

インラインペアモードでのFTDインターフェイスの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[背景説明](#)

[FTDでのインラインペアインターフェイスの設定](#)

[ネットワーク図](#)

[確認](#)

[FTDのインラインペアインターフェイスの動作の確認](#)

[基本理論](#)

[検証1.Packet-Tracerの使用](#)

[検証2.インラインペアを使用したTCP SYN/ACKパケットの送信](#)

[検証3.許可されたトラフィックのファイアウォールエンジンデバッグ](#)

[検証4.リンクステートプロパゲーションの確認](#)

[検証5.スタティックNATの設定](#)

[インラインペアインターフェイスモードでのパケットのブロック](#)

[タップによるインラインペアモードの設定](#)

[FTDのタップ付きインラインペアのインターフェイス動作の確認](#)

[インラインペアとEtherchannel](#)

[FTDで終端されたEtherChannel](#)

[FTD経由のEtherChannel](#)

[トラブルシューティング](#)

[比較：インラインペアとタップ付きインラインペア](#)

[要約](#)

[関連情報](#)

はじめに

このドキュメントでは、Firepower Threat Defense(FTD)アプライアンスのインラインペアインターフェイス(IPAIR)の設定、検証、および動作について説明します。

前提条件

要件

このドキュメントに関する特定の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower4150 FTD (コード6.1.0.xおよび6.3.x)
- Firepower Management Center(FMC) (コード6.1.0.xおよび6.3.x)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

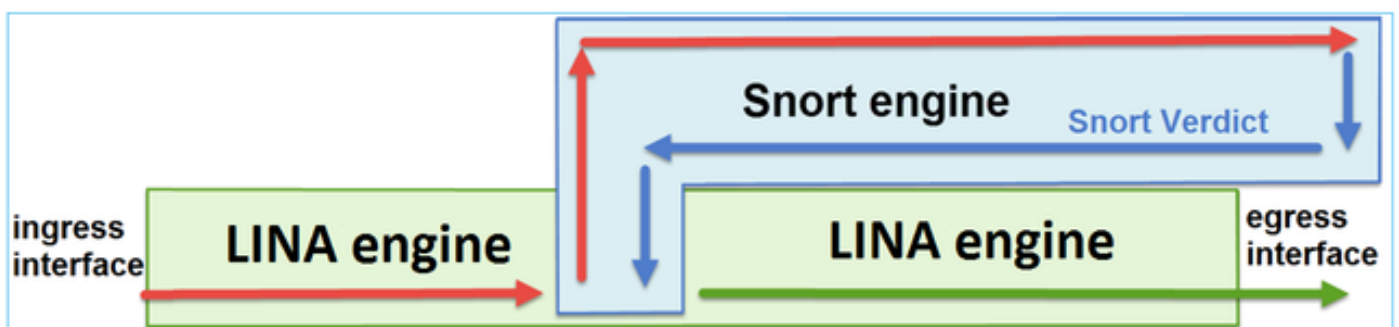
- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR2100, FPR4100, FPR9300
- VMware (ESXi)、Amazon Web Services (AWS)、カーネルベース仮想マシン (KVM)
- FTDソフトウェアコード6.2.x以降

背景説明

FTDは、2つの主要なエンジンで構成される統合ソフトウェアイメージです。

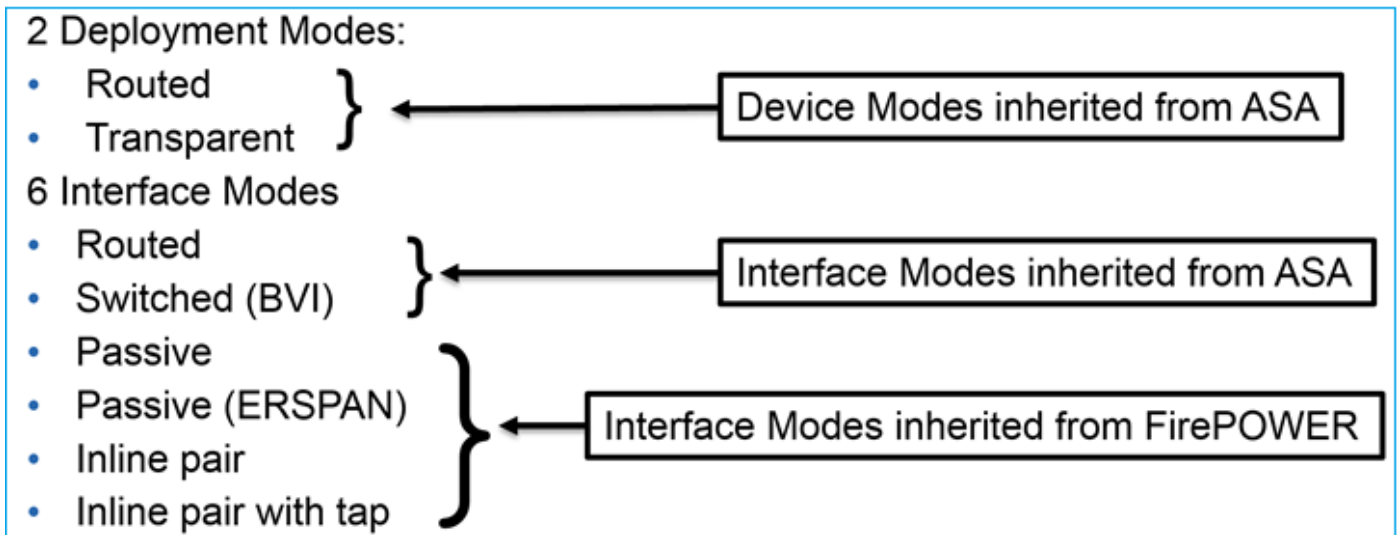
- LINA エンジン
- Snortエンジン

次の図に、2つのエンジンがどのように連携するかを示します。



- パケットが入インターフェイスに入り、LINA エンジンによって処理される
- FTD ポリシーで求められている場合、パケットが Snort エンジンによって検査される
- Snortエンジンは、パケットの判定を返します
- LINA エンジンは、Snort の判定に基づいてパケットをドロップまたは転送する

