Configure FTD Interfaces in Inline-Pair Mode

Contents

Introduction

This document describes the configuration, verification and background operation of an Inline Pair Interface on a Firepower Threat Defense (FTD) appliance.

Prerequisites

Requirements

There are not specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Firepower 4150 FTD (code 6.1.0.x and 6.3.x)
- Firepower Management Center (FMC) (code 6.1.0.x and 6.3.x)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Related Products

This document can also be used with these hardware and software versions:

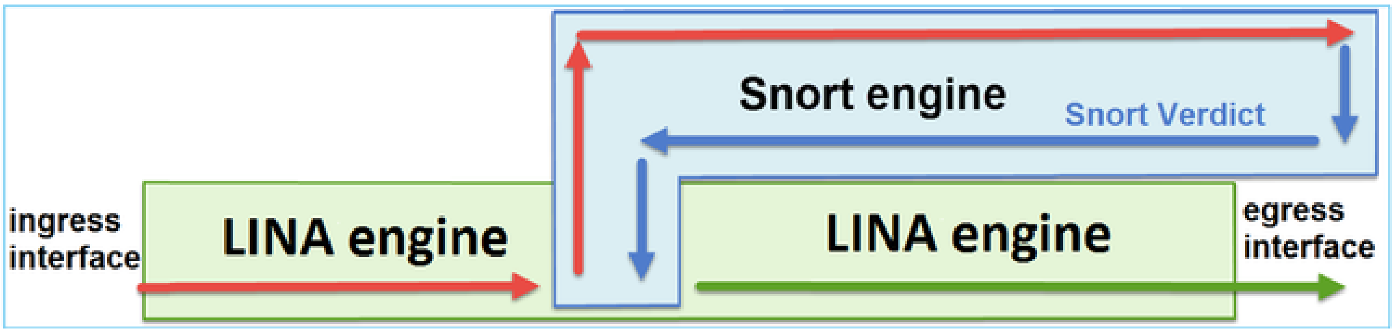
- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), Kernel-based Virtual Machine (KVM)
- FTD software code 6.2.x and later

Background Information

FTD is a unified software image that consists of 2 main engines:

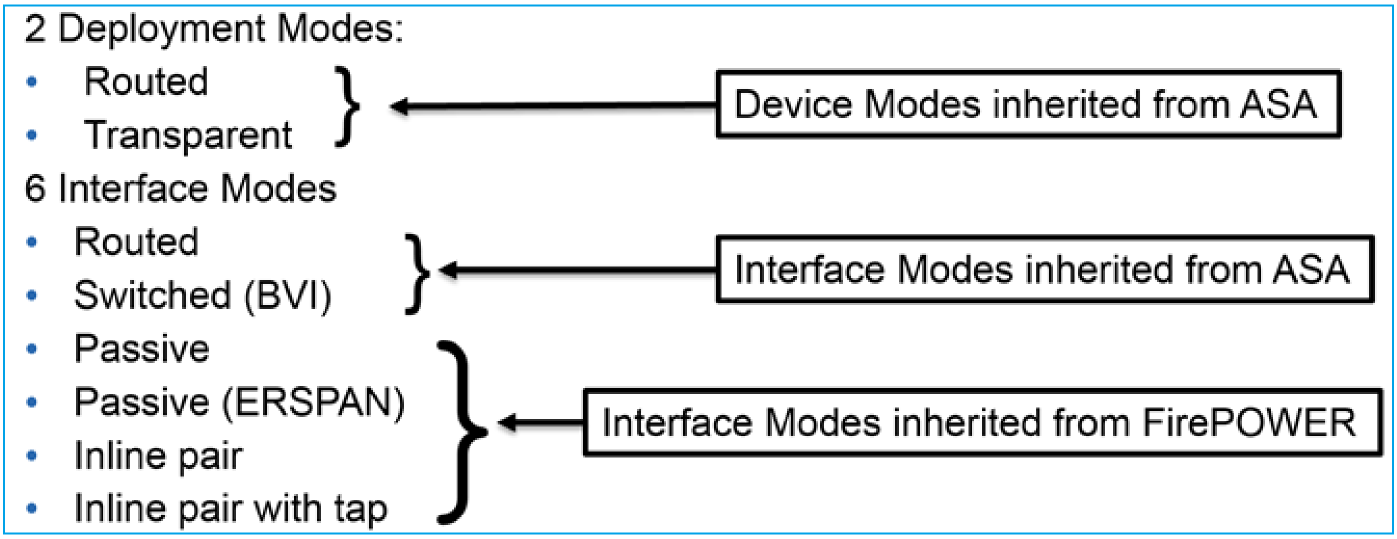
- LINA engine
- Snort engine

This figure shows how the 2 engines interact:



- A packet enters the ingress interface and it is handled by the LINA engine
- If it is required by the FTD policy the packet is inspected by the Snort engine
- The Snort engine returns a verdict for the packet
- The LINA engine drops or forwards the packet based on Snort’s verdict

FTD provides two Deployment modes and six Interface modes as shown in image:



2 Deployment Modes:

- Routed
- Transparent

Device Modes inherited from ASA

6 Interface Modes

- Routed
- Switched (BVI)

Interface Modes inherited from ASA

- Passive
- Passive (ERSPAN)
- Inline pair
- Inline pair with tap

Interface Modes inherited from FirePOWER

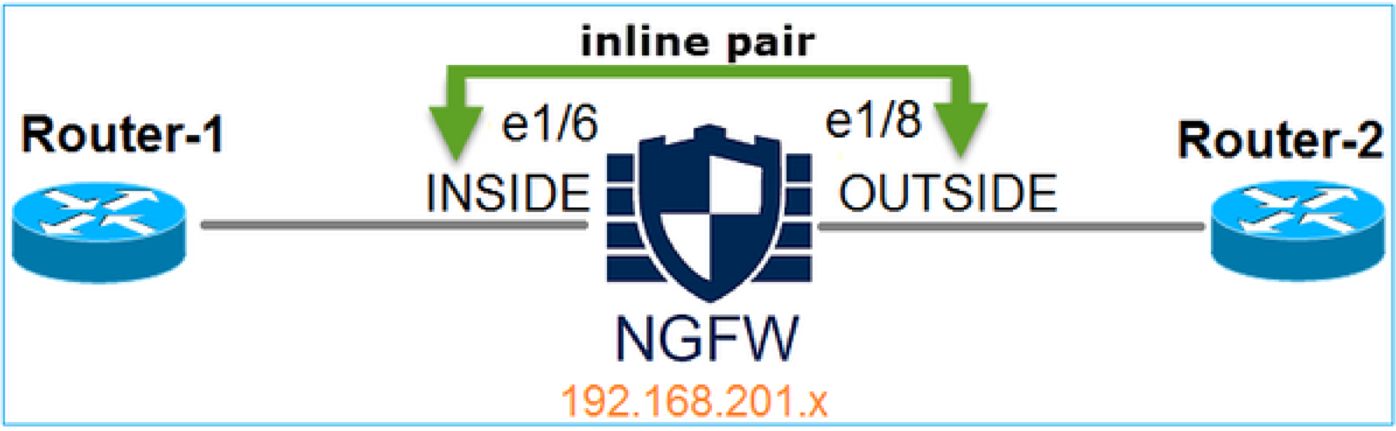
Note: You can mix interface modes on a single FTD appliance.

