在内联对模式下配置FTD接口

目录

简介

本文档介绍Firepower威胁防御(FTD)设备上的内联对接口的配置、验证和操作。

先决条件

要求

本文档没有特定要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Firepower 4150 FTD（代码6.1.0.x和6.3.x）
- Firepower管理中心(FMC)（代码6.1.0.x和6.3.x）

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

相关产品

本文档也可用于以下硬件和软件版本：

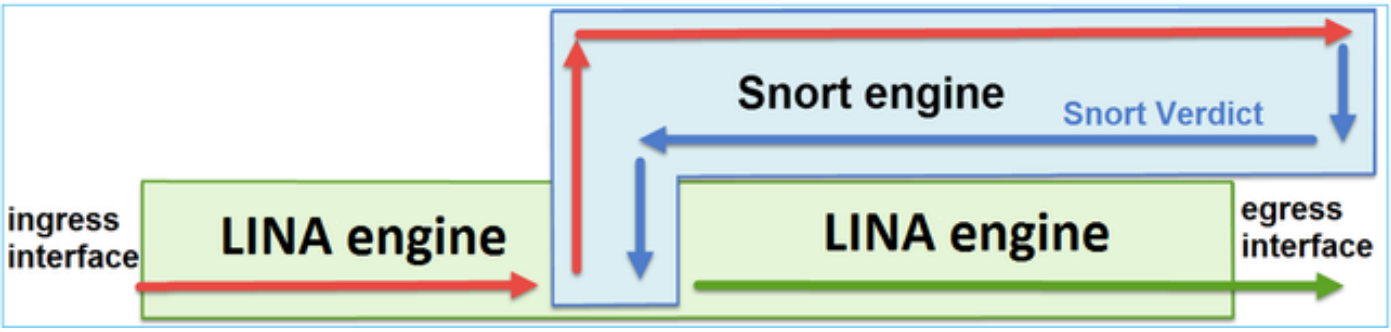
- ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X
- ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X
- FPR2100、FPR4100、FPR9300
- VMware (ESXi)、Amazon Web Services (AWS)、基于内核的虚拟机 (KVM)
- FTD软件代码6.2.x及更高版本

