インライン ペア モードの Firepower Threat Defense インターフェイスの設定

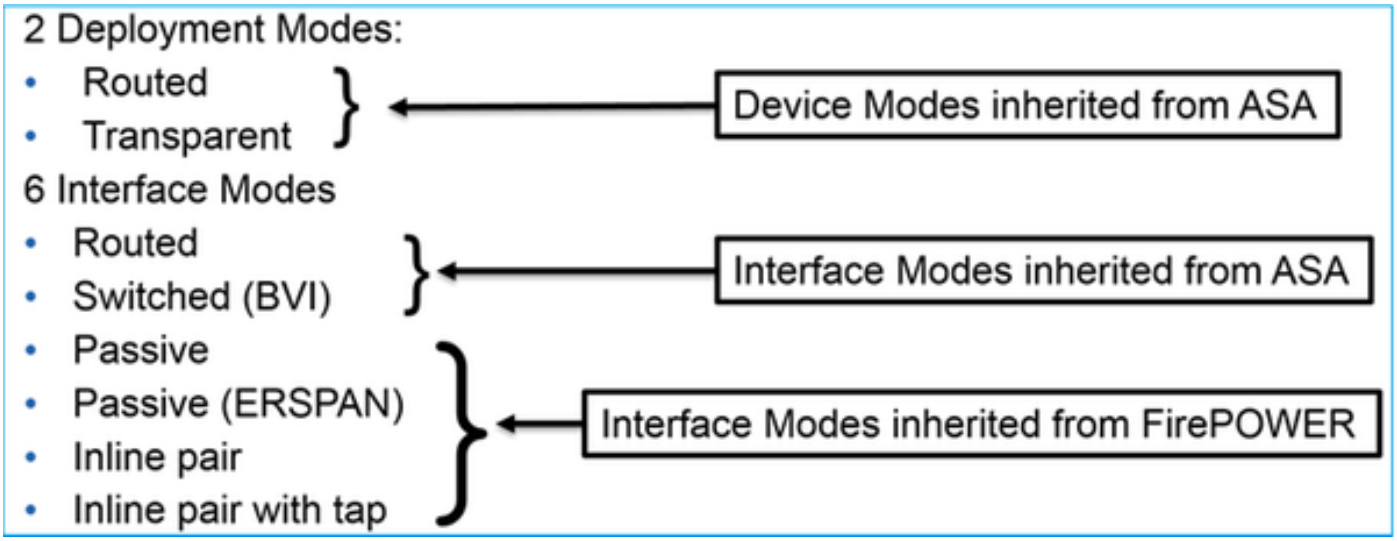
目次

概要

Firepower Threat Defense（FTD）は次のプラットフォームでインストールすることができる統一されたソフトウェア イメージです:

- ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X
- ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X
- FPR4100、FPR9300
- VMware（ESXi）
- アマゾン Web サービス（AW）
- KVM
- ISR ルータモジュール

FTD は 2 つの配置モードおよび 6 つのインターフェイス モードを提供します



注: sigle FTD アプライアンスのインターフェイス モードを混合できます

さまざまな FTD 配備およびインターフェイス モードのハイレベルな概要はここにあります:

FTD インターフェイス モード	FTD 配置モード	説明	トラフィックは廃棄することができます
Routed	Routed	完全な ASA エンジンおよび Snort エンジン チェック	○
交換	トランスペアレント	完全な ASA エンジンおよび Snort エンジン チェック	○
インライン ペア	経路選択済みか透過的な	部分的な ASA エンジンおよび完全な Snort エンジン チェック	○
タップとのインライン ペア	経路選択済みか透過的な	部分的な ASA エンジンおよび完全な Snort エンジン チェック	なし
パッシブ	経路選択済みか透過的な	部分的な ASA エンジンおよび完全な Snort エンジン チェック	なし
受動態（ERSPAN）	Routed	部分的な ASA エンジンおよび完全な Snort エンジン チェック	なし

目標

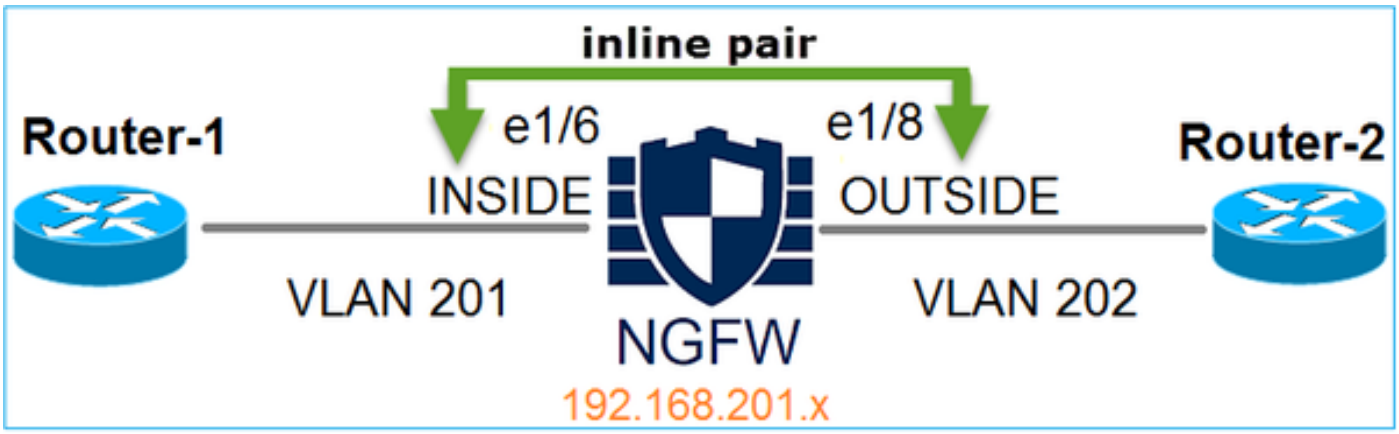
この資料の目標はにあります:

- 設定を示せば FTD インライン ペアのオペレーションはインターフェイスします

使用するコンポーネント

- Firepower 4150 実行 FTD コード 6.1.0.x
- 6.1.0.x を実行する Firepower Management Center（ FMC ）

