配置Firepower威胁防御在线型对模式建立接口

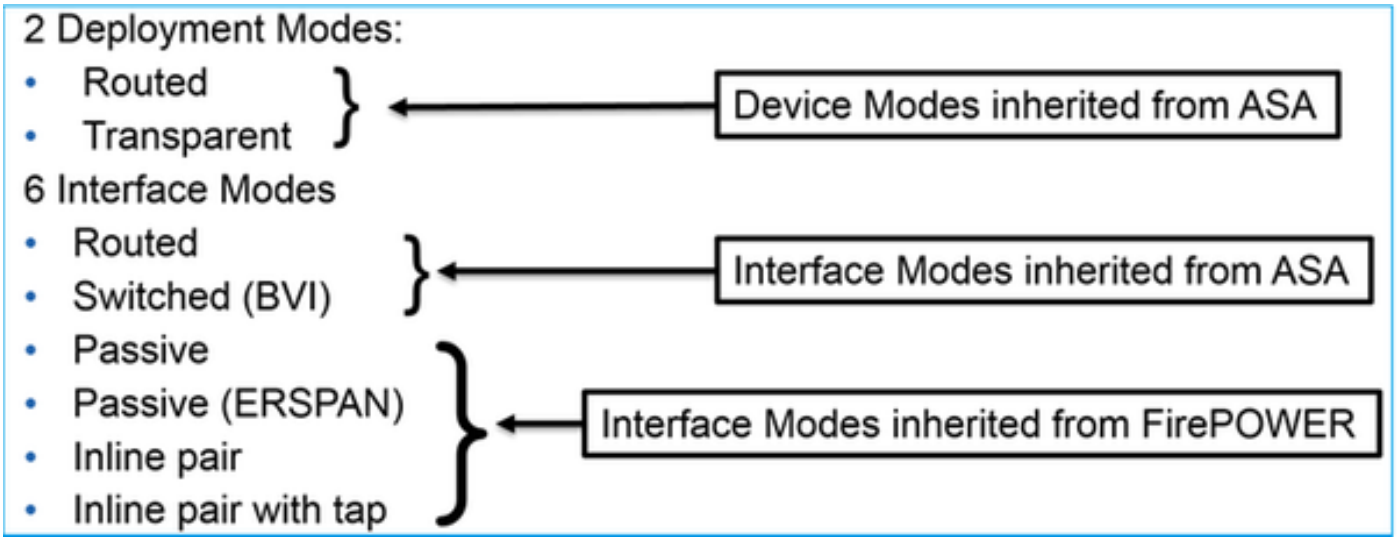
目录

简介

Firepower威胁防御(FTD)是在以下平台可以安装的一个统一的软件镜像：

- ASA5506-X， ASA5506W-X， ASA5506H-X， ASA5508-X， ASA5516-X
- ASA5512-X， ASA5515-X， ASA5525-X， ASA5545-X， ASA5555-X
- FPR4100， FPR9300
- VMware (ESXi)
- 亚马逊网站服务(AW)
- KVM
- ISR路由模块

FTD提供2个部署模式和6个接口模式



注意：您能混合在sigle FTD设备的接口模式

这是多种FTD部署和接口模式的高水平概述：

FTD接口模式	FTD部署模式	说明	流量可以丢弃
已路由	已路由	全双工ASA引擎和喷鼻息引擎检查	是
交换式	透明	全双工ASA引擎和喷鼻息引擎检查	是
轴向对	已路由或透明	部分ASA引擎和全双工喷鼻息引擎检查	是
与点击的轴向对	已路由或透明	部分ASA引擎和全双工喷鼻息引擎检查	否
被动	已路由或透明	部分ASA引擎和全双工喷鼻息引擎检查	否
被动(ERSPAN)	已路由	部分ASA引擎和全双工喷鼻息引擎检查	否

目标

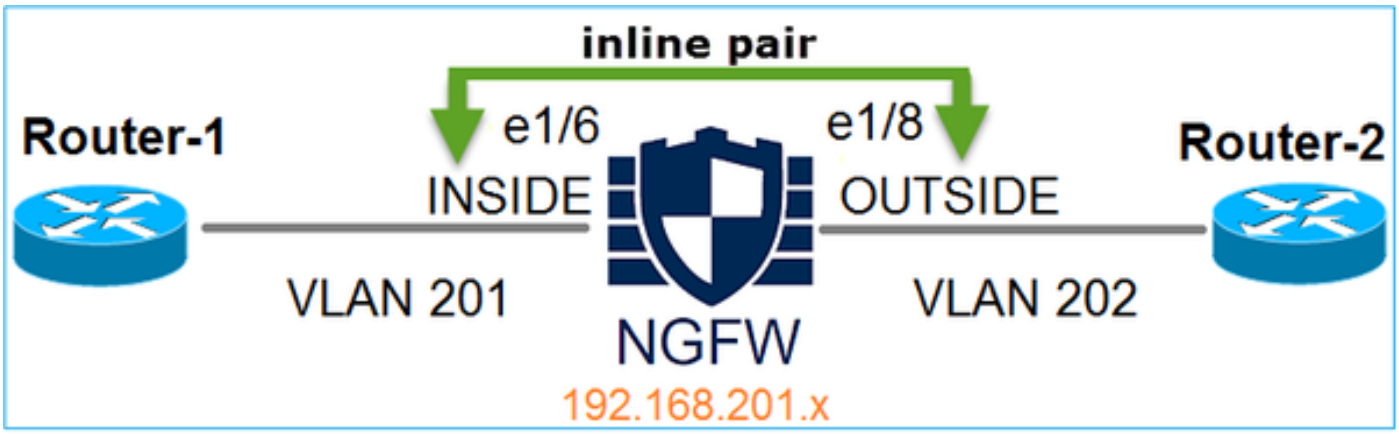
本文目标对：

- 展示配置，并且FTD线型对的操作建立接口

使用的组件

- Firepower 4150运行的FTD代码6.1.0.x
- 运行6.1.0.x的Firepower管理中心(FMC)