Here is a high level overview of the various FTD deployment and interface modes:

FTD interface mode	FTD Deployment mode	Description	Traffic can be dropped
Routed	Routed	Full LINA-engine and Snort-engine checks	Yes
Switched	Transparent	Full LINA-engine and Snort-engine checks	Yes
Inline Pair	Routed or Transparent	Partial LINA-engine and full Snort-engine checks	Yes
Inline Pair with Tap	Routed or Transparent	Partial LINA-engine and full Snort-engine checks	No
Passive	Routed or Transparent	Partial LINA-engine and full Snort-engine checks	No
Passive (ERSPAN)	Routed	Partial LINA-engine and full Snort-engine checks	No

Configure Inline Pair Interface on FTD

Network Diagram



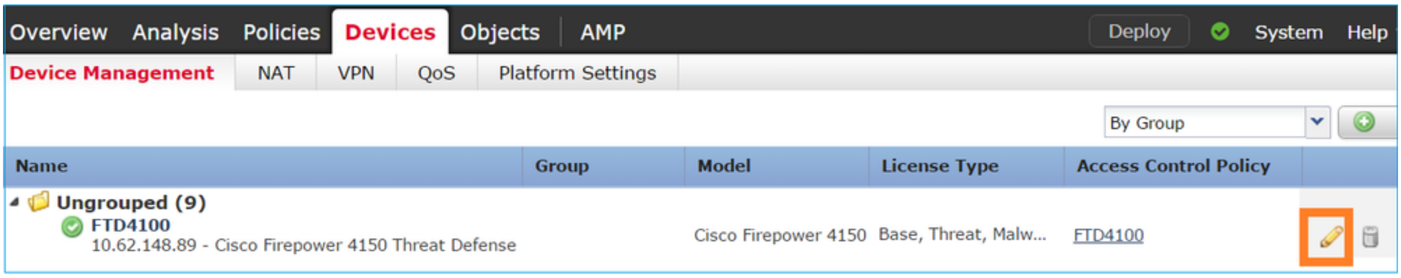
Requirement

Configure physical interfaces e1/6 and e1/8 in Inline Pair Mode as per these requirements:

Interface	e1/6	e1/8
Name	INSIDE	OUTSIDE
Security Zone	INSIDE_ZONE	OUTSIDE_ZONE
Inline Set name	Inline-Pair-1	
Inline Set MTU	1500	
FailSafe	Enabled	
Propagate Link State	Enabled	

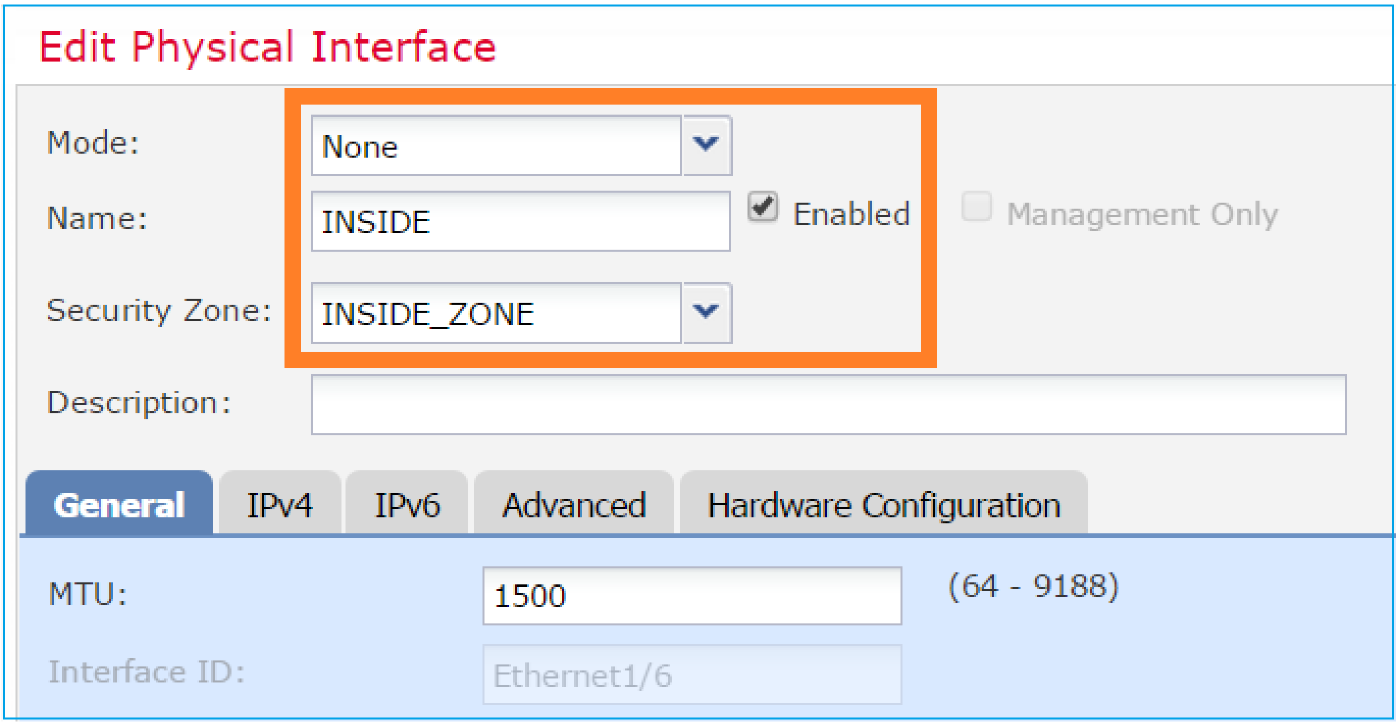
Solution

Step 1. In order to configure to the individual interfaces, Navigate to **Devices > Device Management,** select the appropriate device and select **Edit** as shown in the image.