トポロジ



FTD のインライン ペア インターフェイスの設定

Requirement

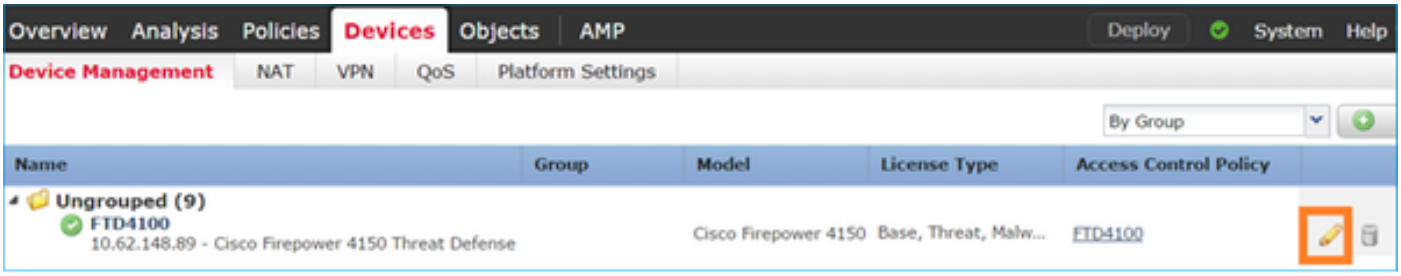
次の必要条件ごとのインライン ペア モードの物理インターフェイス e1/6 および e1/8 を設定して下さい:

interface	e1/6	e1/8
名前	内部	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	1500	
フェイル・ セイフ	[Enabled]	
プロパゲート リンク状態	[Enabled]	

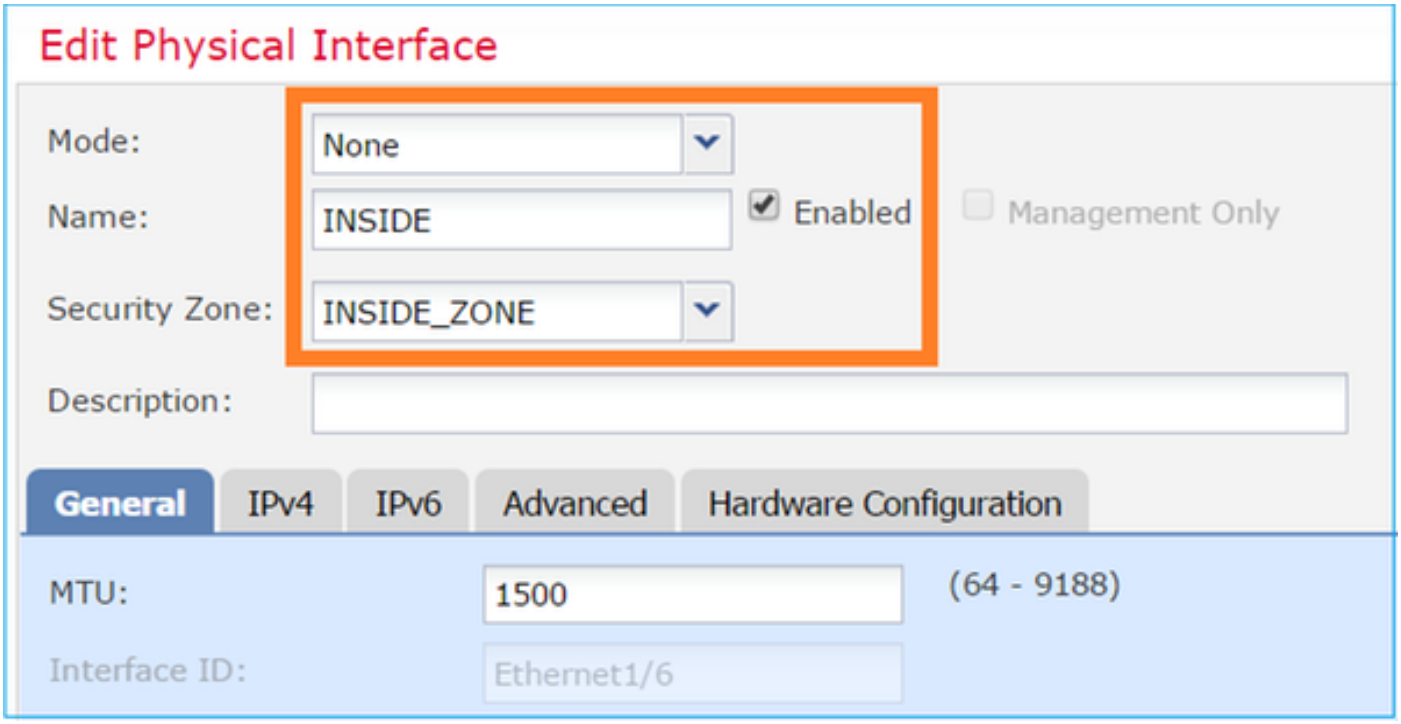
解決策

ステップ 1 –個々のインターフェイスの設定

デバイス > デバイス管理へのナビゲートは、適切なデバイスを選択し、アイコンを『Edit』 をクリック します:

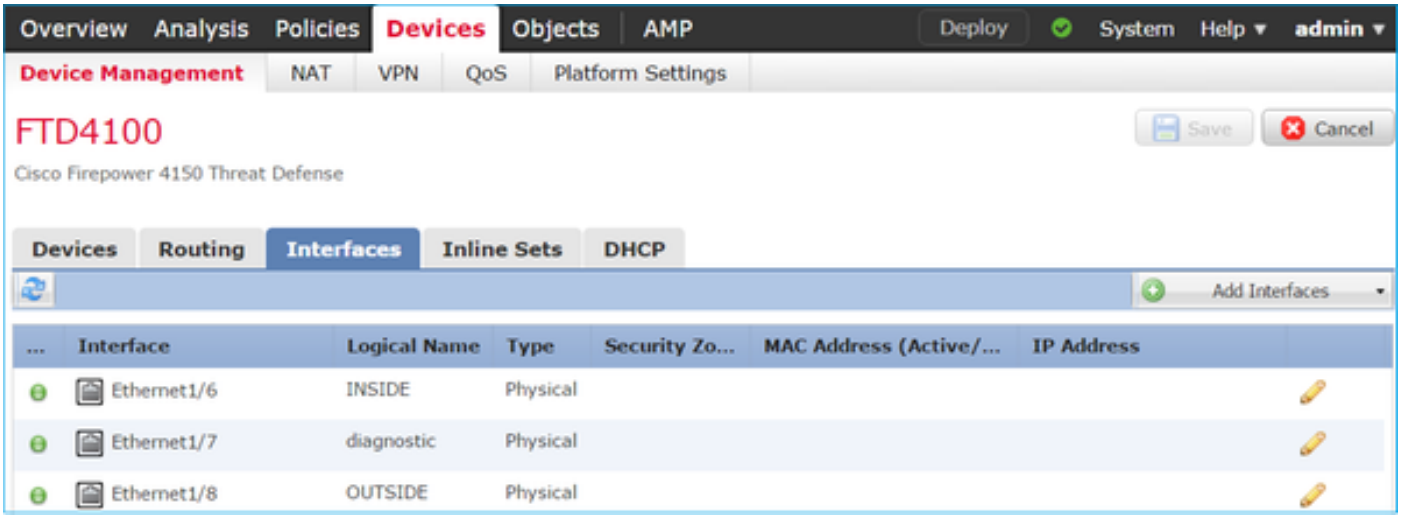


名前を規定 し、インターフェイスをイネーブルに設定して下さい:



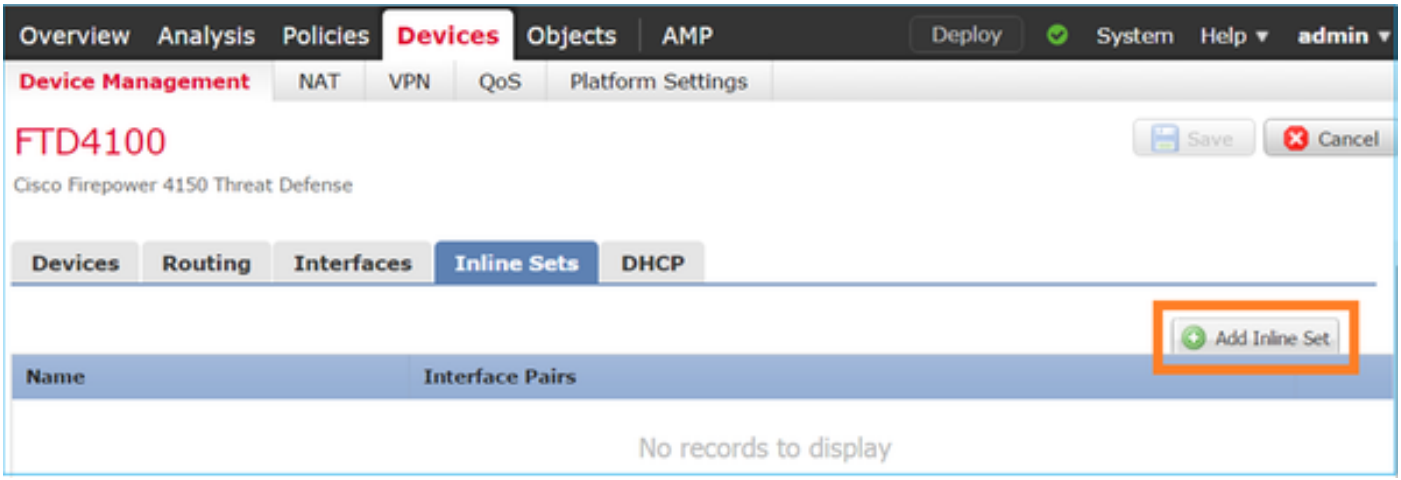
名前はインターフェイスの **nameif** です

同様にインターフェイス Ethernet1/8 のために。 最終結果:

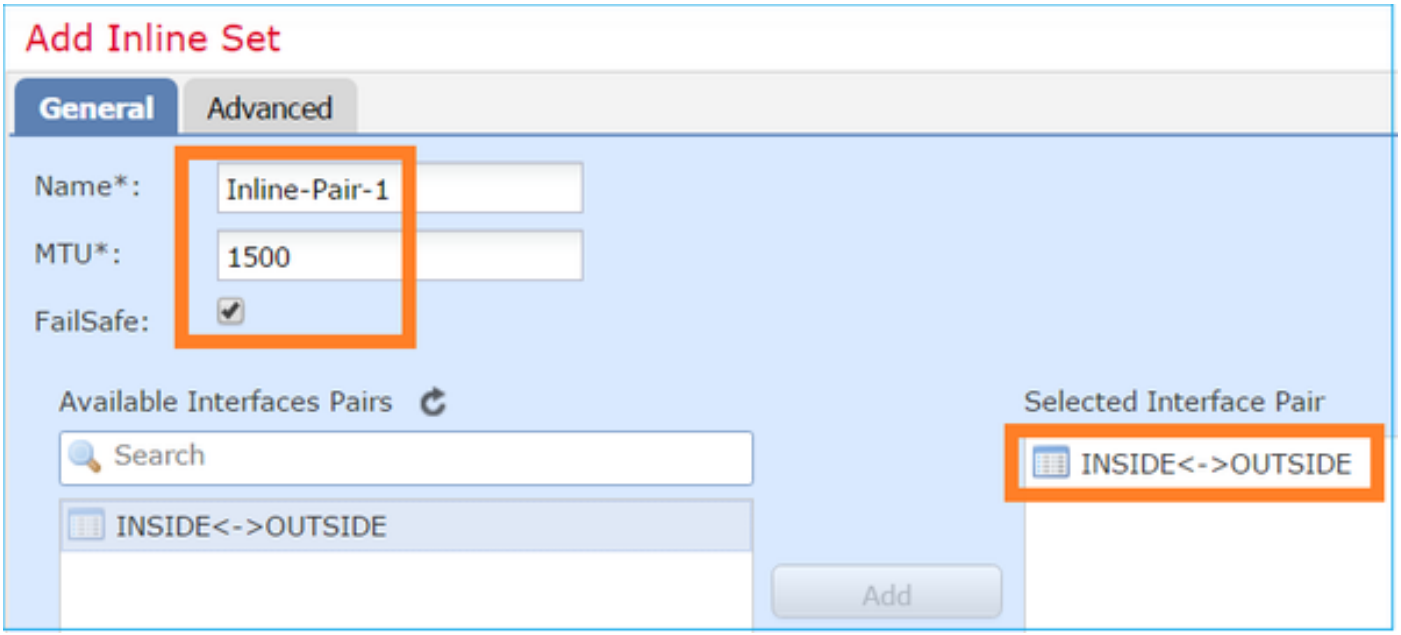


ステップ 2 –インライン ペアの設定

インライン セット タブへのナビゲートは**インライン セットを**『Add』 をクリック し、:

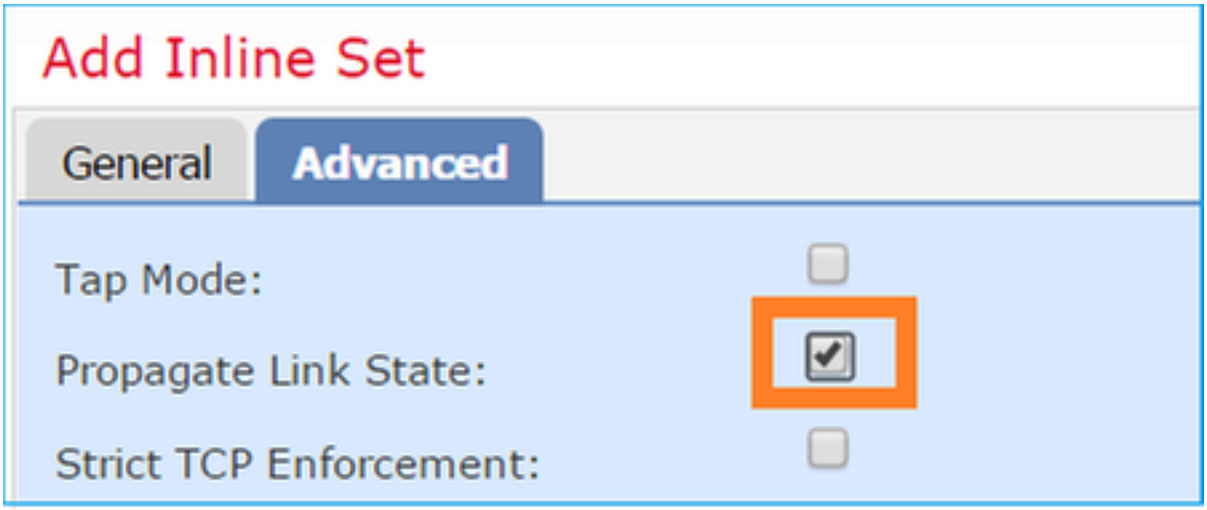


必要条件ごとの設定を設定して下さい:



インターフェイス バッファが完全なら**フェイル・ セイフ** パススルーにトラフィックに uninspected インライン ペアを与えます (一般的に見られてデバイスが過剰になるまたは Snort エンジンは) とき過剰になります。 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 。

イネーブル「**プロパゲート リンク状態**」オプション:



リンク状態伝搬は自動的にインラインに設定 されるのインターフェイスの 1 つがダウン状態になるときインライン インターフェイス ペアの第 2 インターフェイスをダウンさせます。

変更を**保存し、展開して下さい**

インライン ペア インターフェイスコンフィギュレーションの確認

FTD CLI からのインライン ペア設定を確認して下さい

解決策

FTD CLI にログインし、インライン ペア設定を確認して下さい:

```
> 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: ザ・ ブリッジ グループ ID は 0 と別の値です。 タップ モードがにあれば 0 時です

インターフェイスおよびネーム情報:

```
> 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 ステータスの検証:

```
> 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 情報の検証:

```
> 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 インライン ペア インターフェイス オペレーションの検証

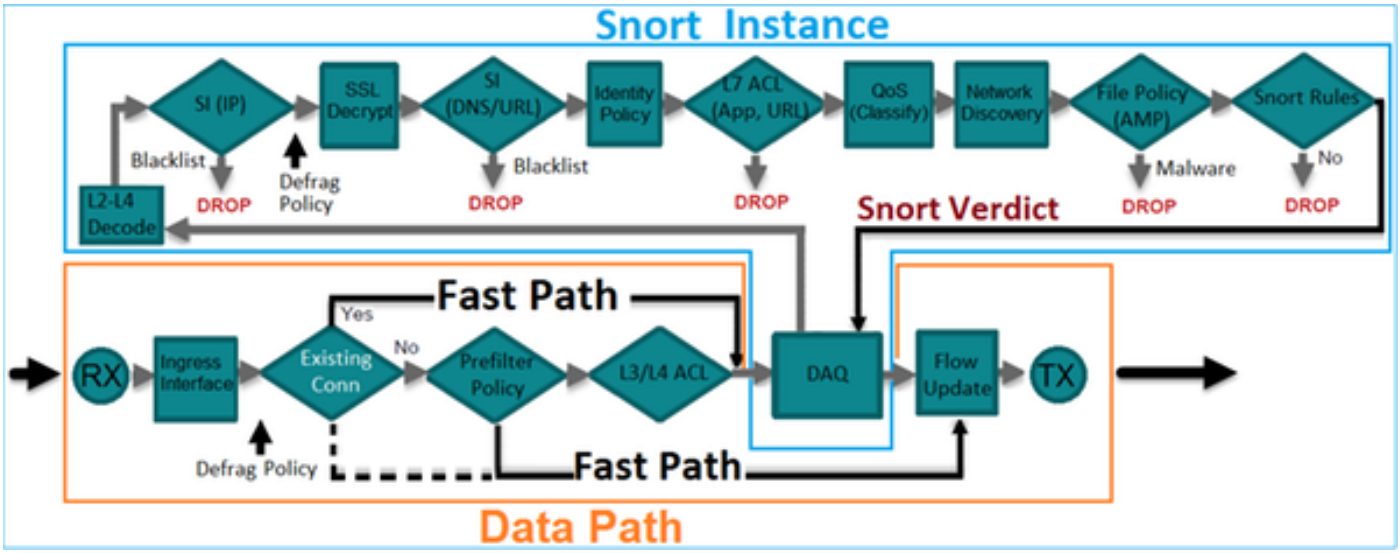
このセクションはインライン ペア オペレーションを確認するために次の確認チェックをカバーします:

- 確認 1 –パケット トレーサーの使用
- 確認 2 –トレースおよび TCP SYN/ACK パケットを送信 することのキャプチャをインライン ペアによって有効に します
- 確認 3 –ファイアウォール エンジン デバッグを使用した FTD トラフィックのモニタ
- 確認 4 –リンク州の伝搬 機能性の検証
- 確認 5 –スタティック NAT の設定