拓扑



配置在FTD的轴向对接口

需求

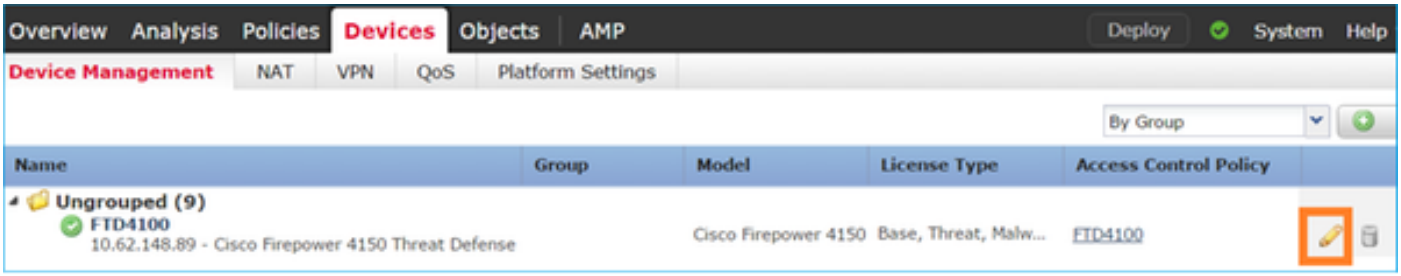
配置在轴向对模式的物理接口e1/6和e1/8每以下需求：

接口	e1/6	e1/8
名称	里面	从外部
安全区域	INSIDE_ZONE	OUTSIDE_ZONE
轴向集名	Inline-Pair-1	
轴向集MTU	1500	
故障自动保险	已启用	
繁殖林克状态	已启用	

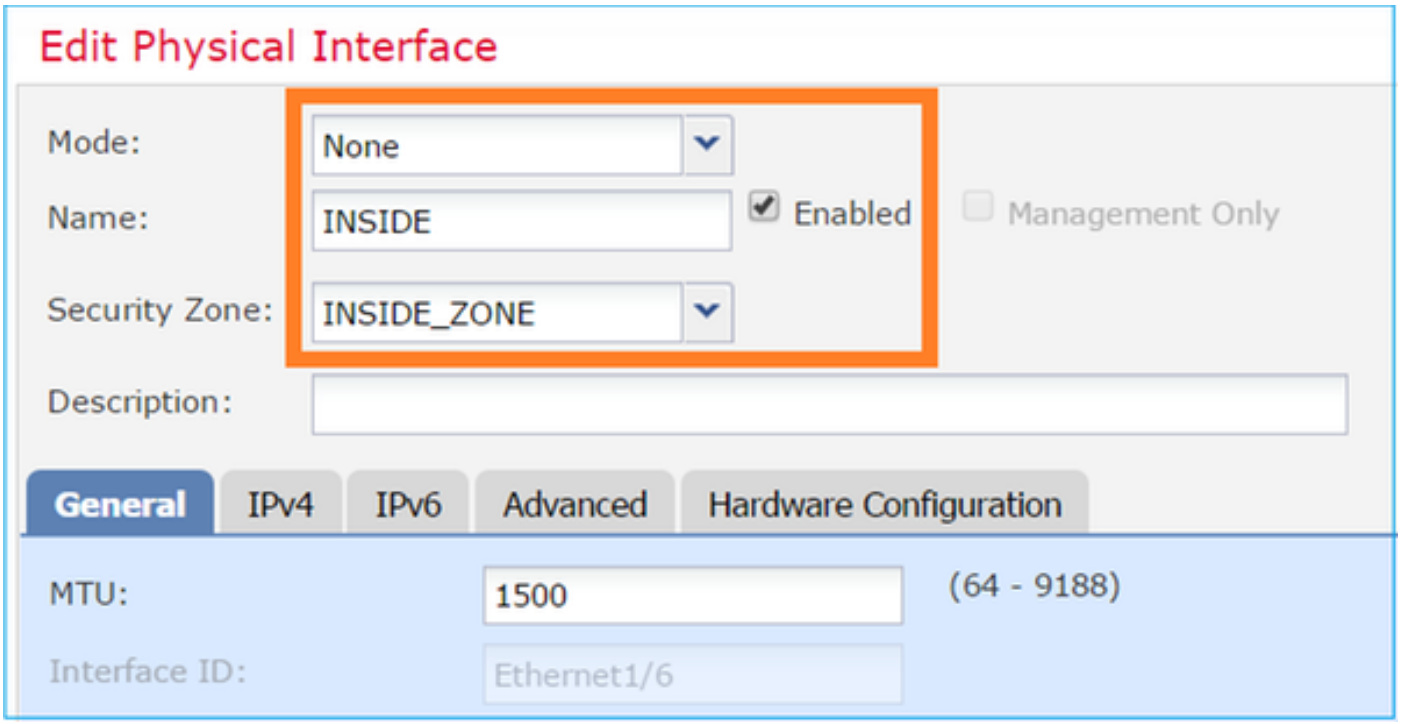
[解决方案]