図に示すように、FTDは2つの導入モードと6つのインターフェイスモードを提供します。



注：単一のFTDアプライアンスで複数のインターフェイスモードを混在させることができます。

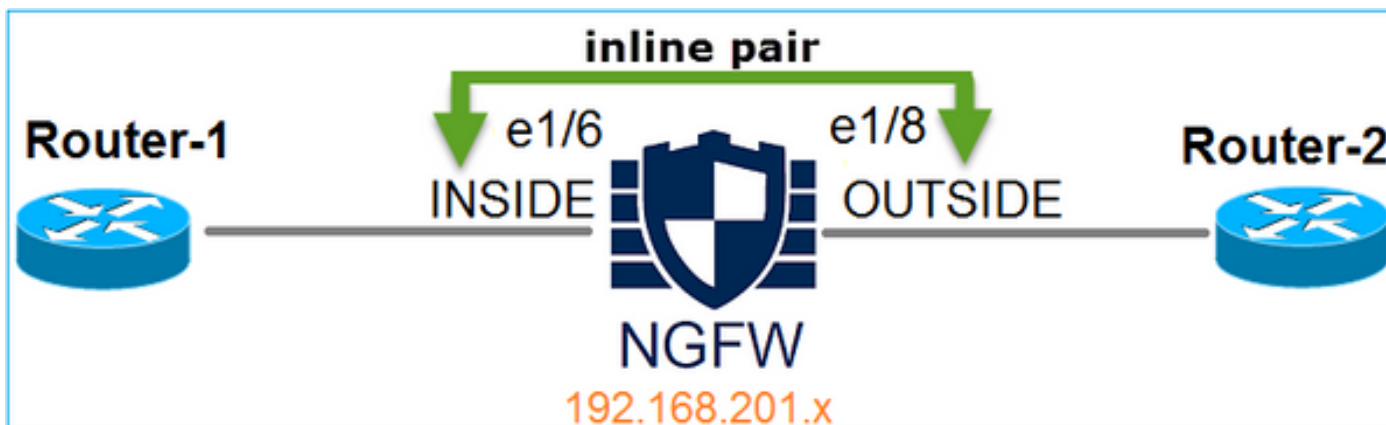
FTD のさまざまな展開モードおよびインターフェイスモードの概要を次に示します。

FTD インターフェイスモード	FTD 展開モード	説明	トラフィックのドロップの可否
Routed	Routed	LINAエンジンおよびSnortエンジンのフルチェック	Yes
交換された	トランスペアレント	LINAエンジンおよびSnortエンジンのフルチェック	Yes
インライン ペア	ルーテッドまたはトランスペアレント	部分的なLINAエンジンおよび完全なSnortエンジンのチェック	Yes
タップ付きインライン ペア	ルーテッドまたはトランスペアレント	部分的なLINAエンジンおよび完全なSnortエンジンのチェック	いいえ
Passive	ルーテッドまたはトランスペアレント	部分的なLINAエンジンおよび完全なSnortエンジンのチェック	いいえ

パッシブ (ERSPAN)	Routed	部分的なLINAエンジンおよび完全なSnortエンジンのチェック	いいえ
--------------------	--------	----------------------------------	-----

FTDでのインラインペアインターフェイスの設定

ネットワーク図



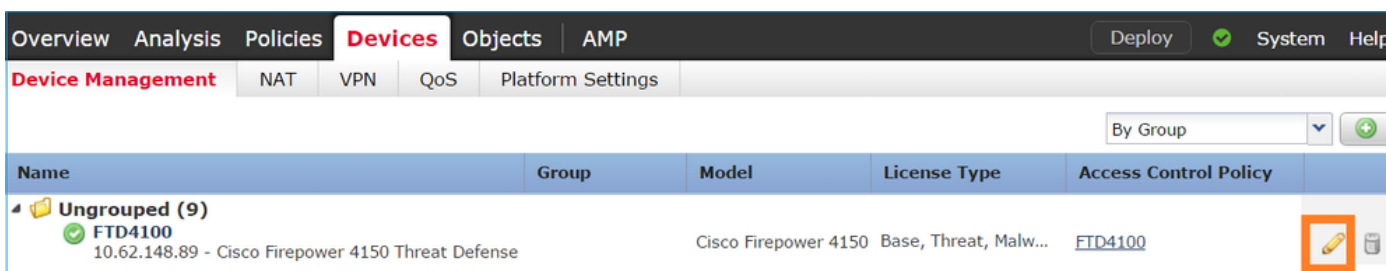
Requirement

次の要件に従って、インラインペアモードで物理インターフェイスe1/6およびe1/8を設定します。

インターフェイス	e1/6	e1/8
[名前(Name)]	INSIDE	OUTSIDE
セキュリティゾーン	INSIDE_ZONE	OUTSIDE_ZONE
インラインセット名	Inline-Pair-1	
インラインセットMTU	1,500	
フェールセーフ	Enabled	
リンクステートの伝達	Enabled	