背景信息

FTD 是由两个主要引擎组成的统一软件映像：

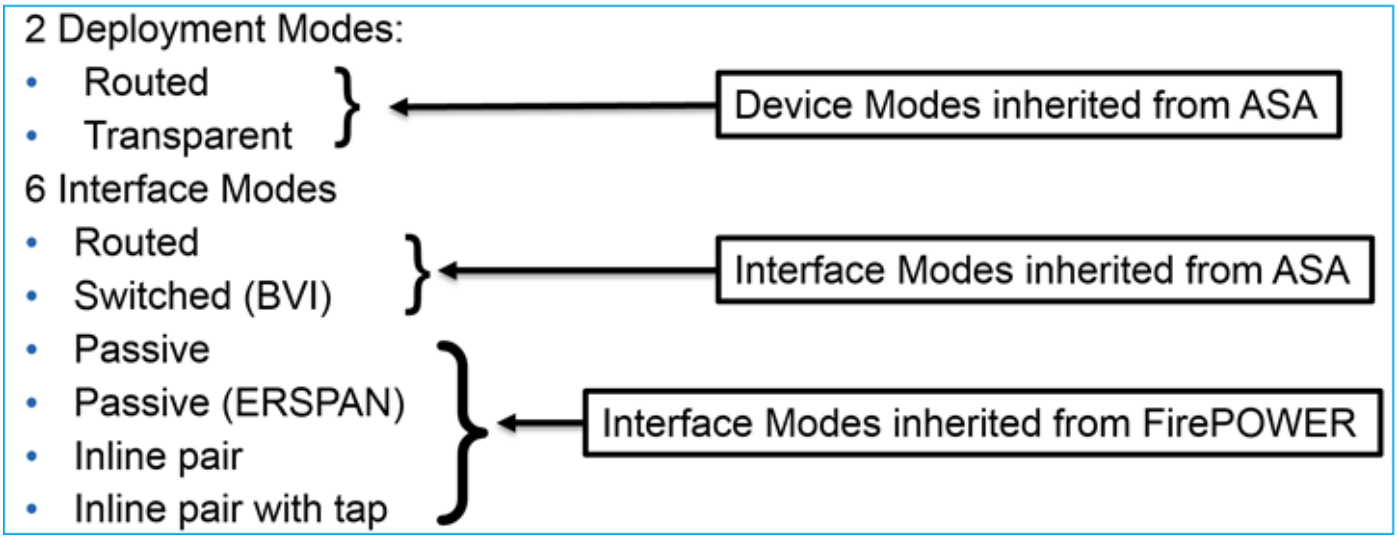
- LINA 引擎
- Snort 引擎

下图显示了这两个引擎的交互方式：



- 数据包进入入口接口并由 LINA 引擎处理
- 如果 FTD 策略要求，数据包将由 Snort 引擎检查
- Snort引擎返回数据包的判定
- LINA 引擎根据 Snort 的判定丢弃或转发数据包

FTD提供两种部署模式和六种接口模式，如图所示：



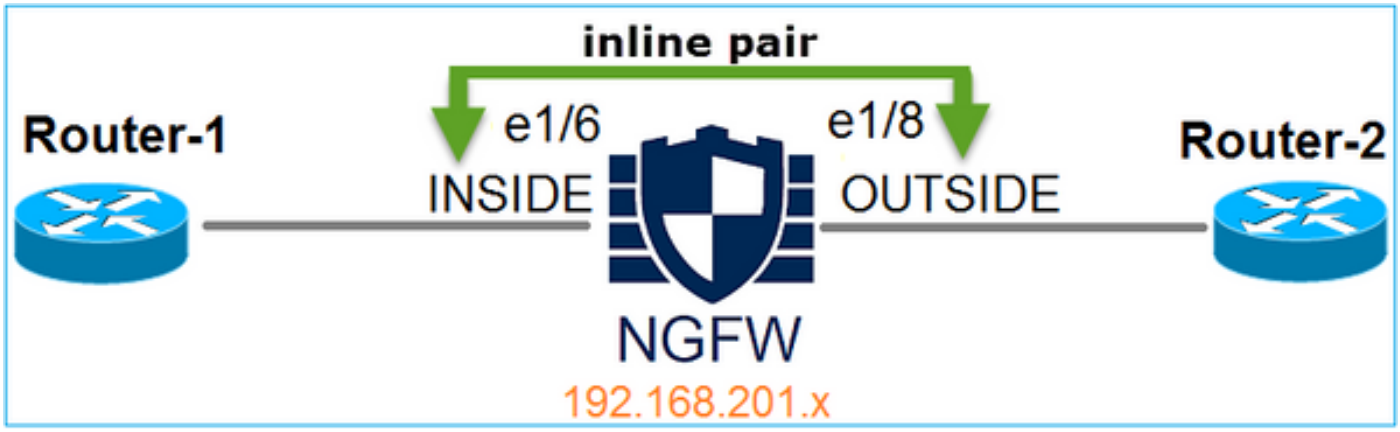
注意：您可以在单个FTD设备上混合接口模式。

以下是各种FTD部署和接口模式的简要概述：

FTD接口模式	FTD部署模式	描述	可以丢弃流量
已路由	已路由	完整的LINA引擎和Snort引擎检查	Yes
交换	透明	完整的LINA引擎和Snort引擎检查	Yes
内联对	路由或透明	部分LINA引擎和完全Snort引擎检查	Yes
带分路器的内联对	路由或透明	部分LINA引擎和完全Snort引擎检查	无
被动	路由或透明	部分LINA引擎和完全Snort引擎检查	无
被动(ERSPAN)	已路由	部分LINA引擎和完全Snort引擎检查	无