Step1 –配置单个接口

导航对**设备>设备管理**，选择适当的设备并且点击**Edit图标**：

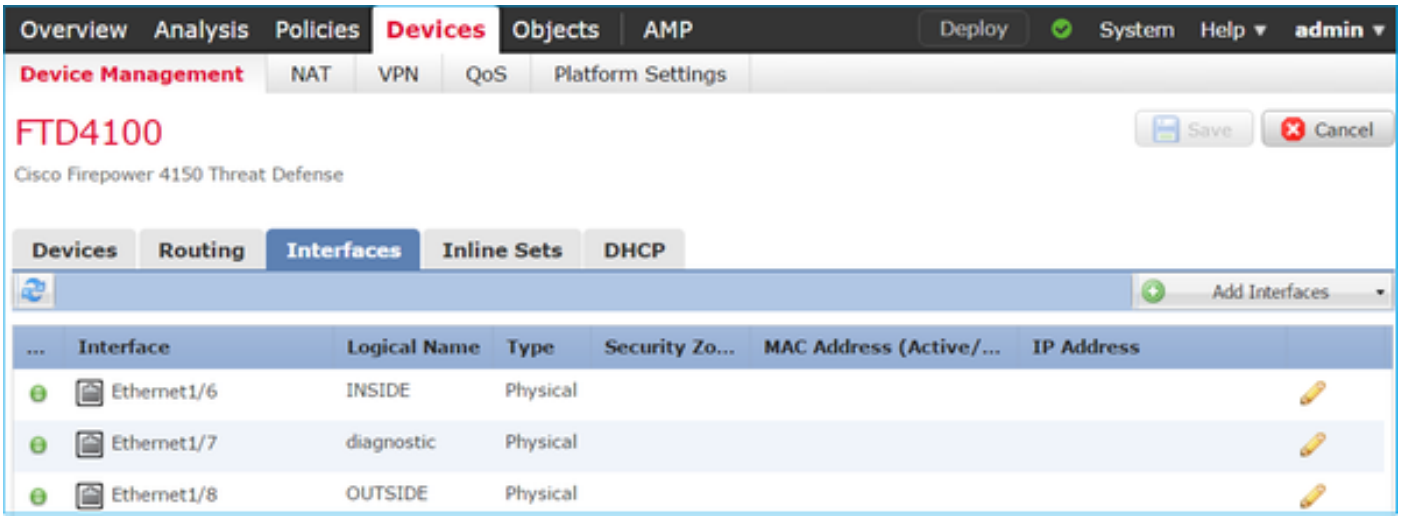


指定名称并且启用接口：



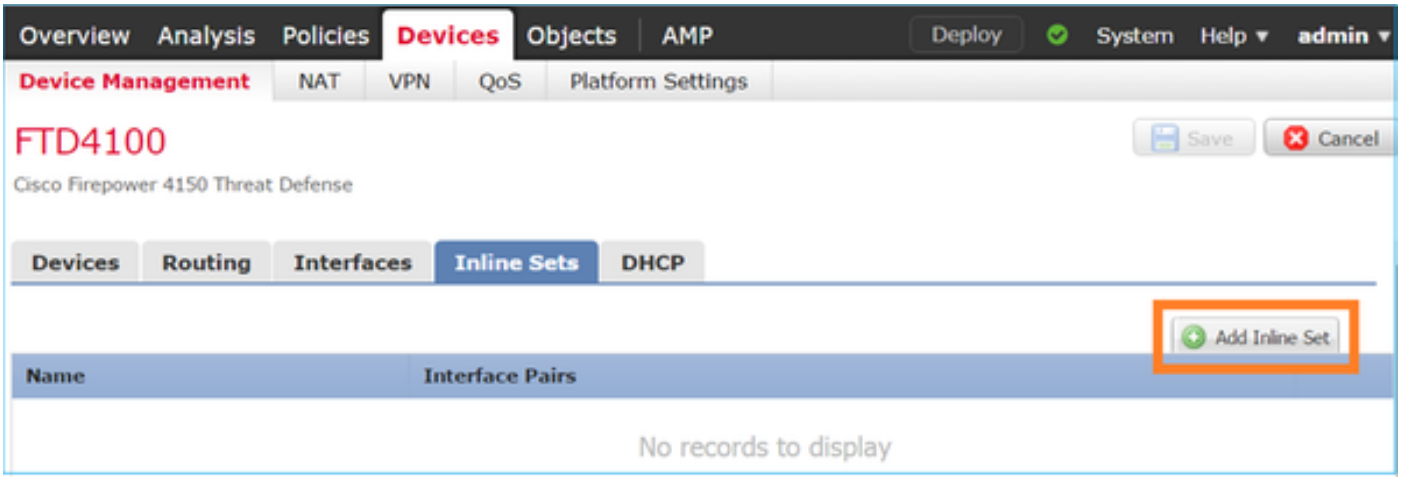
名称将是接口的**nameif**

同样接口Ethernet1/8。最终结果：

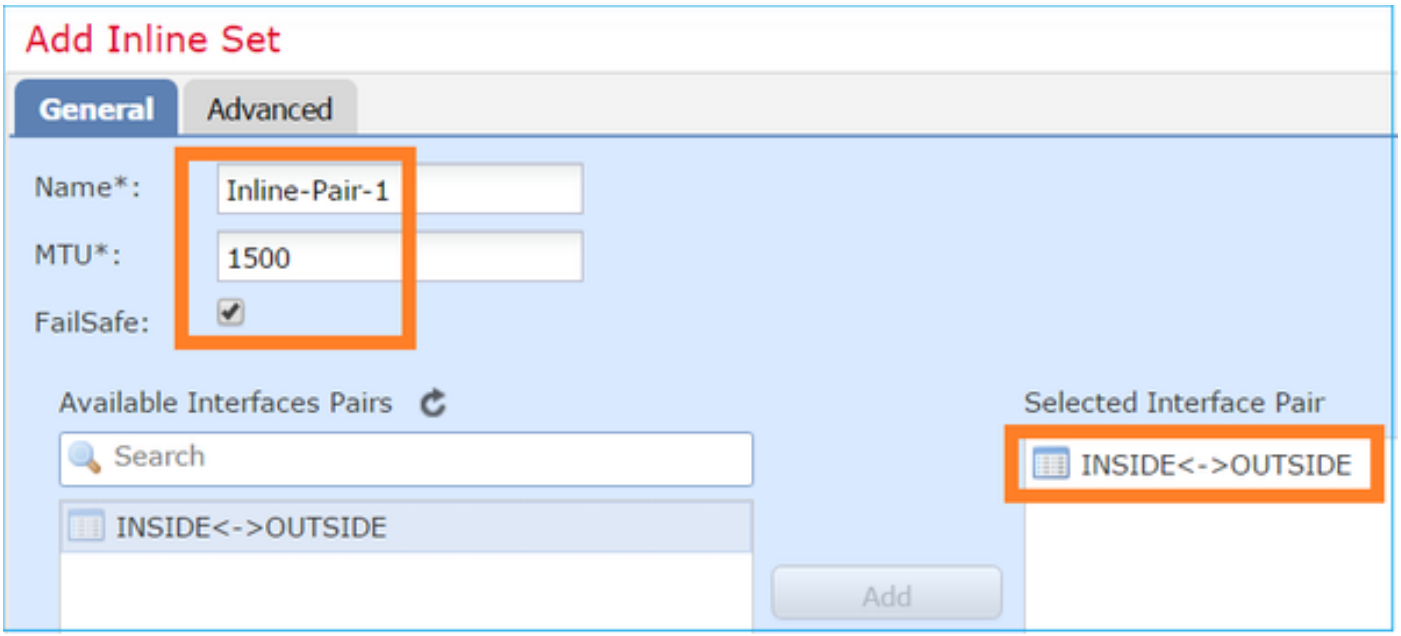


步骤2 –配置轴向对

导航对**轴向集**选项卡并且点击**Add轴向集**：

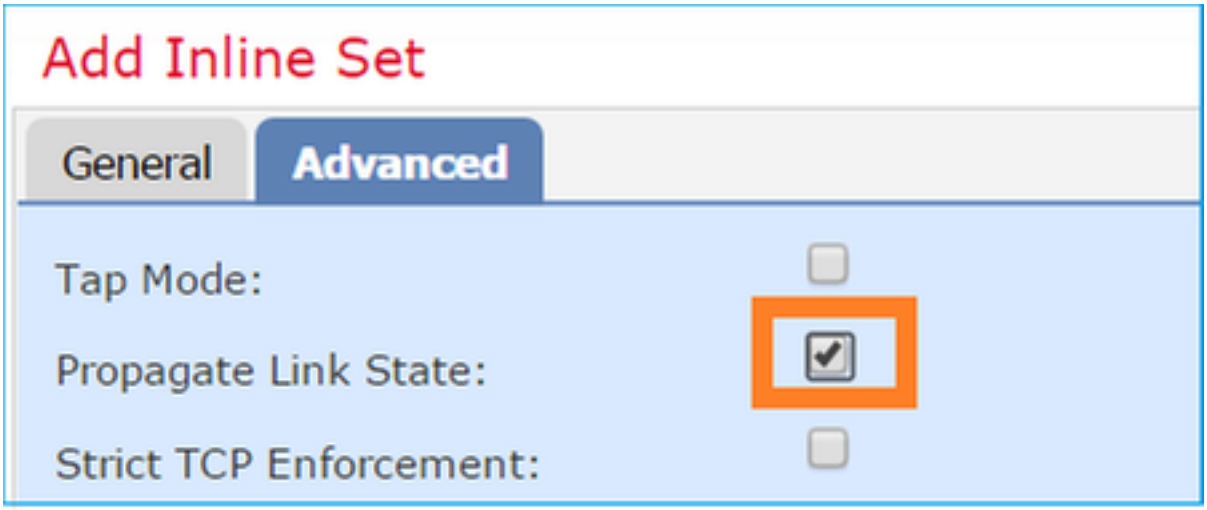


配置每需求的设置：



故障自动保险允许流量穿过未经检查轴向的对，万一接口缓冲区全双工(典型地看到，当超载时设备或超载喷鼻息引擎)。动态地分配接口缓冲区大小。

Enable (event) “**繁殖林克State'**选项：



当其中一个在轴向集的接口断开时，林克状态传播自动地建立下来在轴向接口对的第二个接口。

保存更改并且**部署**

正在验证轴向对接口配置

验证从FTD CLI的轴向对配置

[解决方案]