解決方法

ステップ1：個々のインターフェイスに設定するには、Devices > Device Managementに移動し、適切なデバイスを選択して、図に示すようにEditを選択します。



次に、図に示すように、インターフェイスのNameとEnabledにチェックマークを付けます。

Edit Physical Interface

Mode:

Name: Enabled Management Only


Security Zone:

Description:

General | IPv4 | IPv6 | Advanced | Hardware Configuration

MTU: (64 - 9188)

Interface ID:

 注: 「Name」はインターフェイスのnameifです。







インターフェイス Ethernet1/8 も同様に設定します。最終的な結果は次の図のようになります。

Overview Analysis Policies **Devices** Objects AMP System Help **admin**

Device Management NAT VPN QoS Platform Settings

FTD4100
Cisco Firepower 4150 Threat Defense

Devices Routing **Interfaces** Inline Sets DHCP Add Interfaces

...	Interface	Logical Name	Type	Security Zo...	MAC Address (Active/...	IP Address	
<input checked="" type="checkbox"/>	 Ethernet1/6	INSIDE	Physical				
<input checked="" type="checkbox"/>	 Ethernet1/7	diagnostic	Physical				
<input checked="" type="checkbox"/>	 Ethernet1/8	OUTSIDE	Physical				

ステップ 2: インラインペアを設定します。

図に示すように、Inline Sets > Add Inline Setの順に移動します。

Overview Analysis Policies **Devices** Objects AMP Deploy System Help admin

Device Management NAT VPN QoS Platform Settings

FTD4100

Cisco Firepower 4150 Threat Defense

Save Cancel

Devices Routing Interfaces **Inline Sets** DHCP

Add Inline Set

Name	Interface Pairs
No records to display	

ステップ 3 : 図に示すように、要件に従って一般設定を行います。

Add Inline Set

General Advanced

Name*: Inline-Pair-1

MTU*: 1500

FailSafe:


Available Interfaces Pairs

- INSIDE<->OUTSIDE

Selected Interface Pair

INSIDE<->OUTSIDE

Add

 注 : フェールセーフを使用すると、インターフェイスバッファがいっぱいになった場合 (通常はデバイスが過負荷またはSnortエンジンが過負荷になっている場合) に、トラフィックがインラインペアを非検査で通過できるようになります。インターフェイス バッファ サイズは動的に割り当てられます。

ステップ 4 : 図に示すように、Advanced SettingsのPropagate Link Stateオプションを有効にします。

Add Inline Set

General

Advanced

Tap Mode:

Propagate Link State:

Strict TCP Enforcement:

リンク ステート プロパゲーションにより、インライン セットのいずれかのインターフェイスがダウンした場合に、インライン インターフェイス ペアのもう一方のインターフェイスが自動的にダウンします。

ステップ 5 : 変更を保存して展開します。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

FTD CLIからインラインペアの設定を確認します。


解決方法

FTD CLIにログインし、インラインペアの設定を確認します。

```
> 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
```

```
>
```

 注：ブリッジグループIDは0以外の値です。ただし、タップモードがオンになっている場合は0になります。

インターフェイスと名前の情報を確認します。

```
<#root>
```

```
>
```

```
show nameif
```

Interface	Name	Security
Ethernet1/6	INSIDE	0
Ethernet1/7	diagnostic	0
Ethernet1/8	OUTSIDE	0

```
>
```

インターフェイスのステータスを確認します。

```
<#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

物理インターフェイス情報を確認します。

```
<#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のインラインペアインターフェイスの動作の確認