Name	Group	Model	License Type	Access Control Policy
Ungrouped (9)				
FTD4100 10.62.148.89 - Cisco Firepower 4150 Threat Defense		Cisco Firepower 4150	Base, Threat, Malw...	FTD4100

Next, Specify **Name** and Tick **Enabled** for the interface as shown in the image.



Edit Physical Interface

Mode: None

Name: INSIDE ☑ Enabled □ Management Only

Security Zone: INSIDE_ZONE

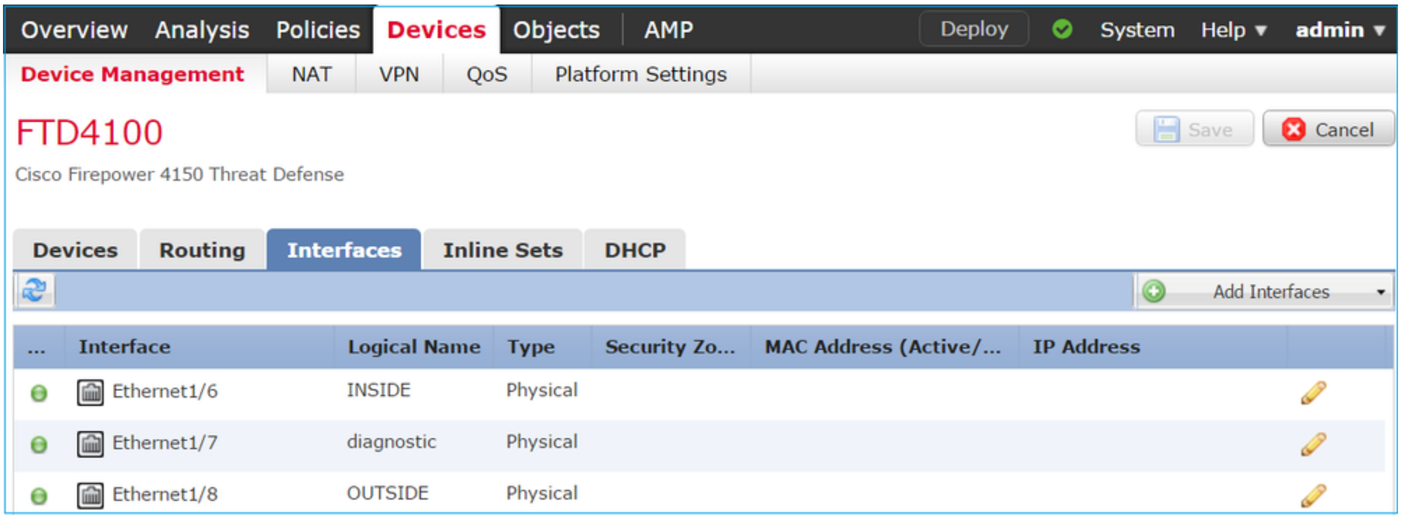
Description:

MTU: 1500 (64 - 9188)

Interface ID: Ethernet1/6

Note: The Name is the the nameif of the interface.

Similarly for interface Ethernet1/8. The final result is as shown in the image.



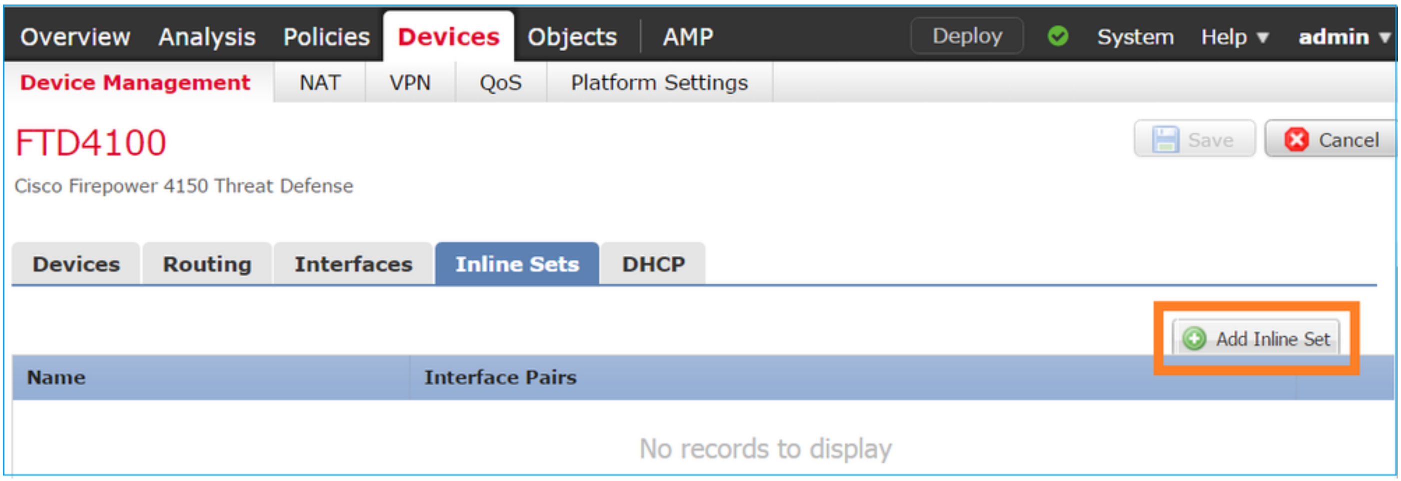
FTD4100

Cisco Firepower 4150 Threat Defense

...	Interface	Logical Name	Type	Security Zo...	MAC Address (Active/...	IP Address
●	Ethernet1/6	INSIDE	Physical			
●	Ethernet1/7	diagnostic	Physical			
●	Ethernet1/8	OUTSIDE	Physical			

Step 2. Configure the Inline Pair.

Navigate to **Inline Sets > Add Inline Set** as shown in the image.