解決策

アーキテクチャーの概要

2 つの FTD インターフェイスがインライン ペア モードで動作するときパケットは次の通り処理されます:



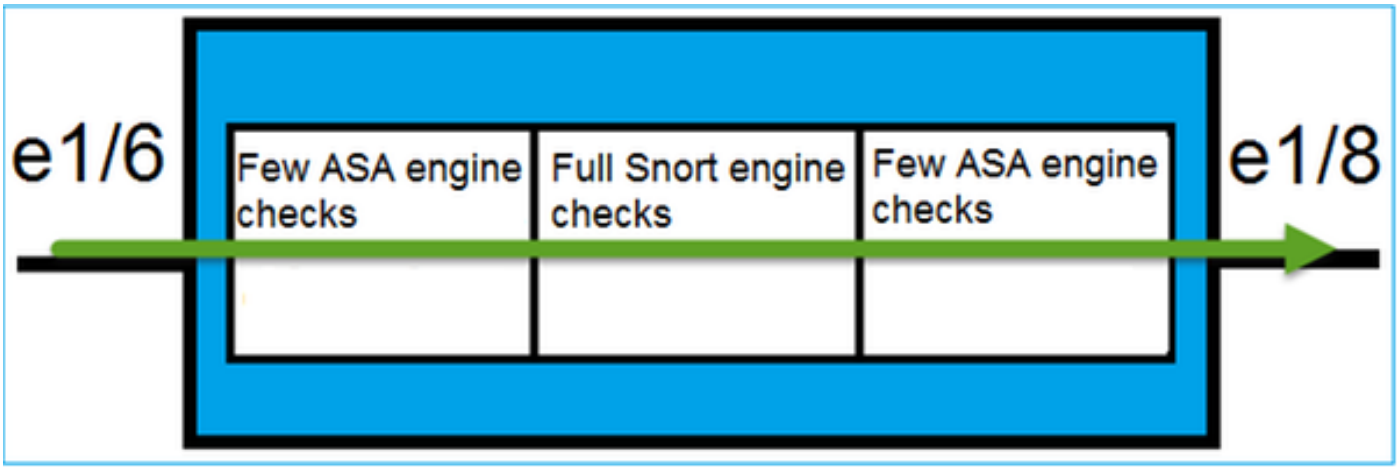
> **注:** 物理インターフェイスだけ設定 されるインライン ペアのメンバーである場合もあります

基本的 な 理論

- インライン ペアを設定するとき 2 つの物理インターフェイスは内部で繋がれます

- **標準的なインライン IPS** に非常に類似した
- **経路選択済み**か**透過的な配置モード**で利用可能
- ASA エンジン 機能 (NAT、ルーティング、L3/L4 ACL 等) のほとんどはインライン ペアを通過するフローのために**利用可能**ではないです
- トランジットトラフィックは**廃棄することができます**
- **少数の ASA エンジン** チェックは**完全な Snort エンジン** チェックと共に適用します

最後のポイントは次の通り視覚化することができます:



確認 1 –パケット トレーサーの使用

出力されるパケット トレーサーはここにありま横断するパケット強調表示される興味深いポイントとのインライン ペア エミュレートします:

```
> 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

>
```

確認 2 –インライン ペアによる TCP SYN/ACK パケットの送信

Scapy のようなユーティリティを細工 して いる TCP SYN/ACK パケットをパケットを使用して生成できます。 次の構文は有効に なった SYN/ACK フラグが付いている 3 つのパケットを生成します:

```
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 の次のキャプチャを有効に し、少数の TCP SYN/ACK パケットを送信して下さい:

```
> 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 によるパケットを送信 した後作成された接続を表示できます:

```
> 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 フラグ**: 標準的な ASA は TCP 州バイパスが有効に ならなかったら 非要請 SYN/ACK パケットを廃棄します。 インライン ペア モードの FTD インターフェイスは TCP 州バイパス モードの TCP 接続を処理し、現在の接続に属さない TCP パケットを廃棄しません
- **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

キャプチャは 3 つのパケットを FTD を横断することを次のように表示できるので上を証明します:

```
> 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 デバイスを終了する 3 つのパケット:

```
> 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 パケットをトレースすることは Snort エンジン評決のようなその他の情報を明らかにします:

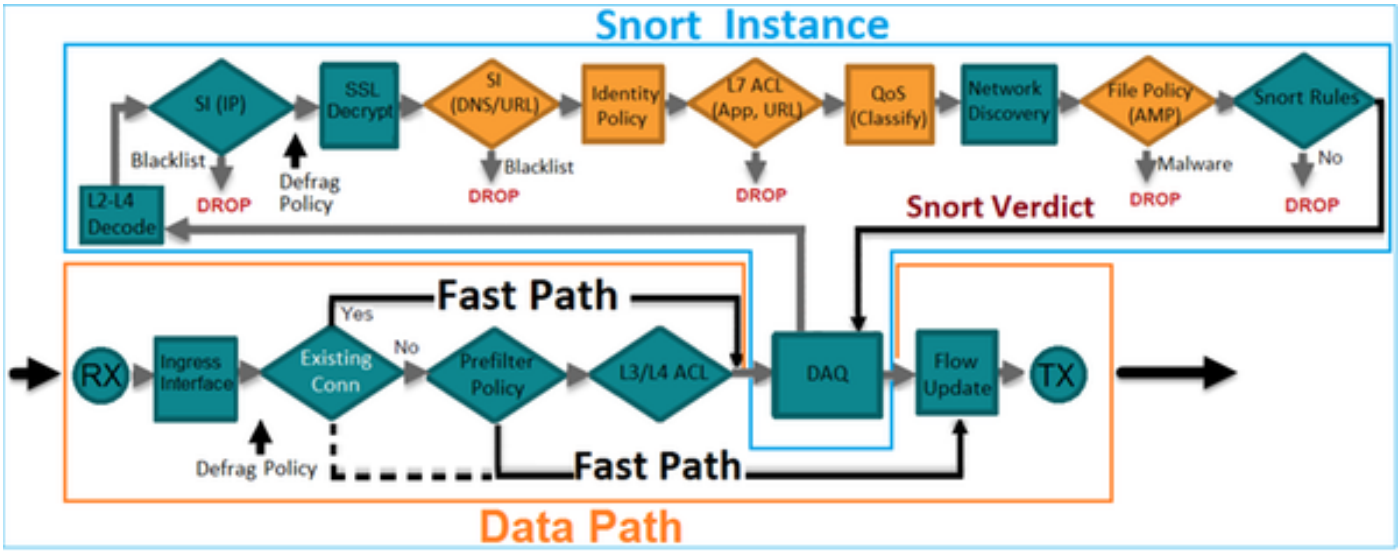
> **show capture CAPI packet-number 1 trace** 3 packets captured 1: 15:27:54.327146 192.168.201.50.20 > 192.168.201.60.80: **S** 0:0(0) **ack** 0 win 8192 Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: 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 >

第 2 キャプチャされるパケットをトレースすることは従って ACL チェックを一致する示しましたり、まだ Snort エンジンによってバイパスするがことをパケットが現在の接続とことを点検されます:

> **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 >

確認 3 –許可されたトラフィックのためのファイアウォール エンジン デバッグ

アクセスコントロール ポリシーのような FTD Snort エンジンの特定 の コンポーネントに対するファイアウォール エンジン デバッグ実行:



TCP SYN/ACK パケットをインライン ペアによって送信 するときデバッグ 出力で見ることができます:

```
> 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
```

確認 4 –リンク州の伝搬の検証

FTD を口グオンし、e1/6 インターフェイスに接続されるスイッチポート シャットダウンされるイネーブル バッファ。 FTD CLI でインターフェイスが両方ともダウン状態になったことがわかるはずです:

```
> 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 ログは示します:

```
> 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)
>
```

インライン設定 されたステータスは 2 人のインターフェイス メンバーの状態を示します:

```
> 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: 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に注意して下さい:

```
> 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
>
```

そして Ethernet1/8 インターフェイスのために:

```
> 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び有効にした後 FTD ログは示します:

```
> 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)
>
```

確認 5 –スタティック NAT の設定

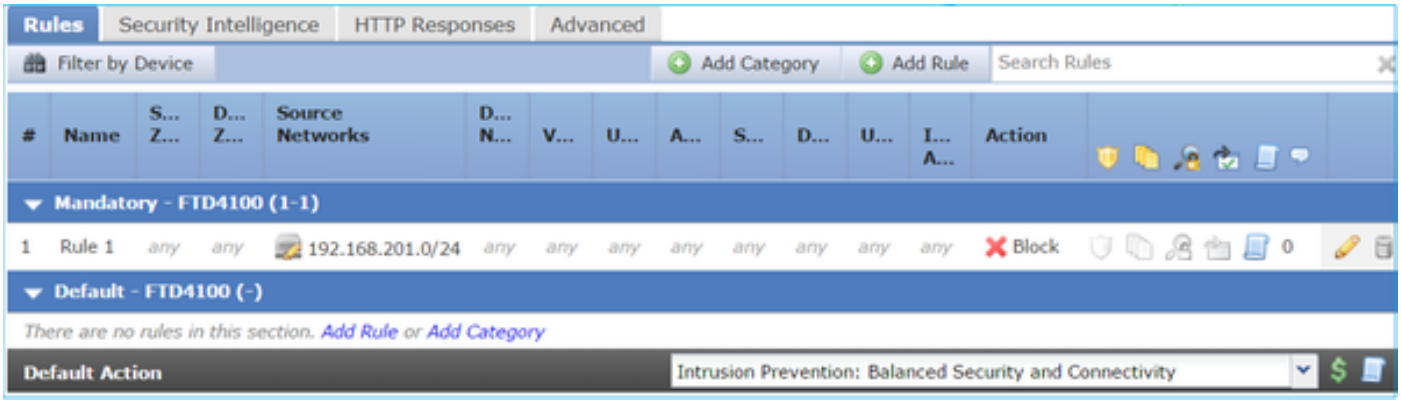
解決策

NAT はインラインの、インライン タップかパッシブモードを操作するインターフェイスのためにサポートされません:

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

インライン ペア インターフェイス モードのパケットのブロック

次の、送信トラフィックのようなブロックルールを FTD インライン ペアによって作成し、動作を観察して下さい:



解決策

トレースのキャプチャを有効に し、FTD インライン ペアによって SYN/ACK パケットを送信して下さい。 トラフィックはブロックされます:

```
> 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
```

パケットをトレースすることは明らかにします:

```
> 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
```

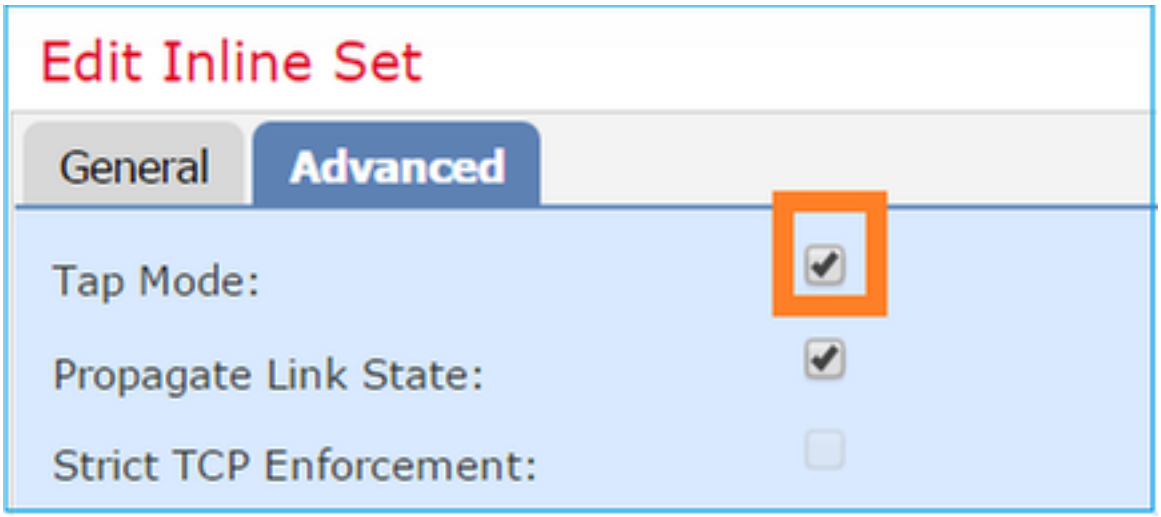
上のトレースでパケットが FTD ASA エンジンによって廃棄され、FTD Snort エンジンに転送されなかったことが見られる場合があります。