このセクションでは、インラインペアの動作を確認するための次の検証チェックについて説明し

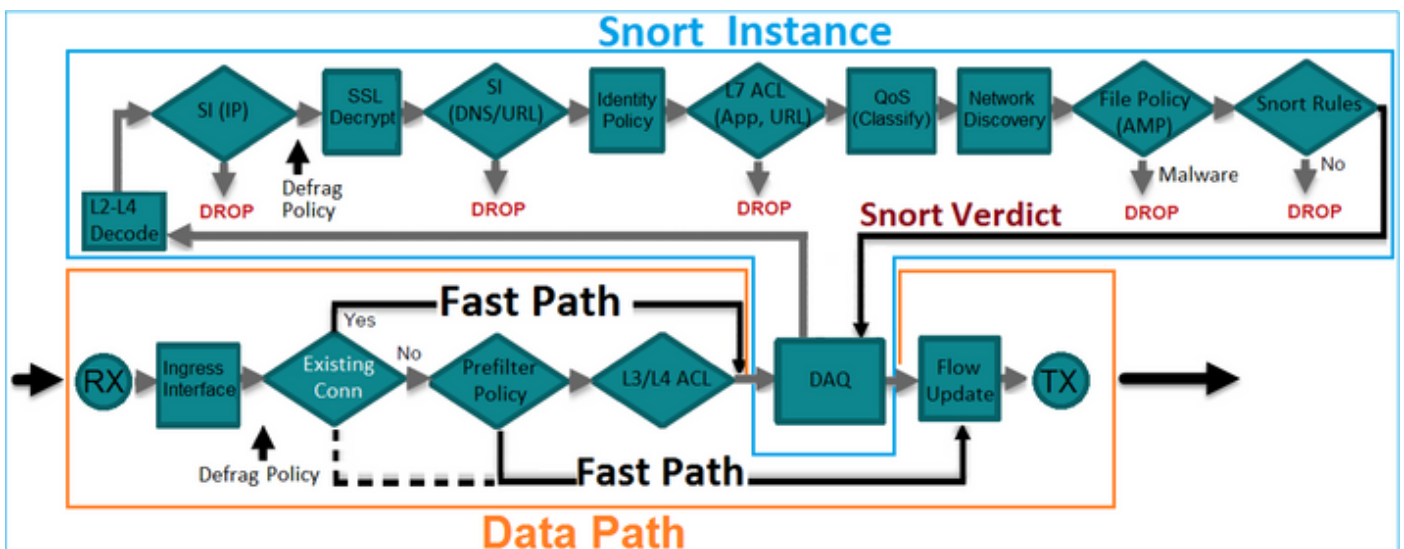
ます。

- 検証1.パケットトレーサの使用
- 検証2.トレースによるキャプチャを有効にし、インラインペアを介してTCP同期/確認応答 (SYN/ACK)パケットを送信します
- 検証3.ファイアウォールエンジンデバッグを使用したFTDトラフィックの監視
- 検証4.リンクステートプロパゲーション機能の確認
- 検証5.スタティックネットワークアドレス変換(NAT)の設定

解決方法

アーキテクチャの概要

2つのFTDインターフェイスがインラインペアモードで動作している場合は、図に示すようにパケットが処理されます。

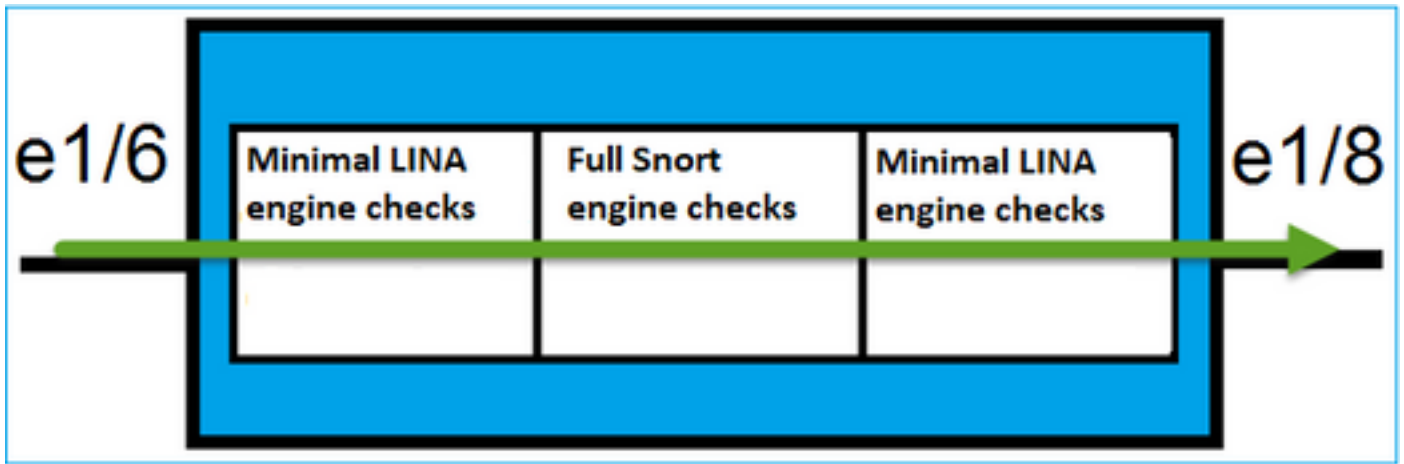


注：インラインペアセットのメンバにできるのは物理インターフェイスだけです

基本理論

- インラインペアを設定すると、2つの物理インターフェイスが内部的にブリッジされます
- 従来のインライン侵入防御システム(IPS)に非常によく似ている
- ルーテッドまたはトランスペアレント展開モードで使用できる。
- ほとんどのLINAエンジン機能 (NAT、ルーティングなど) は、インラインペアを通過するフローには使用できません
- 中継トラフィックをドロップできる。
- Snortエンジンのフルチェックとともに、いくつかのLINAエンジンチェックが適用されます

最後の点は、次の図のように視覚化できます。



検証1.Packet-Tracerの使用

次のパケットトレーサの出力では、インラインペアを通過するパケットをエミュレートしていますが、重要な点が強調表示されています。

```
<#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 ingress 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

>

検証2. インラインペアを使用したTCP SYN/ACKパケットの送信

Scapyなどのユーティリティを作成するパケットを使用して、TCP SYN/ACKパケットを生成できます。次の構文では、SYN/ACKフラグが有効な3つのパケットが生成されます。

```
<#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 CLIでこのキャプチャを有効にし、いくつかのTCP SYN/ACKパケットを送信します。

```
<#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
```

```
>
```

FTDを介してパケットを送信した後、作成された接続を確認できます。

```
<#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
```

```
>
```

 注:bフラグ：従来のASAは、TCP状態バイパスが有効になっていない限り、非要請SYN/ACKパケットをドロップします。インラインペアモードのFTDインターフェイスは、TCP状態バイパスモードのTCP接続を処理し、既存の接続に属さないTCPパケットをドロップしません。

 注：Nフラグ：パケットはFTD Snortエンジンによって検査されます。

FTDを通過する3つのパケットを確認できるため、キャプチャはこれを証明します。

```
<#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パケットがFTDデバイスから出力されます。