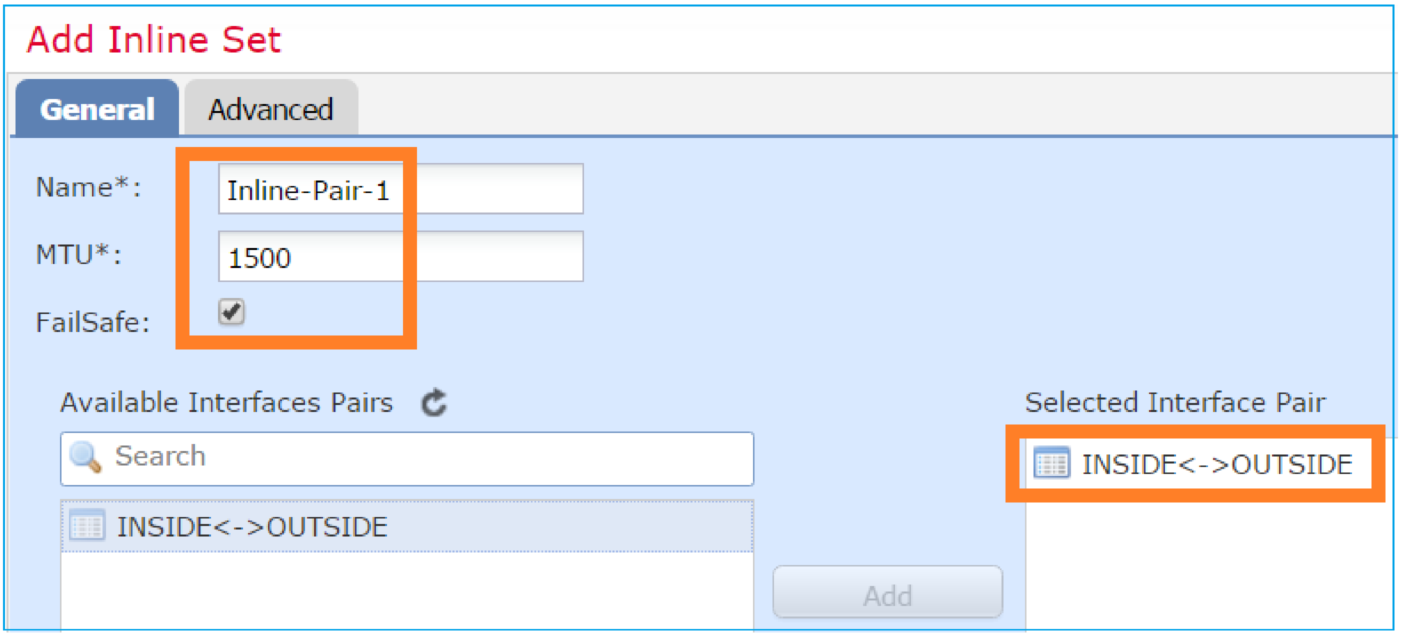
FTD4100

Cisco Firepower 4150 Threat Defense

Name	Interface Pairs

No records to display

Step 3. Configure the General settings as per the requirements as shown in the image.



Add Inline Set

Name*: Inline-Pair-1

MTU*: 1500

FailSafe: ☑

Available Interfaces Pairs

Search

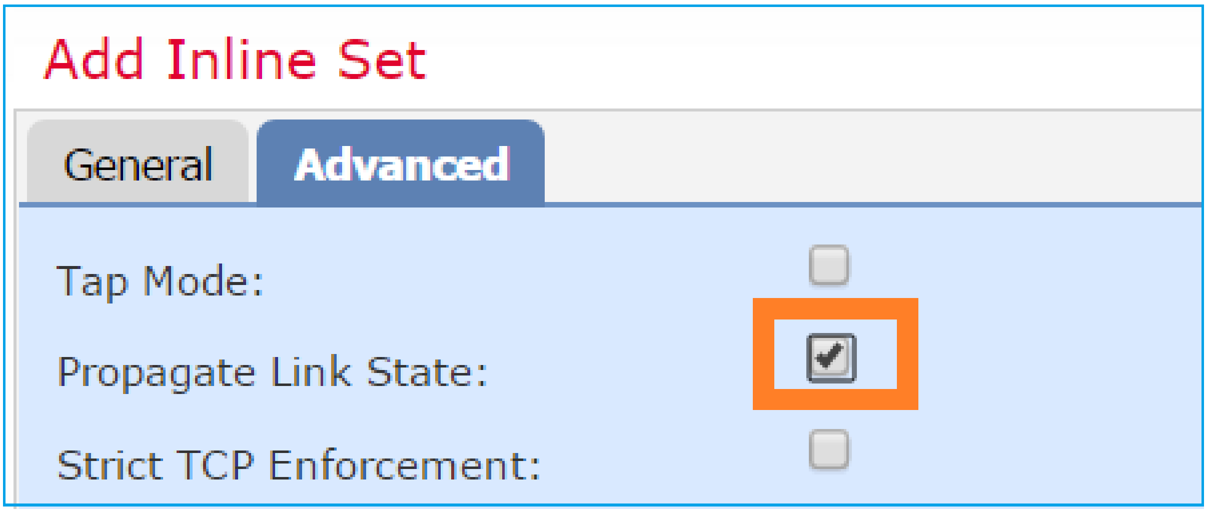
INSIDE<->OUTSIDE

Selected Interface Pair

INSIDE<->OUTSIDE

> **Note**: Failsafe allows the traffic to pass through the inline pair uninspected in case the interface buffers are full (typically seen when the device is overloaded or the Snort engine is overloaded). The interface buffer size is dynamically allocated.

Step 4. Enable **Propagate Link State** option in the Advanced Settings as shown in the image.



Add Inline Set

Tap Mode: □

Propagate Link State: ☑

Strict TCP Enforcement: □

Link state propagation automatically brings down the second interface in the inline interface pair when one of the interfaces in the inline set goes down.

Step 5. **Save** the changes and **Deploy**.

Verify

Use this section in order to confirm that your configuration works properly.

Verify the Inline Pair configuration from the FTD CLI.