登陆对FTD CLI并且验证轴向对配置：

```
> 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
>
```

注意：网桥Group ID跟0是值不同。如果点击模式在那么是0

接口和名称信息：

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

正在验证接口状态：

```
> 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
```

正在验证的物理接口信息：

```
> 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
>
```

正在验证FTD轴向对接口操作

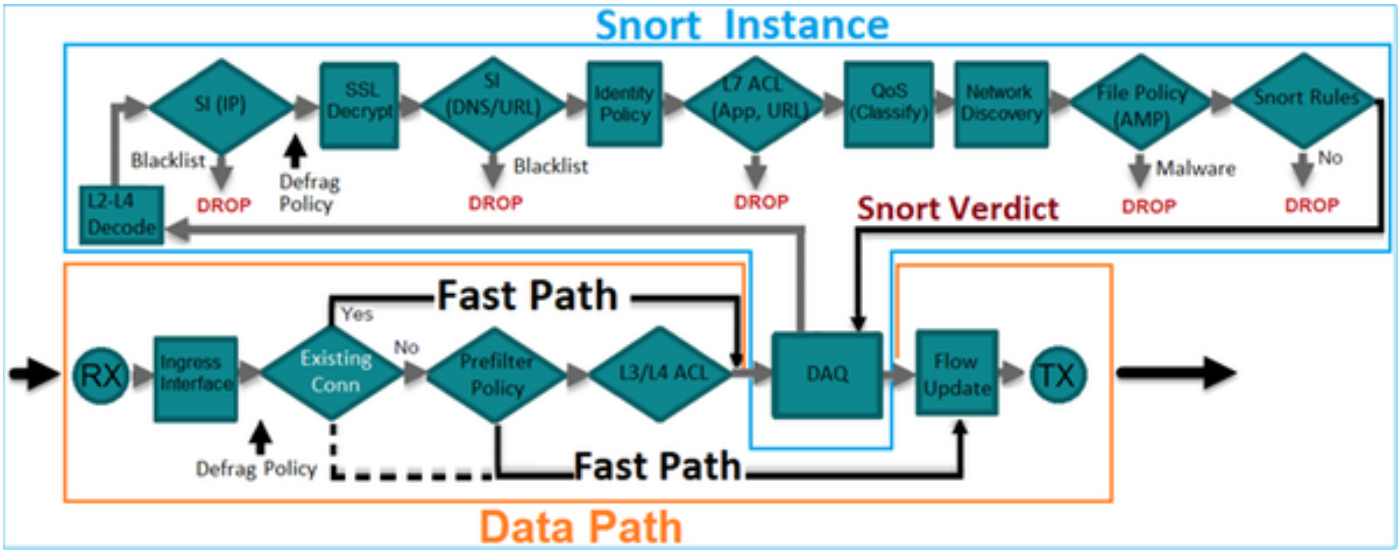
此部分包括以下验证检查为了验证轴向对操作：

- 验证1 –使用数据包追踪器
- 验证2 –启用与trace和发送TCP SYN/ACK数据包的捕获通过轴向对
- 验证3 –监控FTD流量使用防火墙引擎调试
- 验证4 –正在验证连接状态的传播功能
- 验证5 –配置静态NAT