```
<#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
>
```

最初のキャプチャパケットのトレースによって、Snortエンジンの判定などの追加情報が明らかになります。

```
<#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
>
```

2番目にキャプチャされたパケットのトレースでは、パケットが現在の接続に一致するため、ACLチェックをバイパスするものの、Snortエンジンによって検査されることが示されています。

```
<#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

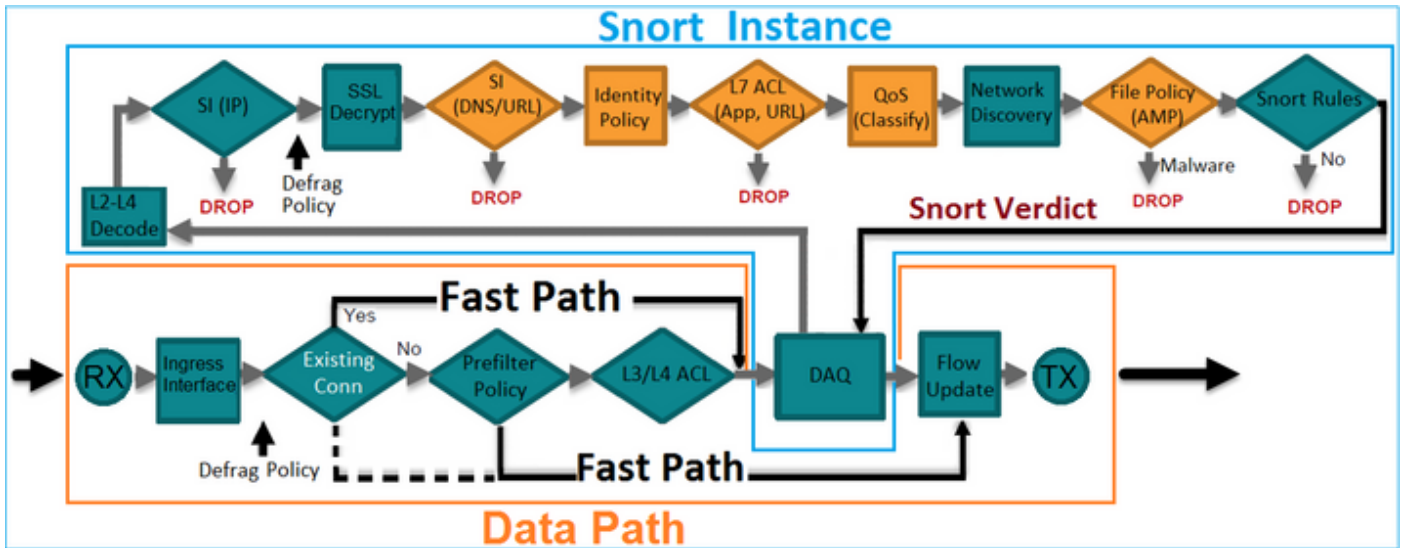
Phase: 6
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

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

1 packet shown
>

検証3.許可されたトラフィックのファイアウォールエンジンデバッグ

ファイアウォールエンジンのデバッグは、図に示すように、アクセスコントロールポリシーなどのFTD Snortエンジンの特定のコンポーネントに対して実行されます。



インラインペア経由でTCP SYN/ACKパケットを送信すると、デバッグ出力に次のように表示されます。

```
<#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
```

検証4. リンクステートプロパゲーションの確認

FTDのバッファログを有効にし、e1/6インターフェイスに接続されたスイッチポートをシャットダウンします。FTD CLIで、両方のインターフェイスがダウンしたことを確認する必要があります。

```
<#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 のログは次のとおりです。

```
<#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 ステータスには、2つのインターフェイスメンバーの状態が示されます。

<#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

>

2つのインターフェイスのステータスの違いを確認します。

<#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 インターフェイスの状態は次のとおりです。

<#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

>

スイッチポートを再度有効にすると、FTDログに次のように表示されます。

```
<#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) brid
```

```
>
```

検証5.スタティックNATの設定

解決方法

NATは、インラインモード、インラインタップモード、またはパッシブモードで動作するインターフェイスではサポートされません。

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

インラインペアインターフェイスモードでのパケットのブロック

ブロックルールを作成し、FTDインラインペアを介してトラフィックを送信し、図に示すように動作を確認します。

Rules														Security Intelligence	HTTP Responses	Advanced	
#	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				
▼ Default - FTD4100 (-)																	
There are no rules in this section. Add Rule or Add Category																	
Default Action														Intrusion Prevention: Balanced Security and Connectivity			

解決方法

トレースでのキャプチャを有効にして、FTD のインライン ペア経由で SYN/ACK パケットを送信します。トラフィックがブロックされず。

```
<#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
```