Solution

Log in to FTD CLI and verify the Inline Pair configuration:

```
> 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
```

```
>
```

Note: The Bridge Group ID is a value different than 0. If Tap Mode is on then it is 0

Interface and name information:

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

Verify the interface status:

```
> 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
```

Verify physical interface information:

```
> 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
>
```

Verify FTD Inline Pair Interface Operation

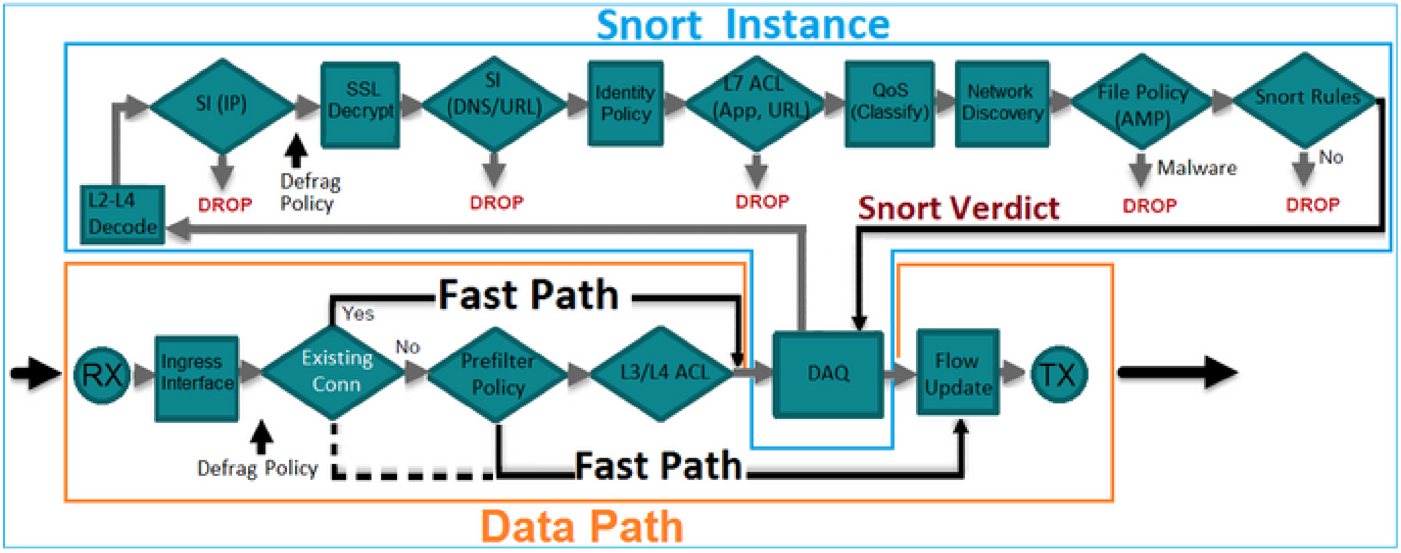
This section covers these verification checks in order to verify the Inline Pair operation:

- Verification 1. With the use of packet-tracer
- Verification 2. Enable capture with trace and send a TCP synchronize/acknowledge (SYN/ACK) packet through the Inline Pair
- Verification 3. Monitor FTD traffic with the use of firewall engine debug
- Verification 4. Verify the Link-State Propagation functionality
- Verification 5. Configure Static Network Address Translation (NAT)

Solution

Architectural overview

When 2 FTD interfaces operate in Inline-pair mode a packet is handled as shown in the image.



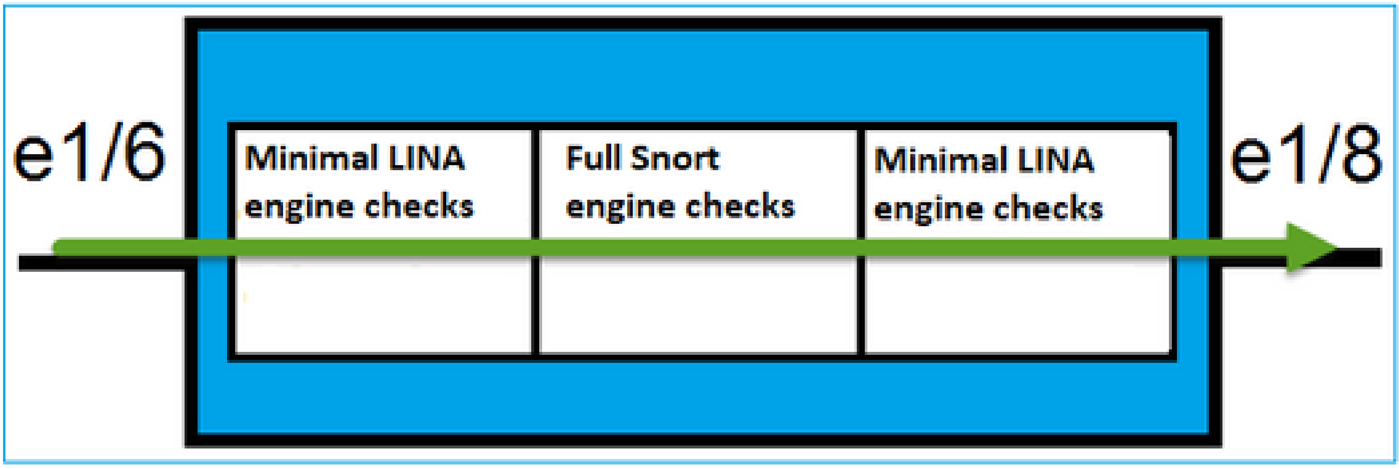
Note: Only physical interfaces can be members of an Inline pair set

Basic Theory

- When you configure an Inline Pair 2 Physical interfaces are internally bridged
- Very similar to classic inline Intrusion Prevention System (IPS)
- Available in Routed or Transparent Deployment modes
- Most of the LINA engine features (NAT, Routing etc) are not available for flows which go through an Inline Pair
- Transit traffic can be dropped

- A few LINA engine checks are applied along with full Snort engine checks

The last point can be visualized as shown in the image:



Verification 1. With the Use of Packet-Tracer

The packet-tracer output which emulates a packet that traverses the inline pair with the important points highlighted:

```
> 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

>
```

Verification 2. Send TCP SYN/ACK Packets Through Inline Pair

You can generate TCP SYN/ACK packets with the use of a packet that crafts utility like Scapy. This syntax generates 3 packets with SYN/ACK flags enabled:

```
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)
```

Enable this capture on FTD CLI and send a few TCP SYN/ACK packets:

```
> 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
>
```

After you send the packets through the FTD you can see a connection that was created:

```
> 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

>
```

> **Note**: b flag - A classic ASA would drop an unsolicited SYN/ACK packet unless TCP state-bypass was enabled. An FTD interface in Inline Pair mode handles a TCP connection in a TCP state-bypass mode and doesn't drop TCP packets that don't belong to the connections that already exist.

> **Note:** N flag - The packet is inspected by the FTD Snort engine.