解决方案

架构概述

当2个FTD接口在线型对模式时运行数据包被处理如下：

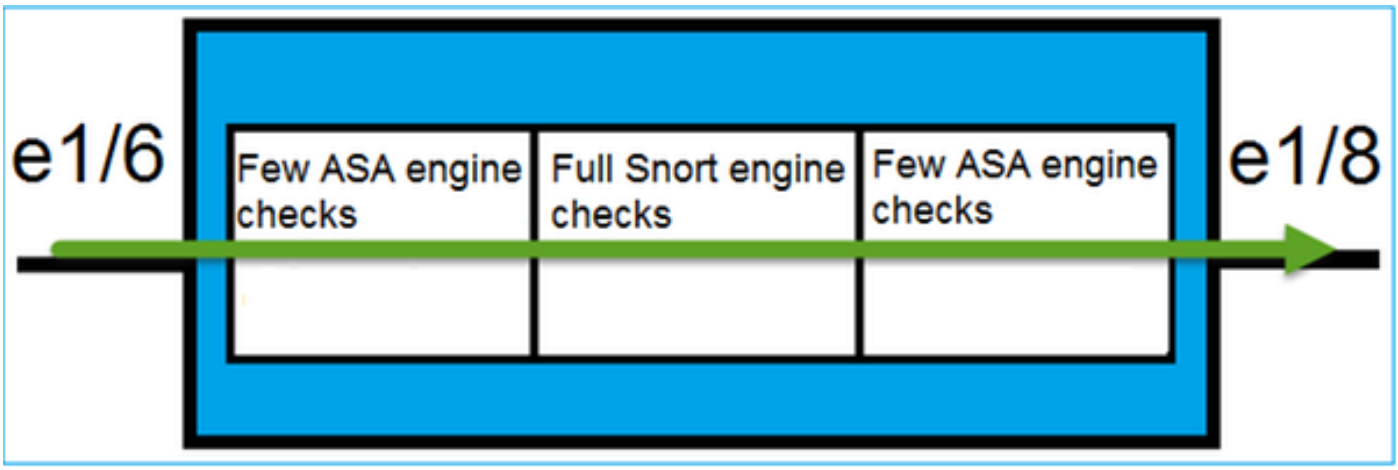


注意：仅物理接口可以是设置的一个轴向对的成员

基本理论

- 当配置一个轴向对时2个物理接口内部地桥接
- 非常类似于**经典轴向IPS**
- 在**已路由**或**透明部署**模式的联机
- 大多ASA引擎功能(NAT、路由， L3/L4 ACL等)为去的流不是**可用的**通过一个轴向对
- 中转流量**可以丢弃**
- **少量ASA引擎**检查与**全双工喷鼻息引擎**检查一起应用

最后点可以形象化如下：



验证1 –使用数据包追踪器

这是输出的数据包追踪器模拟横断的数据包轴向对用突出显示的触发的点：

```
> 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

>
```

验证2 –发送TCP SYN/ACK数据包通过轴向对

使用一个数据包制作的工具类似Scapy，您能生成TCP SYN/ACK数据包。以下语法将生成3数据包用启用的SYN/ACK标志：

```
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)
```

启用在FTD CLI的以下捕获并且发送少量TCP SYN/ACK数据包：

```
> 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
>
```

在发送数据包以后通过FTD您能看到创建的连接：

```
> 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标志**：除非TCP状态旁路启用，经典ASA将丢弃一未经请求的SYN/ACK数据包。在轴向对模式的一个FTD接口处理在TCP状态旁路模式的一TCP连接，并且不丢弃不属于现有连接的TCP信息包
- **N标志**：数据包将乘FTD喷鼻息引擎检查

因为您能看到3数据包横断FTD，捕获证明在上面：

```
> 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
>
```

退出FTD设备的3数据包：

```
> 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
>
```

跟踪第一捕获数据包暴露一些其他信息类似喷鼻息引擎判决：