トレースを使用すると、パケットは次の内容を明らかにします。

```
<#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 ingresses 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

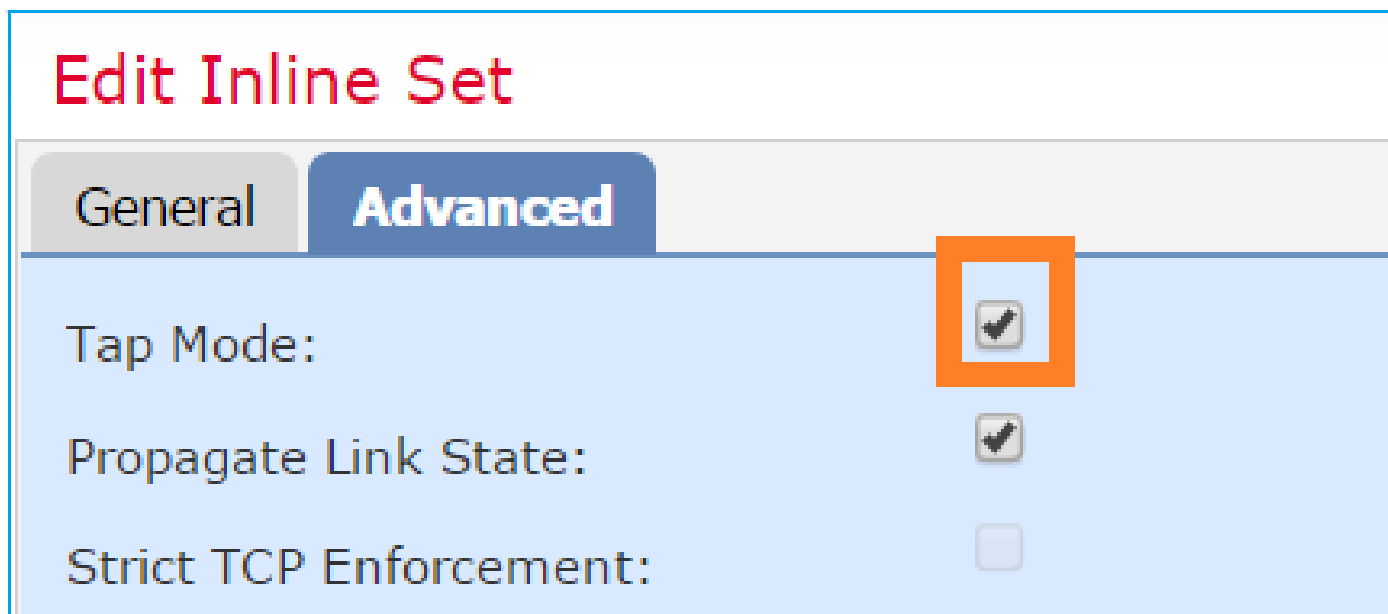
このトレースでは、パケットがFTD LINAエンジンによってドロップされ、FTD Snortエンジンに転送されなかったことがわかります。

タップによるインラインペアモードの設定

インラインペアでタップモードを有効にします。

解決方法

図に示すように、Devices > Device Management > Inline Sets > Edit Inline Set > Advancedの順に移動し、Tap Modeを有効にします。



検証

```
<#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
```

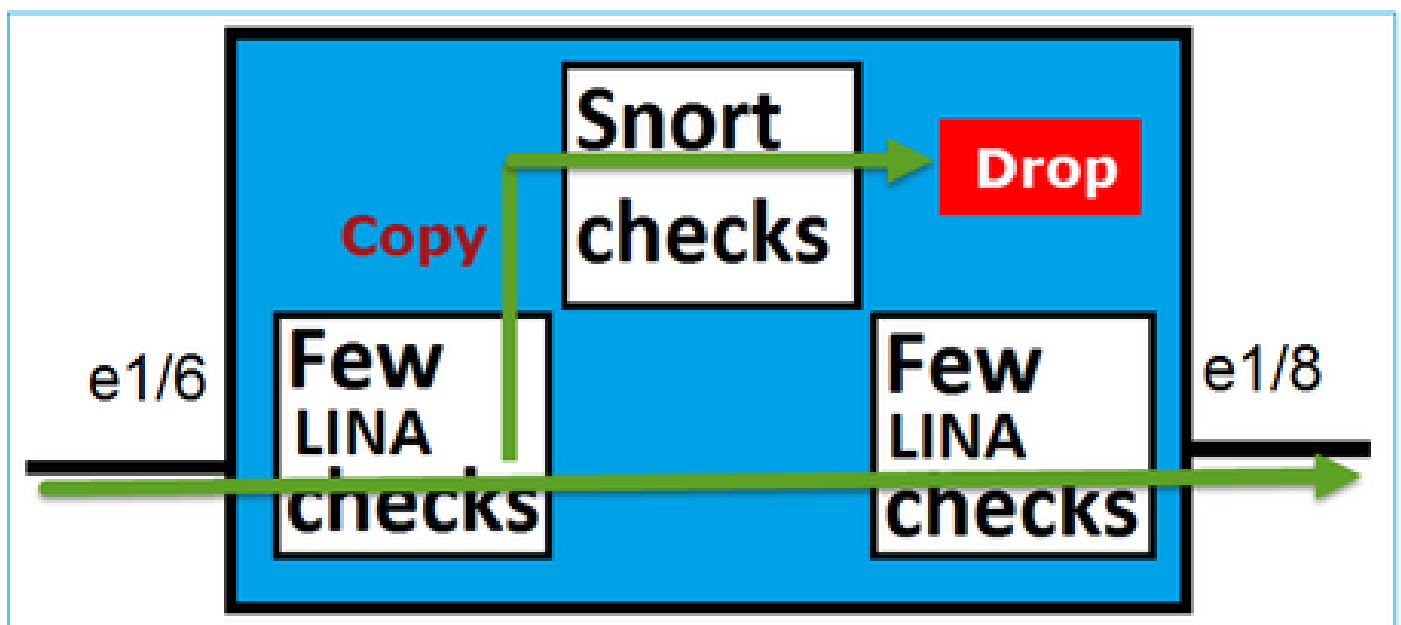
>

FTDのタップ付きインラインペアのインターフェイス動作の確認

基本理論

- タップ2を使用してインラインペアを設定すると、物理インターフェイスは内部でブリッジされます
- ルーテッドまたはトランスペアレント展開モードで使用できる
- ほとんどのLINAエンジン機能 (NAT、ルーティングなど) は、インラインペアを通過するフローには使用できません
- 実際のトラフィックはドロップできない。
- 実際のトラフィックのコピーに対するSnortエンジンのフルチェックとともに、いくつかのLINAエンジンチェックが適用されます

最後の点は次の図のようになります。



タップ付きインラインペアのモードでは、中継トラフィックはドロップされません。パケットのトレースを使用して、これを確認します。