在FTD上配置内联对接口

网络图



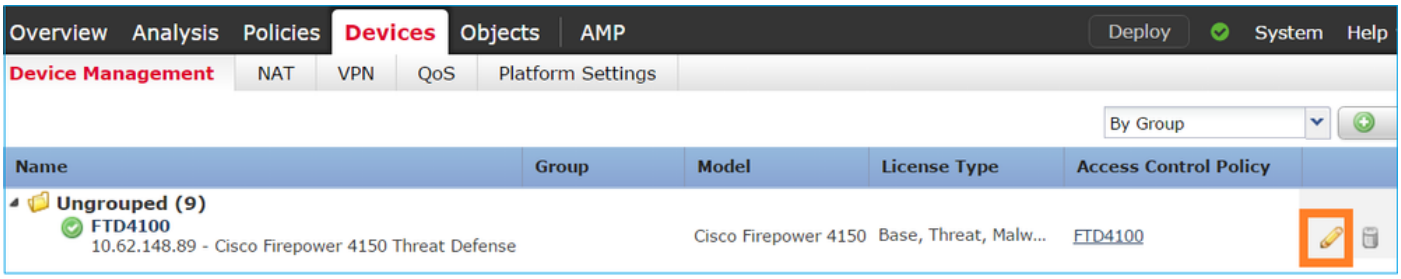
要求

按照以下要求在内联对模式下配置物理接口e1/6和e1/8:

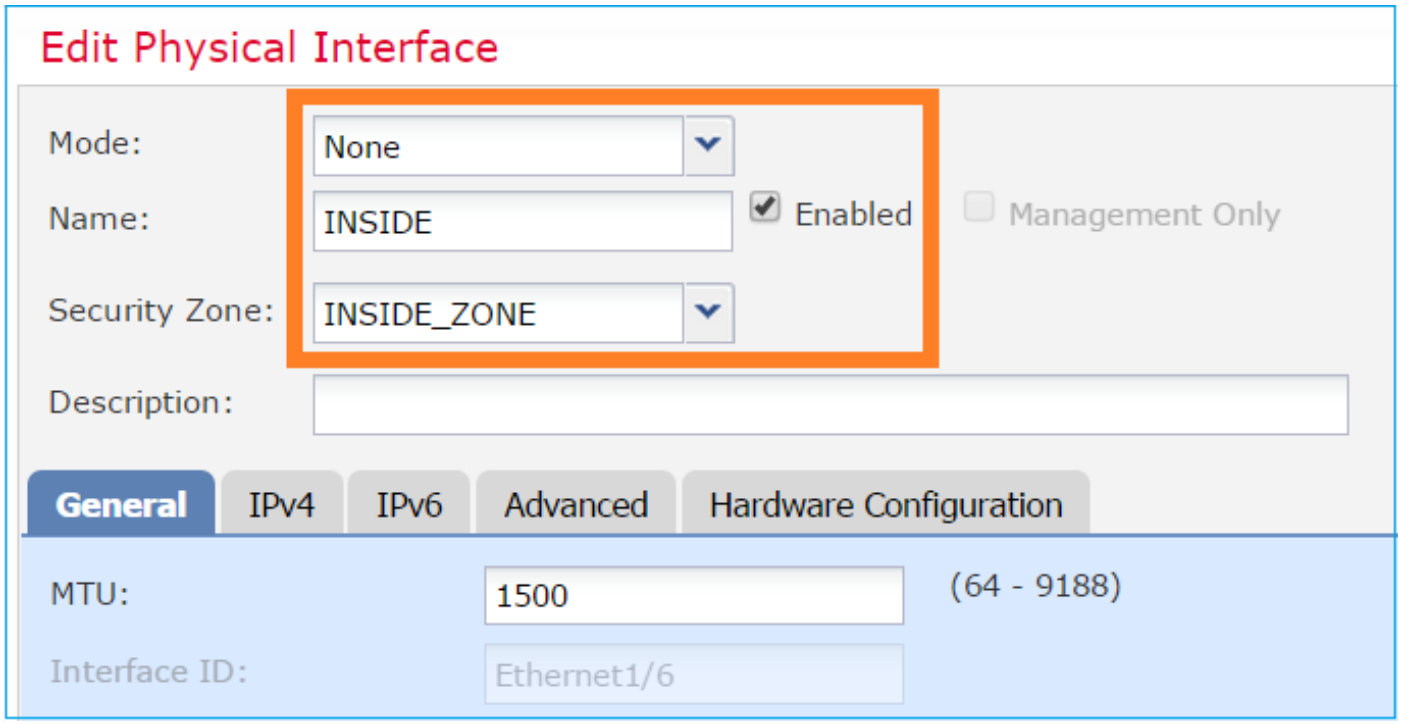
接口	e1/6	e1/8
名称	内部	外部
安全区域	INSIDE_ZONE	OUTSIDE_ZONE
内联集名称	内联对1	
内联集MTU	1500	
FailSafe	启用	
传播链路状态	启用	