タップでのインライン ペア モードの設定

インライン ペアのイネーブル タップ モード

解決策

> インラインにセットはデバイス > デバイス管理にナビゲート し、インライン ペアを編集し、タブを『Advanced』 をクリック し、**蛇口モードを**有効に します:



確認

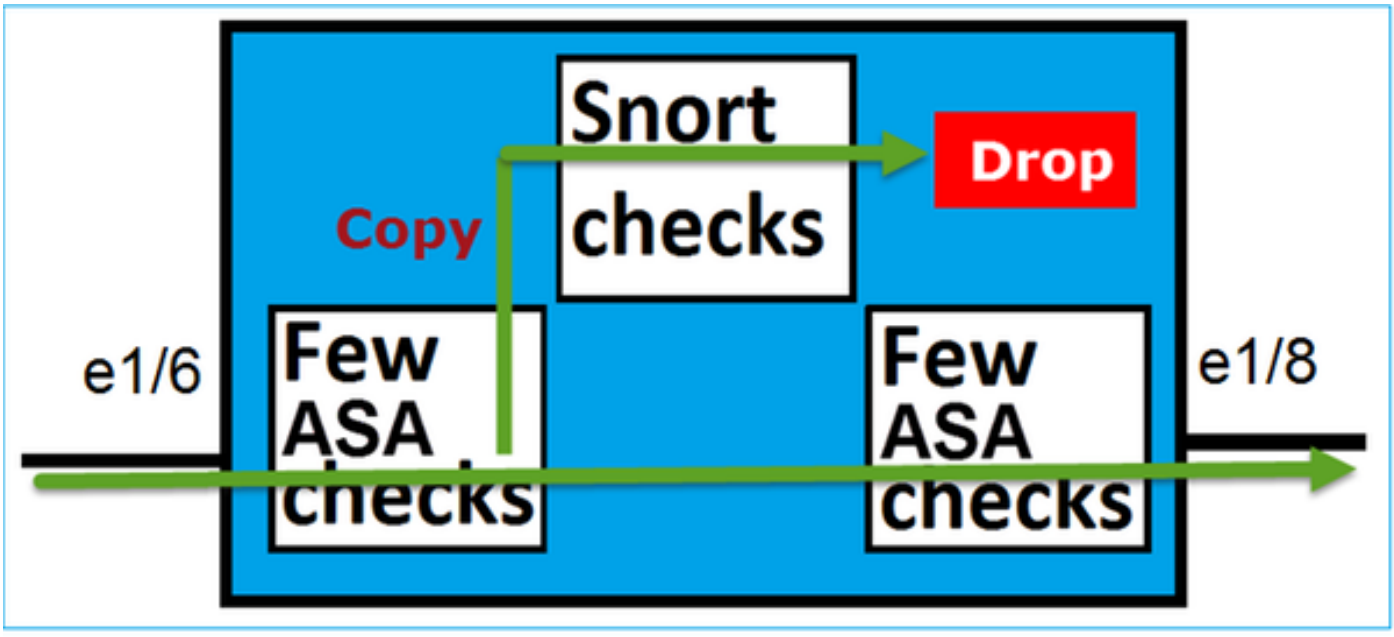
```
> show inline-set Inline-set Inline-Pair-1 Mtu is 1500 bytes Failsafe mode is on/activated
Failsecure mode is off Tap mode is on Propagate-link-state option is on hardware-bypass mode is
disabled Interface-Pair[1]: Interface: Ethernet1/6 "INSIDE" Current-Status: UP Interface:
Ethernet1/8 "OUTSIDE" Current-Status: UP Bridge Group ID: 0 >
```

タップ インターフェイス オペレーションによる FTD インライン ペアの検証

基本的 な 理論

- インライン ペアをタップ 2 物理インターフェイスで設定するとき内部で繋がれます
- **経路選択済み**か**透過的な配置モード**で利用可能
- **ASA エンジン 機能** (NAT、ルーティング、L3/L4 ACL 等) **のほとんどは**インライン ペアを通過するフローのために**利用可能ではないです**
- 実際のトラフィックは**廃棄することができません**
- **少数の ASA エンジン** チェックは**実際のトラフィックのコピーに完全な Snort エンジン** チェックと共に適用します

最後のポイントは次の通り視覚化することができます:



タップ モードでのインライン ペアはトランジットトラフィックを廃棄しません。 パケットをト

レースすることはこれを確認します:

```
> 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
>
```

Comparison: インライン ペア vs タップとのインライン ペア

	インライン ペア	タップとのインライン ペア
インライン設定 される示して下さい	>インライン設定 される示して下さい インライン設定 された Inline-Pair-1 MTU は 1500 バイトです フェイル・セイフ モードは on/activated です Failsecure モードは消えています **タップ モードは消えています** プロパゲート リンク州のオプションはオンになっています ハードウェア バイパス モードは無効です インターフェイスPair[1]: Interface: Ethernet1/6 「内部」 現在のステータス: UP Interface: Ethernet1/8 「外部」 現在のステータス: UP **ブリッジ グループ ID: 509** >	**> インライン設定 される示して下さい** インライン設定 された Inline-Pair-1 MTU は 1500 バイトです フェイル・セイフ モードは on/activated Failsecure モードは消えています **タップ モードはオンになっています** プロパゲート リンク州のオプションはオ なっています ハードウェア バイパス モードは無効です インターフェイスPair[1]: Interface: Ethernet1/6 「内部」 現在のステータス: UP Interface: Ethernet1/8 「外部」 現在のステータス: UP **ブリッジ グループ ID: 0** >
show interface	>show interface e1/6 インターフェイス Ethernet1/6 「内部」は、行プロトコル稼働しています稼働しています ハードウェアは EtherSVI、BW 1000 Mbps、DLY 1000 usec です MAC アドレス 5897.bdb9.770e、MTU 1500 IPS インターフェイス モード: **インライン**に、インライン設定 される: Inline-Pair-1 未指定 IP アドレス 「内部」のためのトラフィック 統計: 3957 パケット入力、264913 バイト 144 のパケット出力、58664 バイト 廃棄される 4 つのパケット 1 分入力速度 0 pkts/秒、26 バイト/秒 1 毎分心拍出量 比率 0 pkts/秒、7 バイト/秒	>show interface e1/6 インターフェイス Ethernet1/6 「内部」は プロトコル稼働しています稼働しています ハードウェアは EtherSVI、BW 1000 Mb DLY 1000 usec です MAC アドレス 5897.bdb9.770e、MT 1500 IPS インターフェイス モード: インラ 設定 されるインライン **タップ**: Inline-Pair 未指定 IP アドレス 「内部」のためのトラフィック 統計: 24 パケット入力、1378 バイト 0 パケット出力、0 バイト 廃棄される 24 のパケット 1 分入力速度 0 pkts/秒、0 バイト/秒 1 毎分心拍出量 比率 0 pkts/秒、0 バイ