The captures prove this, since you can see the 3 packets that traverse the FTD:

```
> 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 packets exits the FTD device:

```
> 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
>
```

With the Trace of the first capture packet reveals some additional information like the Snort engine verdict:

```
> 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
>
```

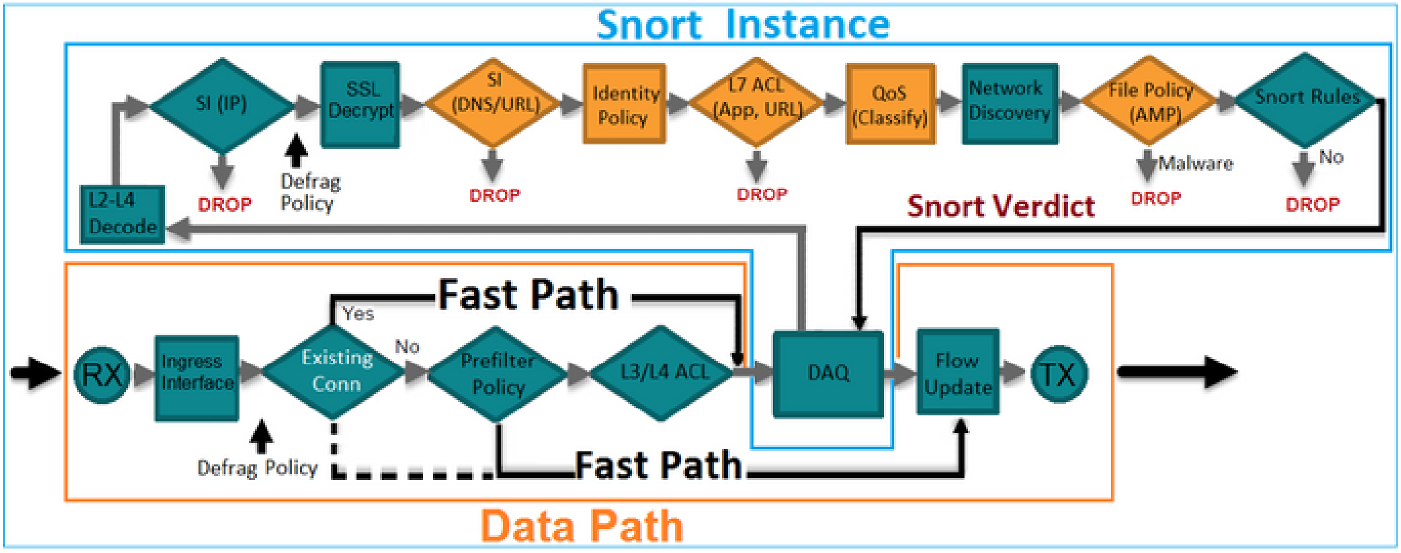
With the Trace of the second captured packet shows that the packet matches an existing connection so it bypasses the ACL check, but still is inspected by the Snort engine:

```
> 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 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
>
```

Verification 3. Firewall Engine Debug For Allowed Traffic

Firewall engine debug runs against specific components of the FTD Snort Engine like the Access Control Policy as shown in the image:



When you send the TCP SYN/ACK packets through Inline Pair you can see in the debug output:

```
> 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
```

Verification 4. Verify Link-State Propagation

Enable buffer logging on FTD and shutdown the switchport connected to e1/6 interface. On FTD CLI you must see that both interfaces went down:

```
> 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
>
```

The FTD logs show:

```
> 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)
>
```

The inline-set status shows the state of the 2 interface members:

```
> 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
>
```

Note the difference in the status of the 2 interfaces:

```
> 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
>
```

And for the Ethernet1/8 interface:

```
> 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
>
```

After you re-enable the switchport the FTD logs show:

```
> 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)
>
```

Verification 5. Configure Static NAT

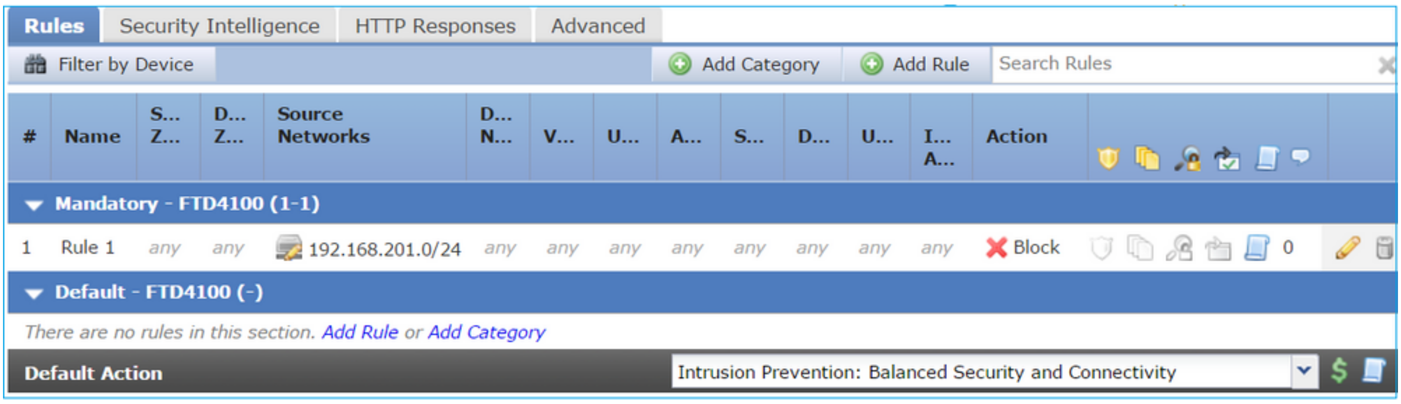
Solution

NAT is not supported for interfaces that operates in inline, inline tap or passive modes:

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

Block Packet on Inline Pair Interface Mode

Create a Block rule, send traffic through the FTD Inline Pair and observe the behavior as shown in the image.



#	Name	S... Z...	D... Z...	Source Networks	D... N...	V...	U...	A...	S...	D...	U...	I... A...	Action	
Mandatory - FTD4100 (1-1)														
1	Rule 1	any	any	192.168.201.0/24	any	any	any	any	any	any	any	any	Block	0
Default - FTD4100 (-)														
There are no rules in this section. Add Rule or Add Category														

Default Action: Intrusion Prevention: Balanced Security and Connectivity

Solution

Enable capture with trace and send the SYN/ACK packets through the FTD Inline Pair. The traffic is blocked:

```
> 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
```

With the trace, a packet reveals:

```
> 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
```

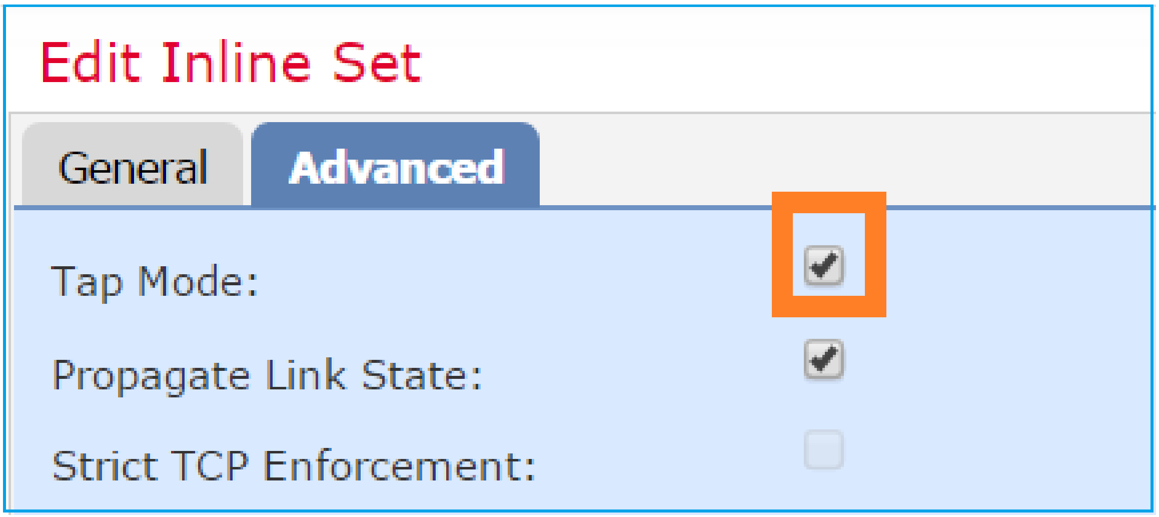
In this trace, it can be seen that the packet was dropped by the FTD LINA engine and was not forwarded to the FTD Snort engine.

Configure Inline Pair Mode With Tap

Enable Tap mode on the Inline Pair.

Solution

Navigate to **Devices > Device Management > Inline Sets > Edit Inline Set > Advanced** and enable **Tap Mode** as shown in the image.



Tap Mode: ☑

Propagate Link State: ☑

Strict TCP Enforcement: □

Verification

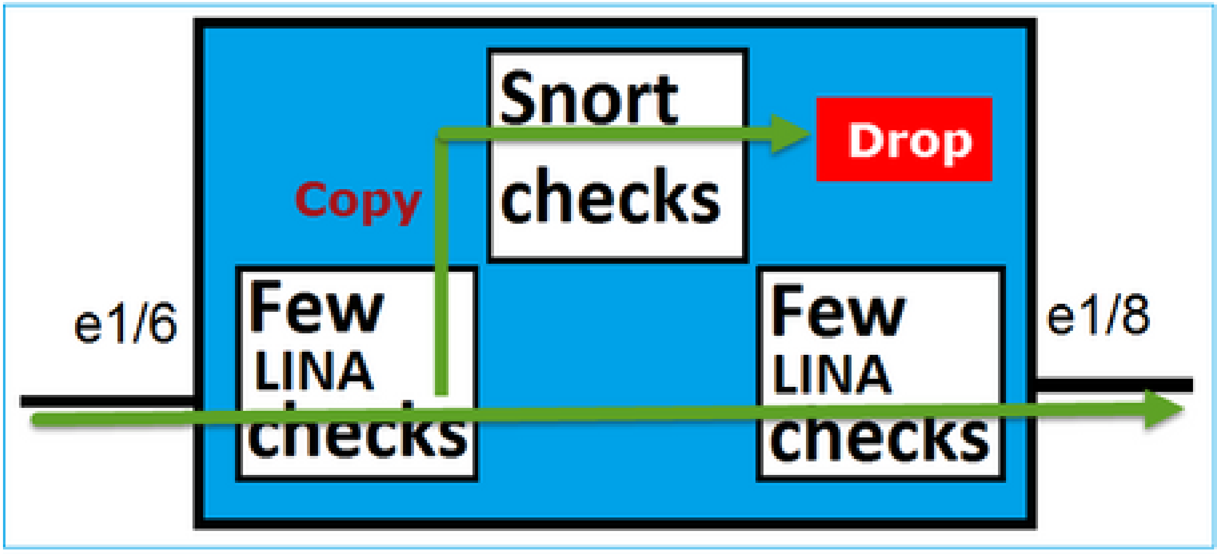
```
> show inline-set

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
>
```

Verify FTD Inline Pair With Tap Interface Operation

Basic theory

- When you configure an Inline Pair with Tap 2, physical interfaces are internally bridged
- It is available in Routed or Transparent Deployment modes
- Most of LINA engine features (NAT, Routing etc) are not available for flows which go through the Inline Pair
- Actual traffic cannot be dropped
- A few LINA engine checks are applied along with full Snort engine checks to a copy of the actual traffic

The last point is as shown in the image:



Inline Pair with Tap Mode doesn't drop the transit traffic. With the trace of a packet it confirms this:

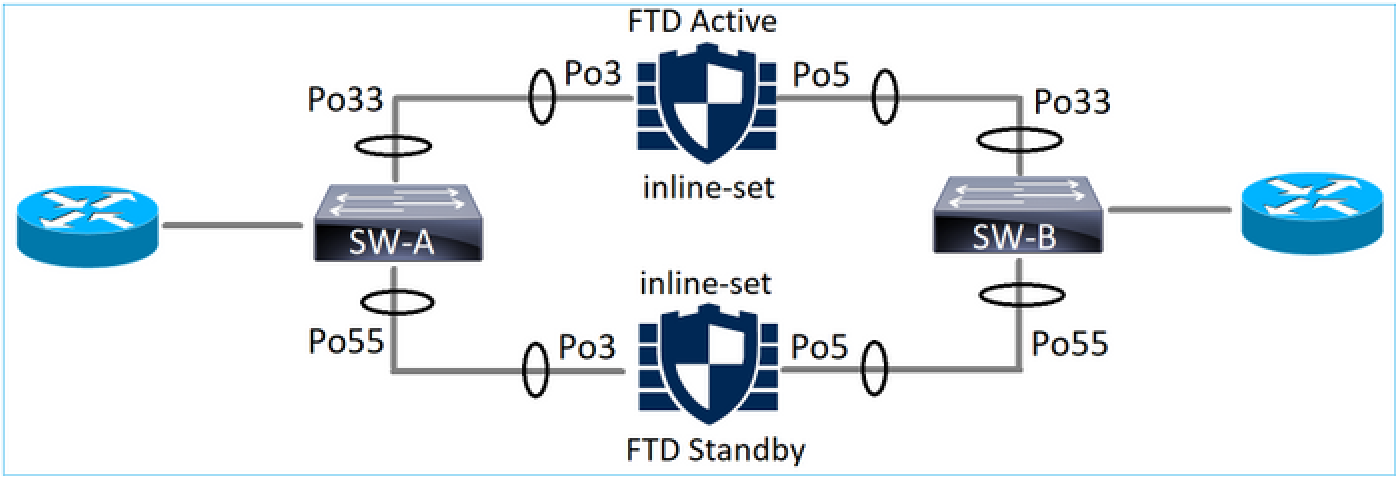
```
> show capture CAPI packet-number 2 trace