解决方案

步骤1:要配置各个接口，请导航到Devices > Device Management，选择适当的设备并选择Edit，如图所示。

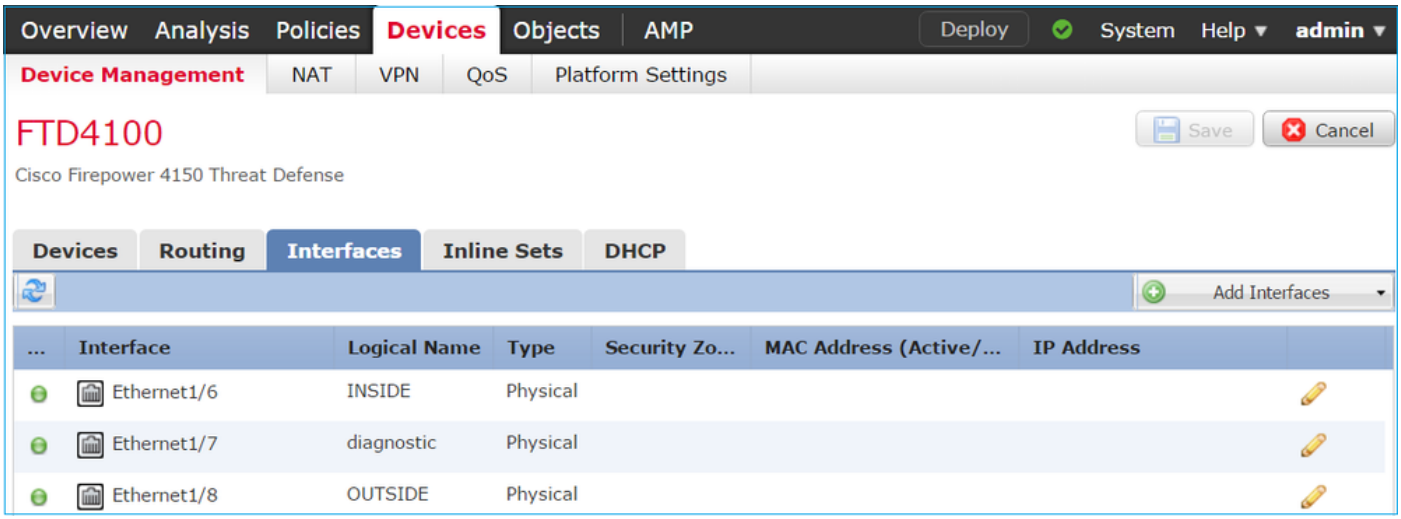


接下来，为接口指定Name和Tick Enabled，如图所示。



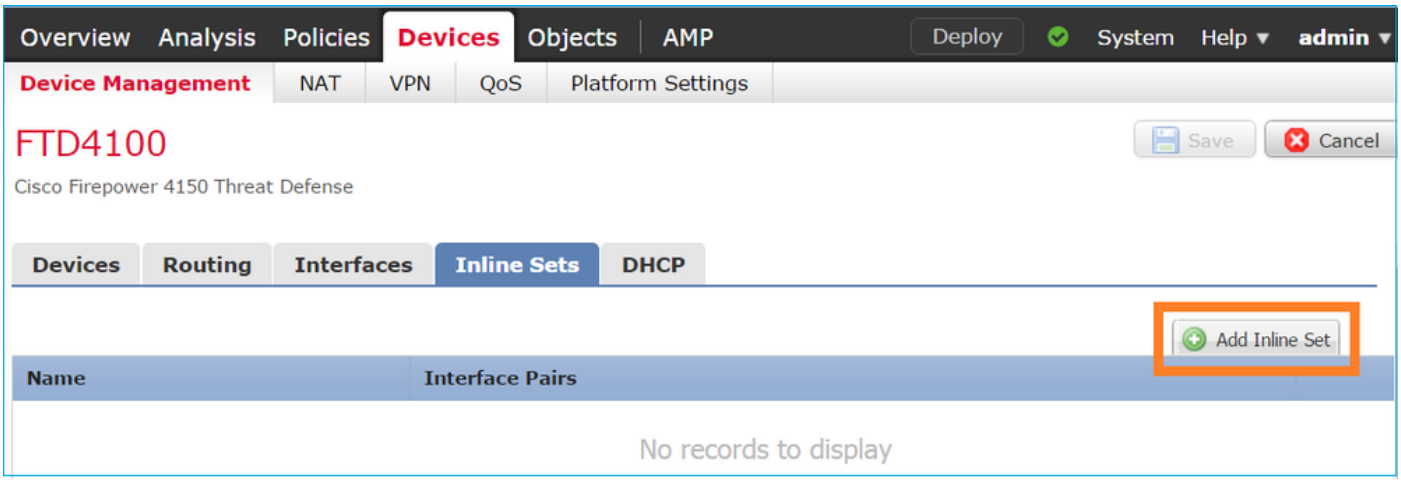
注:Name是接口的名称。

对于接口Ethernet1/8也是类似的。最终结果如图所示。

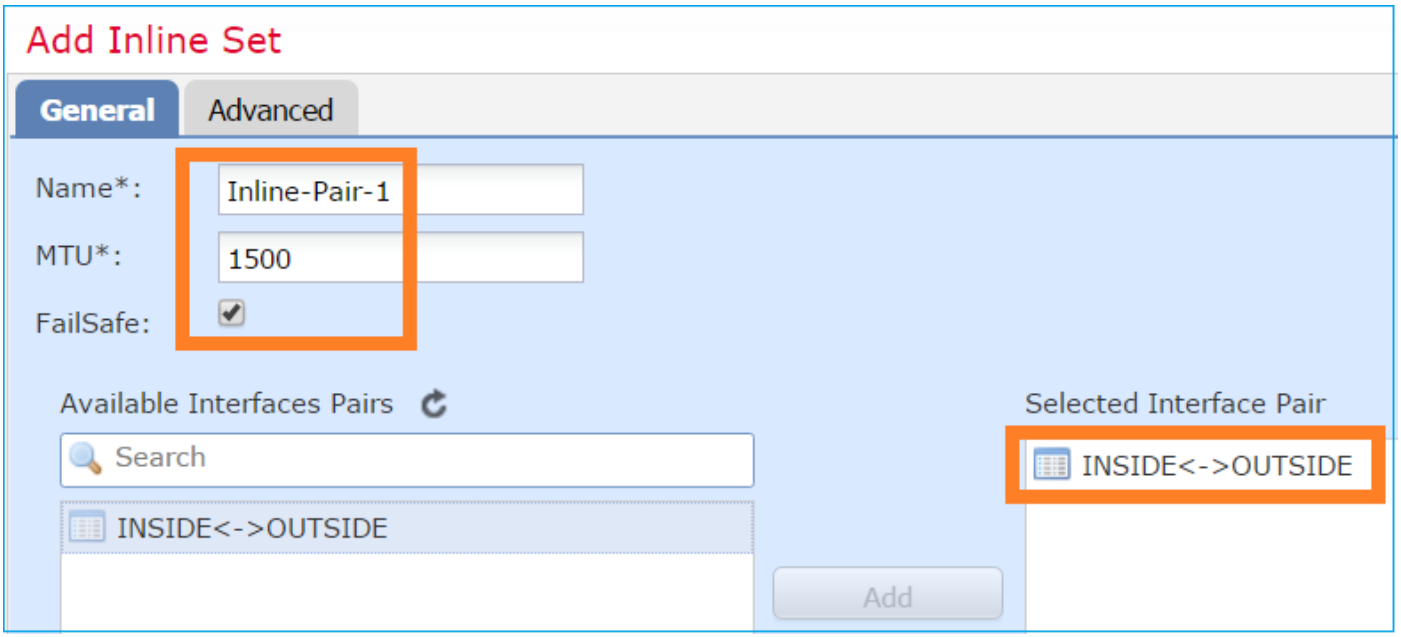


第二步：配置内联对。

导航到内联集>添加内联集，如图所示。

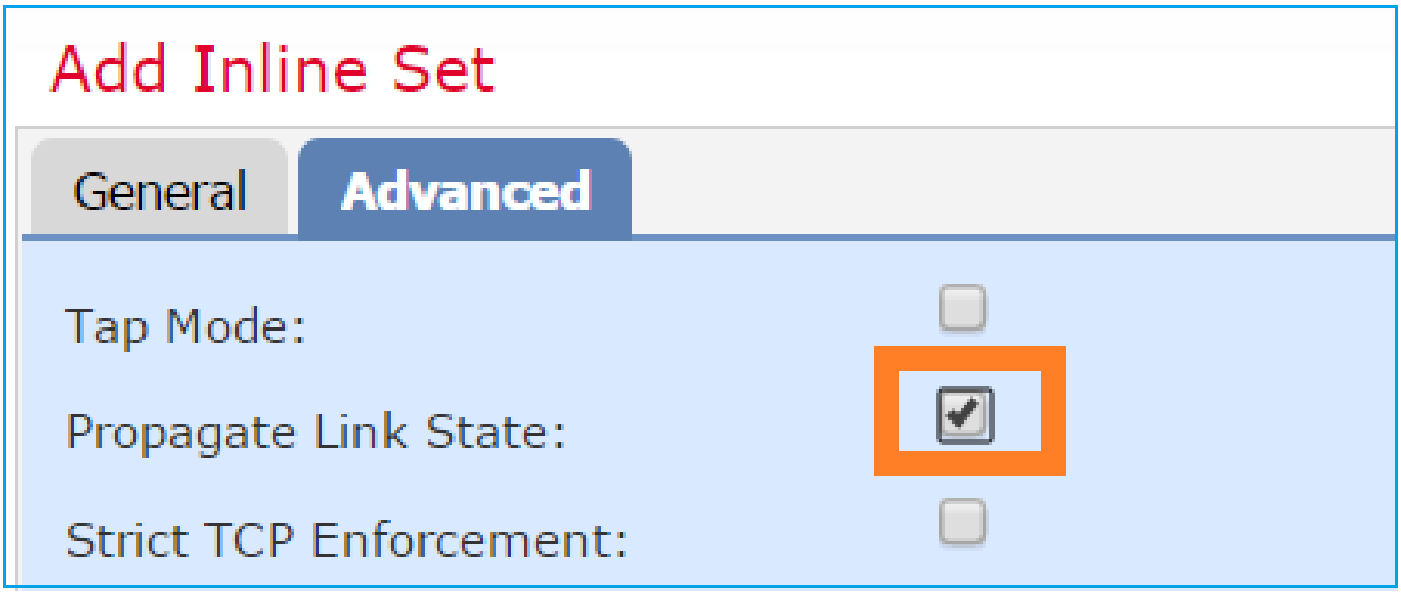