```
<#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 ingressd 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

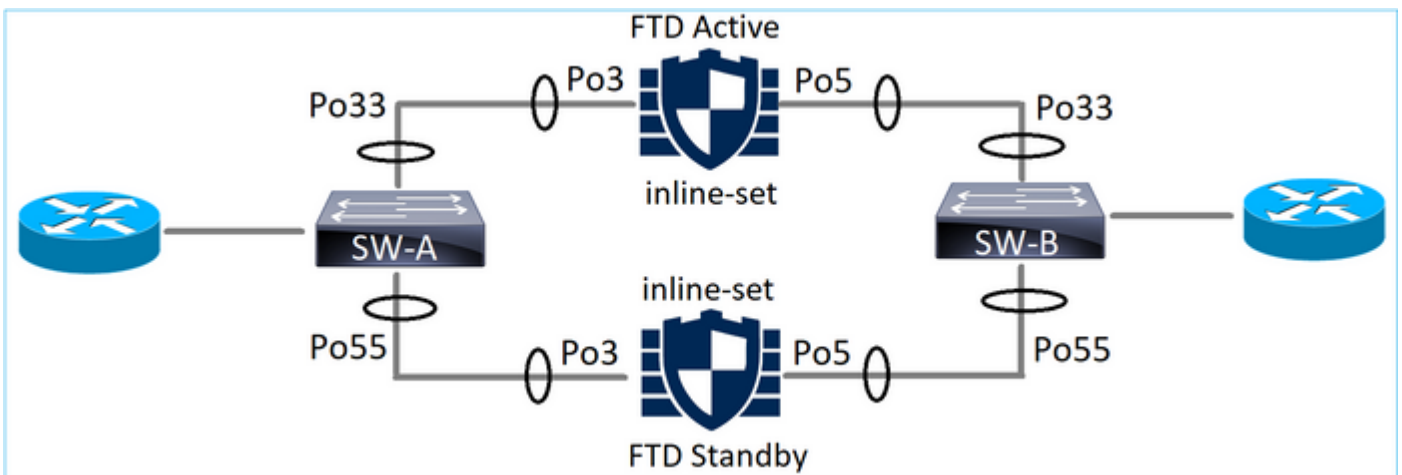
>

インラインペアとEtherchannel

Etherchannelを使用してインラインペアを設定するには、次の2つの方法があります。

1. FTDで終端されたEtherChannel
2. EtherchannelはFTDを通過します (FXOSコード2.3.1.3以降が必要) 。

FTDで終端されたEtherChannel



SW-Aの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-Bの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)
```

トラフィックは、MACアドレスラーニングに基づいてアクティブFTDを介して転送されます。

<#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

FTDのインラインセット :

<#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]:

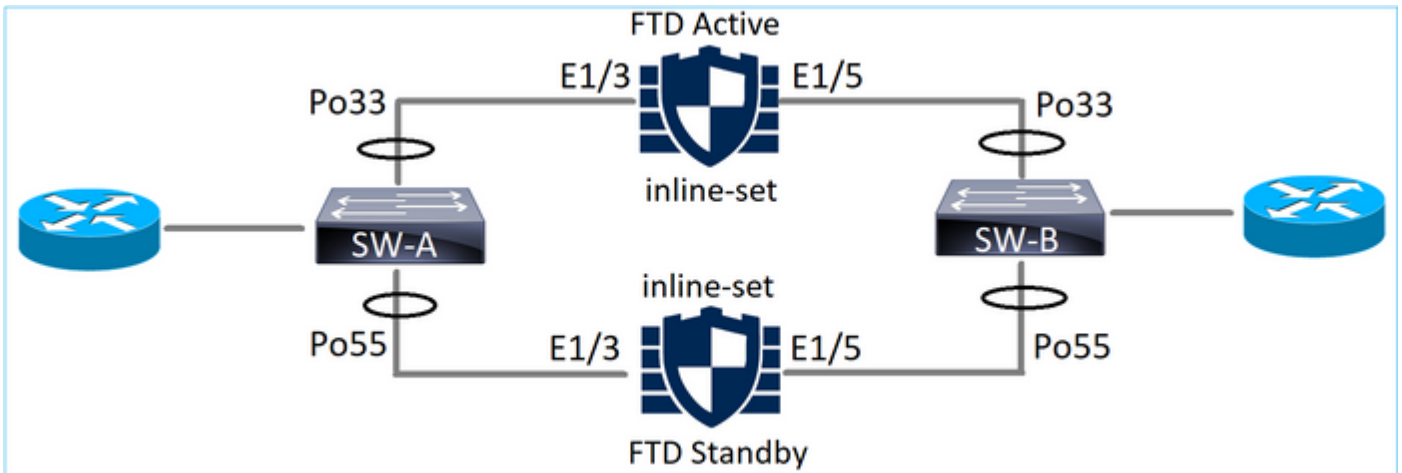
```
Interface: Port-channel3 "INSIDE"
Current-Status: UP
Interface: Port-channel5 "OUTSIDE"
Current-Status: UP
```

Bridge Group ID: 775

 注:FTDフェールオーバーイベントの場合、トラフィックの停止は、主にスイッチがリモー

 トピアのMACアドレスを学習するのにかかる時間に依存します。

FTD経由のEtherChannel



SW-AのEtherChannel:

```
<#root>
```

```
SW-A#
```

```
show etherchannel summary | i Po33|Po55
```

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

```
(1)
```

スタンバイFTDを通過するLACPパケットはブロックされます。

```
<#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-Bの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)

トラフィックは、MACアドレスラーニングに基づいてアクティブFTDを介して転送されます。

<#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

FTDのインラインセット :

<#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

 注意：このシナリオでは、FTDフェールオーバーイベントの場合、コンバージェンス時間は主にEtherchannel LACPネゴシエーションに依存し、停止にかかる時間が非常に長くなる可能性があります。EtherchannelモードがON (LACPなし) の場合、コンバージェンス時間はMACアドレスラーニングによって異なります。

トラブルシュート

現在のところ、この設定に関する特定の情報はありません。

比較：インラインペアとタップ付きインラインペア

	インライン ペア	タップ付きインライン ペア
show inline-set	<pre>> show inline-setの順に選択します。 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]: インターフェイス : Ethernet1/6 「 INSIDE」 現在のステータス : UP インターフェイス : Ethernet1/8 「 OUTSIDE」 現在のステータス : UP ブリッジグループID:509 ></pre>	<pre>> show inline-setの順に選択します。 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]: インターフェイス : Ethernet1/6 「 INSIDE」 現在のステータス : UP インターフェイス : Ethernet1/8 「 OUTSIDE」 現在のステータス : UP ブリッジグループID:0 ></pre>

<p>show interface</p>	<pre>> 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インターフェイスモード : イン ライン、インラインセット : インライン ペア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インターフェイスモード : イン ライン、インラインセット : インライン ペア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</pre>	<pre>> 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インターフェイスモード : イン ラインタップ、インラインセット : イン ラインペア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 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インターフェイスモード : イン ラインタップ、インラインセット : イン ラインペア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</pre>
-----------------------	---	---

	<p>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 ></p>	<p>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 ></p>
<p>ブロックルールを使用してパケットを処理するには</p>	<p>> show capture CAPI packet-number 1 traceの順に選択します</p> <p>3 packets captured</p> <p>1: 16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192 フェーズ : 1 タイプ : CAPTURE Subtype: 結果 : 許可 Config: Additional Information: MAC Access list</p> <p>フェーズ : 2 タイプ : ACCESS-LIST Subtype: 結果 : 許可 Config: Implicit Rule Additional Information: MAC Access list</p> <p>フェーズ : 3 タイプ : NGIPS-MODE サブタイプ : ngips-mode 結果 : 許可 Config: Additional Information: NGIPSモードに設定されたインターフェイスに入力されたフローとNGIPSサービスが適用されます</p> <p>フェーズ : 4 タイプ : ACCESS-LIST サブタイプ : ログ</p>	<p>> show capture CAPI packet-number 1 traceの順に選択します</p> <p>3 packets captured</p> <p>1: 16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) win 8192 フェーズ : 1 タイプ : CAPTURE Subtype: 結果 : 許可 Config: Additional Information: MAC Access list</p> <p>フェーズ : 2 タイプ : ACCESS-LIST Subtype: 結果 : 許可 Config: Implicit Rule Additional Information: MAC Access list</p> <p>フェーズ : 3 タイプ : NGIPS-MODE サブタイプ : ngips-mode 結果 : 許可 Config: Additional Information: NGIPSモードに設定されたインターフェイスに入力されたフローとNGIPSサービスが適用されます</p> <p>フェーズ : 4 タイプ : ACCESS-LIST サブタイプ : ログ 結果 : ドロップされる</p>

	<pre> 結果 : 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 : アクセスポリシー : FTD4100 – 必須/1 access-list CSM_FW_ACL_ remark rule- id 268441600: L4 RULE: Rule 1 Additional Information: Result: 入インターフェイス : 内部 入ステータス : アップ input-line-status:up (入力回線ステータ ス : アップ) アクション : ドロップ ドロップ理由 : (acl-drop)設定されたル ールによってフローが拒否されます 1 packet shown > </pre>	<pre> 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 : アクセスポリシー : FTD4100 – 必須/1 access-list CSM_FW_ACL_ remark rule- id 268441600: L4 RULE: Rule 1 Additional Information: Result: 入インターフェイス : 内部 入ステータス : アップ input-line-status:up (入力回線ステータ ス : アップ) アクション : アクセスリストはドロップ されますが、パケットはインラインタッ プにより転送されます 1 packet shown > </pre>
--	--	---

要約

- インラインペアモードを使用すると、パケットは主にFTD Snortエンジンを通過します
- TCP ステートバイパス モードの TCP 接続が処理される。
- FTD LINAエンジンの観点からは、ACLポリシーが適用されます
- インラインペアモードが使用されている場合、パケットはインラインで処理されるためブロックできません
- タップモードが有効な場合、実際のトラフィックが変更されずにFTDを通過する間、パケットのコピーが内部で検査され、ドロップされます

関連情報

- [Cisco Firepower NGFW](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。