```
> 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
```

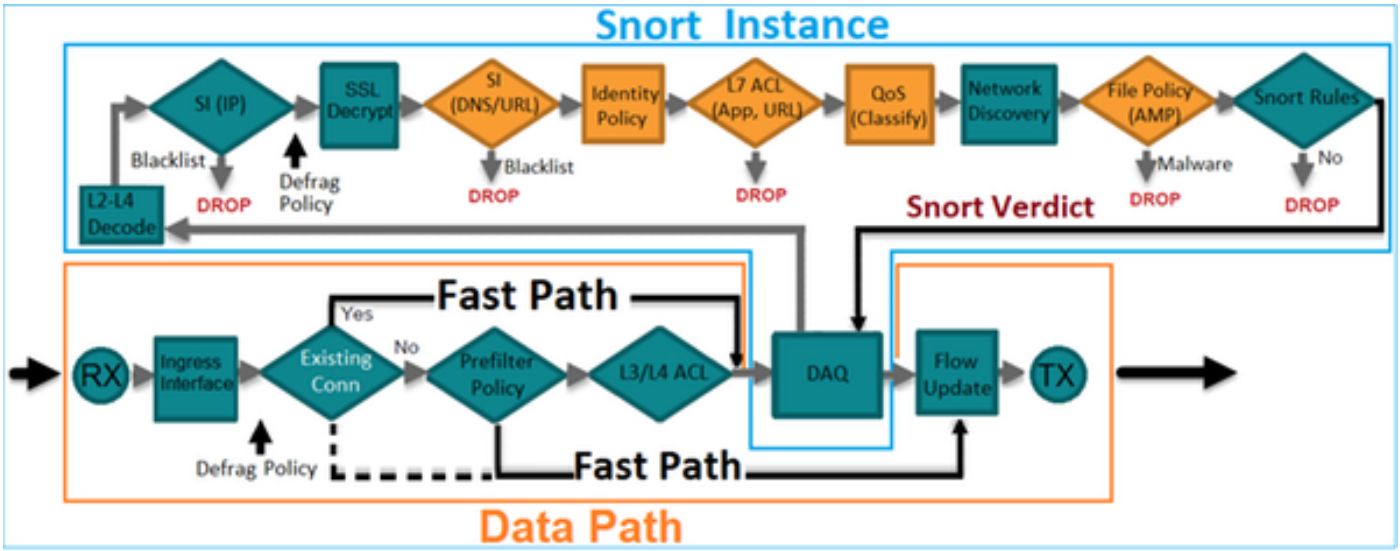
```
Information: New flow created with id 282, packet dispatched to next module Phase: 7 Type:
EXTERNAL-INSPECT Subtype: Result: ALLOW Config: Additional Information: Application: 'SNORT
Inspect' Phase: 8 Type: SNORT Subtype: Result: ALLOW Config: Additional Information: Snort
Verdict: (pass-packet) 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 >
```

跟踪第二获取数据包显示数据包匹配现有连接，因此绕过ACL检查，但是乘喷鼻息引擎仍然检查：

```
> 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 >
```

验证3 –防火墙允许流量的引擎调试

防火墙引擎FTD喷鼻息引擎的特定组件的调试运行类似访问控制策略：



当发送TCP SYN/ACK数据包通过轴向对时您在debug输出中能看到：

```
> 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
```

验证4 –正在验证的连接状态的传播

被关闭Enable (event)的缓冲区注册FTD和switchport连接对e1/6接口。在FTD CLI您应该看到两个接口断开了：

```
> 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日志显示：

```
> 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)
>
```

线型设置的状态显示2个接口成员的状态：

```
> 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
>
```

注意在2个接口的状况的差异：

```
> 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
>
```

并且Ethernet1/8接口：

```
> 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
>
```

在重新启用switchport以后FTD日志显示：

```
> 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)
>
```

验证5 –配置静态NAT

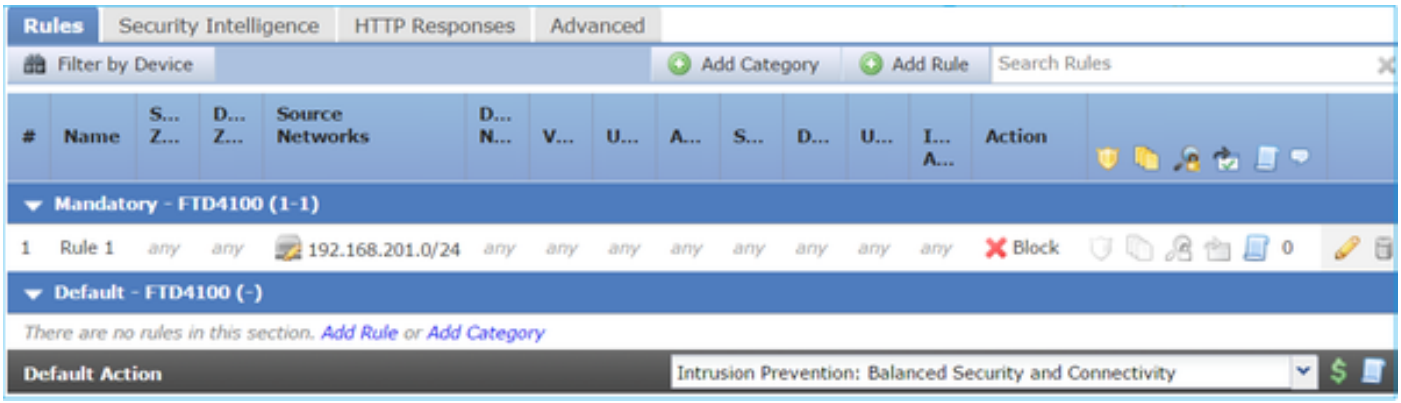
解决方案

NAT不为操作轴向，轴向点击或被动模式的接口支持：

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

阻塞在轴向对接口模式的数据包

创建一个分块规则类似以下，通过FTD轴向对发送流量并且观察行为：



解决方案

启用与trace的捕获并且通过FTD轴向对发送SYN/ACK数据包。流量阻塞：

```
> 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
```

跟踪数据包显示：

```
> 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
```

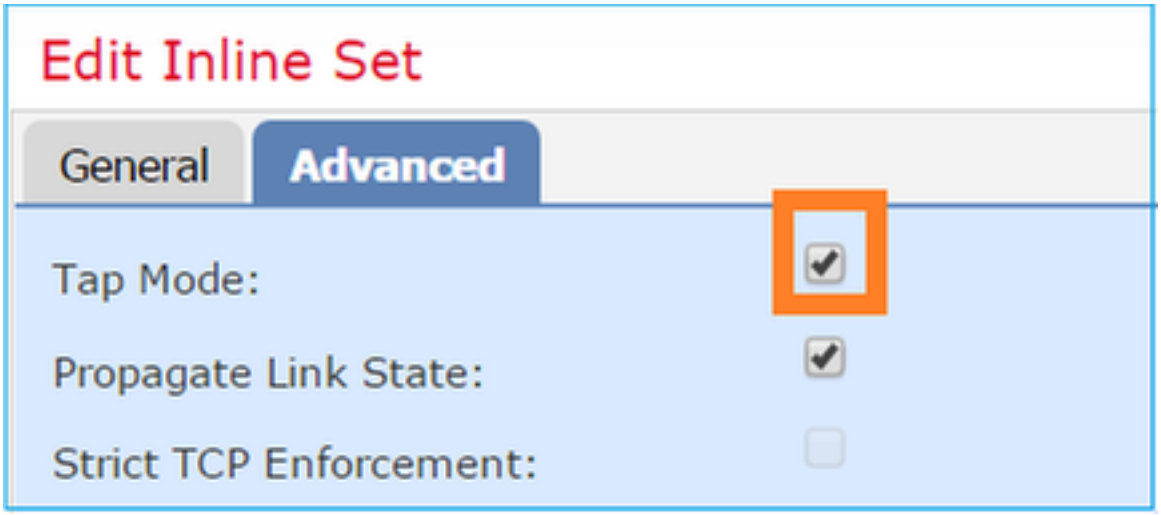
在上述trace能被看到数据包乘FTD ASA引擎丢弃和未转发到FTD喷鼻息引擎。