1 分ドロップする 比率、0 pkts/秒
5 つの分入力速度 0 pkts/秒、28 バイト/秒
5 毎分心拍出量 比率 0 pkts/秒、9 バイト/秒
5 分ドロップする 比率、0 pkts/秒

> show interface e1/8

インターフェイス Ethernet1/8 「外部」は、行プロトコル稼働しています稼働しています
ハードウェアは EtherSVI、BW 1000 Mbps、DLY 1000 usec です
MAC アドレス 5897.bdb9.774d、MTU 1500
IPS インターフェイス モード: **インライン**に、インライン設定 される: Inline-Pair-1
未指定 IP アドレス
「外部」のためのトラフィック 統計:
144 パケット入力、55634 バイト
3954 のパケット出力、339987 バイト
廃棄される 0 パケット
1 分入力速度 0 pkts/秒、7 バイト/秒
1 毎分心拍出量 比率 0 pkts/秒、37 バイト/秒
1 分ドロップする 比率、0 pkts/秒
5 つの分入力速度 0 pkts/秒、8 バイト/秒
5 毎分心拍出量 比率 0 pkts/秒、39 バイト/秒
5 分ドロップする 比率、0 pkts/秒

>

>キャプチャ CAPI パケット数 1 トレースを示して下さい

キャプチャ される 3 つのパケット

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
Type: キャプチャ
サブタイプ:
結果： プライベート ネットワーク間で
構成:
その他の情報：
MAC アクセス リスト

ブロックルールと処理するパケット

フェーズ: 2
Type: アクセス リスト
サブタイプ:
結果： プライベート ネットワーク間で
構成:
暗示ルール
その他の情報：
MAC アクセス リスト

フェーズ: 3
Type: NGIPS-MODE

1 分ドロップする 比率、0 pkts/秒
5 つの分入力速度 0 pkts/秒、0 バイト
5 毎分心拍出量 比率 0 pkts/秒、0 バイ
5 分ドロップする 比率、0 pkts/秒

> show interface e1/8

インターフェイス Ethernet1/8 「外部」は
プロトコル稼働しています稼働しています
ハードウェアは EtherSVI、BW 1000 Mb
DLY 1000 usec です
MAC アドレス 5897.bdb9.774d、MT
1500
IPS インターフェイス モード: インラ
設定 されるインライン **タップ**: Inline-Pair
未指定 IP アドレス
「外部」のためのトラフィック 統計:
1 パケット入力、441 バイト
0 パケット出力、0 バイト
廃棄される 1 パケット
1 分入力速度 0 pkts/秒、0 バイト/秒
1 毎分心拍出量 比率 0 pkts/秒、0 バイ
1 分ドロップする 比率、0 pkts/秒
5 つの分入力速度 0 pkts/秒、0 バイト
5 毎分心拍出量 比率 0 pkts/秒、0 バイ
5 分ドロップする 比率、0 pkts/秒

>

> キャプチャ CAPI パケット数 1 トレース して下さい

キャプチャ される 3 つのパケット

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
Type: キャプチャ
サブタイプ:
結果： プライベート ネットワーク間で
構成:
その他の情報：
MAC アクセス リスト

フェーズ: 2
Type: アクセス リスト
サブタイプ:
結果： プライベート ネットワーク間で
構成:
暗示ルール
その他の情報：
MAC アクセス リスト

フェーズ: 3
Type: NGIPS-MODE

サブタイプ: ngips モード
結果： プライベート ネットワーク間で
構成:
その他の情報：
フローは NGIPS モードのために設定されたインターフェイスを ingressed、NGIPS サービスは適用します

フェーズ: 4
Type: アクセス リスト
サブタイプ: log
結果： [DROP]
構成:
グローバル な アクセスグループ CSM_FW_ACL_
access-list CSM_FW_ACL_ によって進められる拒否 IP 192.168.201.0 255.255.255.0 ルール ID 268441600 イベントログ フロー開始する
access-list CSM_FW_ACL_ 解説ルール ID 268441600: アクセスポリシー: FTD4100 - Mandatory/1
access-list CSM_FW_ACL_ 解説ルール ID 268441600: L4 ルール: ルール 1
その他の情報：

結果：
インプットインターフェイス: 内部
入力ステータス: up
入力行ステータス: up
アクション： drop
ドロップする原因: (ACL ドロップする) フローは設定されたルールによって否定されます

示されている 1 パケット
>

サブタイプ: ngips モード
結果： プライベート ネットワーク間で
構成:
その他の情報：
フローは NGIPS モードのために設定されたインターフェイスを ingressed、NGIPS サービスは適用します

フェーズ: 4
Type: アクセス リスト
サブタイプ: log
結果： 廃棄された HAS
構成:
グローバル な アクセスグループ CSM_FW_ACL_
access-list CSM_FW_ACL_ によって進める拒否 IP 192.168.201.0 255.255.255.0 ル ID 268441600 イベントログ フロー開始す
access-list CSM_FW_ACL_ 解説ルール ID 268441600: アクセスポリシー: FTD4100 Mandatory/1
access-list CSM_FW_ACL_ 解説ルール ID 268441600: L4 ルール: ルール 1
その他の情報：

結果：
インプットインターフェイス: 内部
入力ステータス: up
入力行ステータス: up
アクション： Access-list は廃棄しました、パケットは当然のインライン タップを転しました

示されている 1 パケット
>

要約

- インライン ペア モードを使用するときパケットは FTD Snort エンジンを主に通過します。
- TCP 接続は TCP 州バイパス モードで処理されます
- FTD ASA エンジン観点から ACL ポリシーは適用しています
- インライン ペア モードが使用中のときパケットはインラインに処理されるのでブロックすることができます

- タップ モードが有効に なるときパケットのコピーは実際のトラフィックが非修飾 FTD を通過する間、内部で点検され、廃棄されます

関連資料

Cisco Firepower NGFW