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
>
```

Inline Pair and Etherchannel

You can configure inline pair with etherchannel in 2 ways:

1. Etherchannel terminated on FTD
2. Etherchannel going through the FTD (requires FXOS code 2.3.1.3 and above)

Etherchannel terminated on FTD



Etherchannels on SW-A:

```
SW-A# show etherchannel summary | i Po33|Po55
33      Po33(SU)         LACP      Gi3/11(P)
35      Po35(SU)         LACP      Gi2/33(P)
```

Etherchannels on SW-B:

```
SW-B# show etherchannel summary | i Po33|Po55
33      Po33(SU)         LACP        Gi1/0/3(P)
55      Po55(SU)         LACP        Gi1/0/4(P)
```

The traffic is being forwarded through the Active FTD based on MAC address learning:

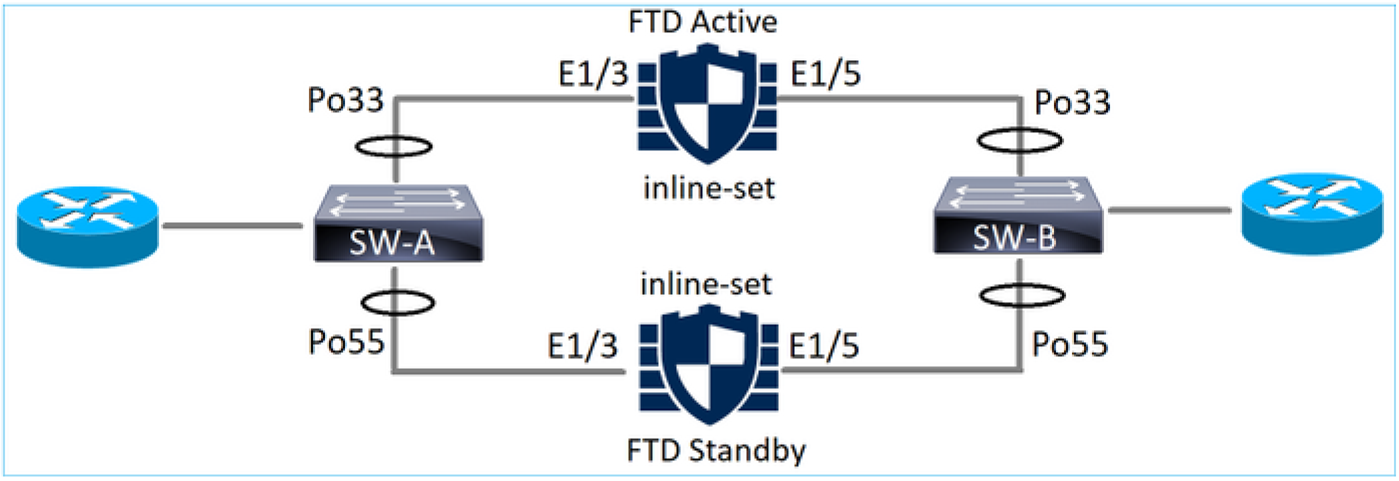
```
SW-B# show mac address-table address 0017.dfd6.ec00
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0017.dfd6.ec00    DYNAMIC     Po33
Total Mac Addresses for this criterion: 1
```

The inline-set on FTD:

```
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
```

> **Note**: In case of an FTD failover event the traffic outage depends mainly on the time it takes on the switches to learn the MAC address of the remote peer.

Etherchannel through the FTD



Etherchannels on SW-A:

```
SW-A# show etherchannel summary | i Po33|Po55
33      Po33(SU)        LACP      Gi3/11(P)
55      Po55(SD)        LACP      Gi3/7(I)
```

The LACP packets going through the Standby FTD are blocked:

```
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
```

Etherchannels on SW-B:

```
SW-B# show etherchannel summary | i Po33|Po55
33      Po33(SU)        LACP        Gi1/0/3(P)
55      Po55(SD)        LACP        Gi1/0/4(s)
```

The traffic is being forwarded through the Active FTD based on MAC address learning:

```
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
```

The inline-set on FTD:

```
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
```

> **Caution**: In this scenario in case of an FTD failover event the convergence time mainly depends on the Etherchannel LACP negotiation and depending on the time it takes the outage can be quite longer. In case the Etherchannel mode is ON (no LACP) then the convergence time depends on MAC address learning.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Comparison: Inline Pair vs Inline Pair with Tap

	Inline pair	Inline pair with Tap
show inline-set	> 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** >	> **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** >
show interface	> **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	> **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-tap**, Inline-Set: 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/sec

To Handle Packet with Block rule

```
    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 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
>
```

```
    1 minute output rate 0 pkts/sec,  0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec,  0 bytes/sec
    5 minute output rate 0 pkts/sec,  0 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-tap, Inline-Set: 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/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,  0 bytes/sec
    5 minute output rate 0 pkts/sec,  0 bytes/sec
    5 minute drop rate, 0 pkts/sec
>

> show capture CAPI packet-number 1 trace

3 packets captured

  1: 16:56:02.631437       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0)
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 NGIP
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
rule-id 268441600 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY:
- 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


1 packet shown
>
```

Summary

- When you use Inline Pair mode, the packet goes mainly through the FTD Snort engine
- TCP connections are handled in a TCP state-bypass mode
- From an FTD LINA engine point of view, an ACL policy is applied
- When Inline Pair Mode is in use, packets can be blocked since they are processed inline
- When Tap Mode is enabled, a copy of the packet is inspected and dropped internally while

the actual traffic goes through FTD unmodified

Related Information

- Cisco Firepower NGFW
- Technical Support & Documentation - Cisco Systems