷은 주로 FTD Snort 엔진을 통과합니다.
- TCP 연결은 TCP 상태 건너뛰기 모드에서 처리됩니다.
- FTD ASA 엔진 측면에서 볼 때 ACL 정책이 적용됩니다.
- 인라인 페어 모드를 사용 중일 때는 패킷이 인라인으로 처리되므로 차단될 수 있습니다.
- 탭 모드가 활성화되어 있으면 패킷의 복사본을 내부적으로 검사하여 삭제하며, 실제 트래픽은 수정되지 않은 상태로 FTD를 통과합니다.

관련 문서

Cisco Firepower NGFW