配置与点击的轴向对模式

Enable (event)在轴向对的点击模式

[解决方案]

导航对**设备>设备管理>线型集**，编辑轴向对，点击**高级选项卡。**并且启动**点击模式**：



验证

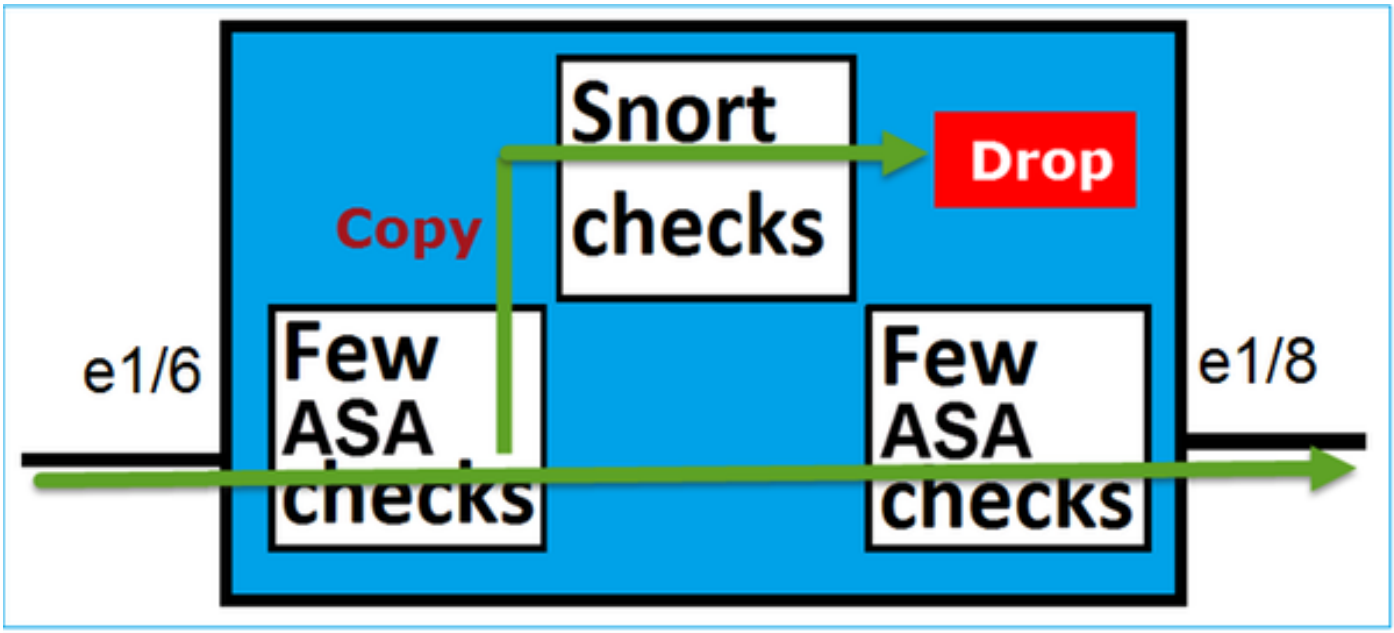
```
> show inline-set Inline-set Inline-Pair-1 Mtu is 1500 bytes Failsafe mode is on/activated
Failsecure mode is off Tap mode is on Propagate-link-state option is on hardware-bypass mode is
disabled Interface-Pair[1]: Interface: Ethernet1/6 "INSIDE" Current-Status: UP Interface:
Ethernet1/8 "OUTSIDE"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

正在验证与点击接口操作的FTD轴向对

基本理论

- 当配置与点击时的一个轴向对2个物理接口内部地桥接
- 在**已路由**或**透明部署**模式的联机
- **大多ASA引擎功能**(NAT、路由， L3/L4 ACL等)为去的流不**是可用的**通过轴向对
- 实际流量不**可能丢弃**
- **少量ASA引擎**检查与**对实际流量的复制的全双工喷鼻息引擎**检查一起应用

最后点可以形象化如下：



轴向对同点击模式不降低中转流量。跟踪数据包确认此：

```
> 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
>
```

比较：轴向对与与点击的轴向对

	轴向对	**与点击的轴向对**
	>显示线型设置	**> 显示线型设置**
显示线型设置	线型设置的Inline-Pair-1 Mtu是1500个字节 故障自动保险的模式是on/activated Failsecure模式关闭 **点击模式关闭** 繁殖林克状态选项打开 硬件旁路模式禁用 接口Pair[1] ： 接口：Ethernet1/6 “里面” 当前状态： 接口：Ethernet1/8 “外部” 当前状态： **网桥Group ID ：509**	线型设置的Inline-Pair-1 Mtu是1500个字节 故障自动保险的模式是on/activated Failsecure模式关闭 **点击模式打开** 繁殖林克状态选项打开 硬件旁路模式禁用 接口Pair[1] ： 接口：Ethernet1/6 “里面” 当前状态： 接口：Ethernet1/8 “外部” 当前状态： **网桥Group ID ：0**

show interface	> **>show interface e1/6** 接口Ethernet1/6 “里面”，是UP，线路通信协议是UP 硬件是EtherSVI， BW 1000 Mbps， DLY 1000 usec MAC地址5897.bdb9.770e， MTU 1500 IPS接口模式：**线型**，线型设置：Inline-Pair-1 未分配的IP地址 “里面的”流量统计： 3957信息包输入， 264913个字节 144 packets output， 58664个字节 4被丢弃的数据包 1分钟输入速率0 pkts /sec， 26字节/秒 1每分钟输出生产率0 pkts /sec， 7字节/秒 1分钟丢弃速率， 0 pkts /sec 5分钟输入速率0 pkts /sec， 28字节/秒 5每分钟输出生产率0 pkts /sec， 9字节/秒 5分钟丢弃速率， 0 pkts /sec **> show interface e1/8** 接口Ethernet1/8 “外部”，是UP，线路通信协议是UP 硬件是EtherSVI， BW 1000 Mbps， DLY 1000 usec MAC地址5897.bdb9.774d， MTU 1500 IPS接口模式：**线型**，线型设置：Inline-Pair-1 未分配的IP地址 “外部的”流量统计： 144信息包输入， 55634个字节 3954 packets output， 339987个字节 0被丢弃的数据包 1分钟输入速率0 pkts /sec， 7字节/秒 1每分钟输出生产率0 pkts /sec， 37字节/秒 1分钟丢弃速率， 0 pkts /sec 5分钟输入速率0 pkts /sec， 8字节/秒 5每分钟输出生产率0 pkts /sec， 39字节/秒 5分钟丢弃速率， 0 pkts /sec >	>**>show interface e1/6** 接口Ethernet1/6 “里面”，是UP，线路通信是UP 硬件是EtherSVI， BW 1000 Mbps， DLY usec MAC地址5897.bdb9.770e， MTU 150 IPS接口模式：**线型点击**，线型设置：Inline-Pair-1 未分配的IP地址 “里面的”流量统计： 24信息包输入， 1378个字节 0 packets output， 0字节 24被丢弃的数据包 1分钟输入速率0 pkts /sec， 0字节/秒 1每分钟输出生产率0 pkts /sec， 0字节 1分钟丢弃速率， 0 pkts /sec 5分钟输入速率0 pkts /sec， 0字节/秒 5每分钟输出生产率0 pkts /sec， 0字节 5分钟丢弃速率， 0 pkts /sec **> show interface e1/8** 接口Ethernet1/8 “外部”，是UP，线路通信是UP 硬件是EtherSVI， BW 1000 Mbps， DLY usec MAC地址5897.bdb9.774d， MTU 150 IPS接口模式：**线型点击**，线型设置：Inline-Pair-1 未分配的IP地址 “外部的”流量统计： 1信息包输入， 441个字节 0 packets output， 0字节 1被丢弃的数据包 1分钟输入速率0 pkts /sec， 0字节/秒 1每分钟输出生产率0 pkts /sec， 0字节 1分钟丢弃速率， 0 pkts /sec 5分钟输入速率0 pkts /sec， 0字节/秒 5每分钟输出生产率0 pkts /sec， 0字节 5分钟丢弃速率， 0 pkts /sec >
与**分块规则的**数据包处理	>**显示捕获CAPI数据包编号1 trace** 捕获的3数据包 1 ：16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80 ：S 0:0(0) ack 0 Win 8192 相位：1 类型：捕获 子类型： 结果：准许 设置： 其它信息： MAC访问列表	> **显示捕获CAPI数据包编号1 trace** 捕获的3数据包 1 ：16:56:02.631437 192.168.201.50.20 192.168.201.60.80 ：S 0:0(0) Win 8192 相位：1 类型：捕获 子类型： 结果：准许 设置： 其它信息： MAC访问列表

相位：2
类型：访问列表
子类型：
结果：准许
设置：
隐式规则
其它信息：
MAC访问列表

相位：3
类型：NGIPS-MODE
子类型：ngips模式
结果：准许
设置：
其它信息：
流ingressed为NGIPS模式配置的接口，并且NGIPS服务将应用

相位：4
类型：访问列表
子类型：日志
结果：丢弃
设置：
全局访问组CSM_FW_ACL_
access-list提前的CSM_FW_ACL_拒绝ip 192.168.201.0 255.255.255.0所有规则id 268441600事件日志流开始
CSM_FW_ACL_访问列表注释规则id 268441600 ：访问策略：FTD4100 - Mandatory/1
CSM_FW_ACL_访问列表注释规则id 268441600 ：L4规则：规则1
其它信息：

结果：
input-interface ：里面
输入状态：
输入线路状态：
操作：丢弃
丢弃原因：(ACL丢弃)流由配置的规则拒绝

显示的1数据包
>

相位：2
类型：访问列表
子类型：
结果：准许
设置：
隐式规则
其它信息：
MAC访问列表

相位：3
类型：NGIPS-MODE
子类型：ngips模式
结果：准许
设置：
其它信息：
流ingressed为NGIPS模式配置的接口，并NGIPS服务将应用

相位：4
类型：访问列表
子类型：日志
结果：会丢弃的HAS
设置：
全局访问组CSM_FW_ACL_
access-list提前的CSM_FW_ACL_拒绝ip 192.168.201.0 255.255.255.0所有规则id 268441600事件日志流开始
CSM_FW_ACL_访问列表注释规则id 268441600 ：访问策略：FTD4100 - Mandatory/1
CSM_FW_ACL_访问列表注释规则id 268441600 ：L4规则：规则1
其它信息：

结果：
input-interface ：里面
输入状态：
输入线路状态：
操作：access-list将丢弃，但是数据包转发于线型点击

显示的1数据包
>

摘要

- 当曾经轴向对模式时数据包通过主要FTD喷鼻息引擎。
- TCP连接在TCP状态旁路模式被处理
- 从FTD ASA引擎观点ACL策略应用
- 当轴向对模式是在使用中的时数据包可以阻塞，因为他们处理线型
- 当点击模式启用时数据包的复制检查并且丢弃内部地，当实际流量通过非限定时的FTD

相关文档

思科Firepower NGFW