第三步：按照图中所示的要求配置General设置。



注意：Failsafe允许流量未经检查通过内联对，以防接口缓冲区已满（通常在设备过载或Snort引擎过载时看到）。接口缓冲区大小是动态分配的。

第四步：如图所示，在Advanced Settings中启用Propagate Link State选项。



当内联集中的一个接口关闭时，链路状态传播会自动关闭内联接口对中的第二个接口。

第五步：保存更改并部署。

验证

使用本部分可确认配置能否正常运行。

从FTD CLI验证内联对配置。

解决方案

登录到FTD CLI并验证内联对配置：

```
> 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：网桥组ID是一个不同于0的值。如果“分路模式”打开，则值为0

接口和名称信息：

<#root>

```
>
show nameif

Interface                Name                    Security
Ethernet1/6              INSIDE                    0

Ethernet1/7              diagnostic                0
Ethernet1/8              OUTSIDE                   0

>
```

检验接口状态：

<#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
```

检验物理接口信息：

<#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
>
```

检验FTD内联对接口操作

本节介绍以下验证检查以验证内联对操作：

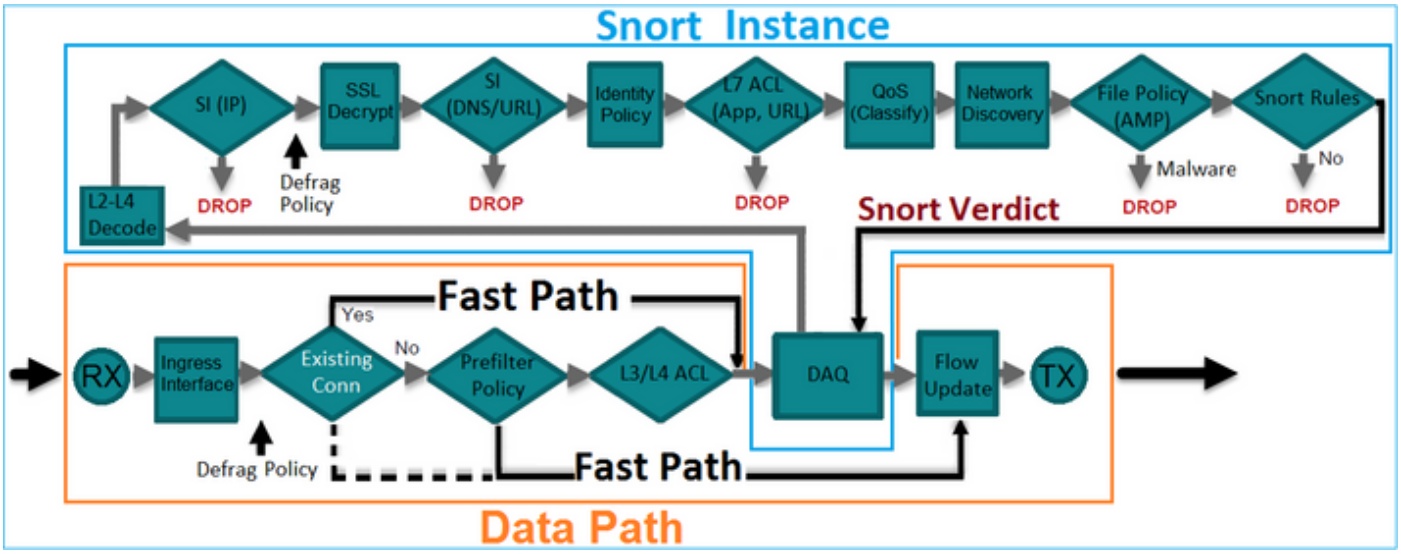
- 验证1.使用Packet Tracer
- 验证2.启用带有跟踪的捕获，并通过内联对发送TCP同步/确认(SYN/ACK)数据包

- 验证3.使用防火墙引擎调试监控FTD流量
- 验证4.检验链路状态传播功能
- 验证5.配置静态网络地址转换(NAT)

解决方案

架构概述

当2个FTD接口在内联对模式下运行时，数据包的处理方式如图所示。

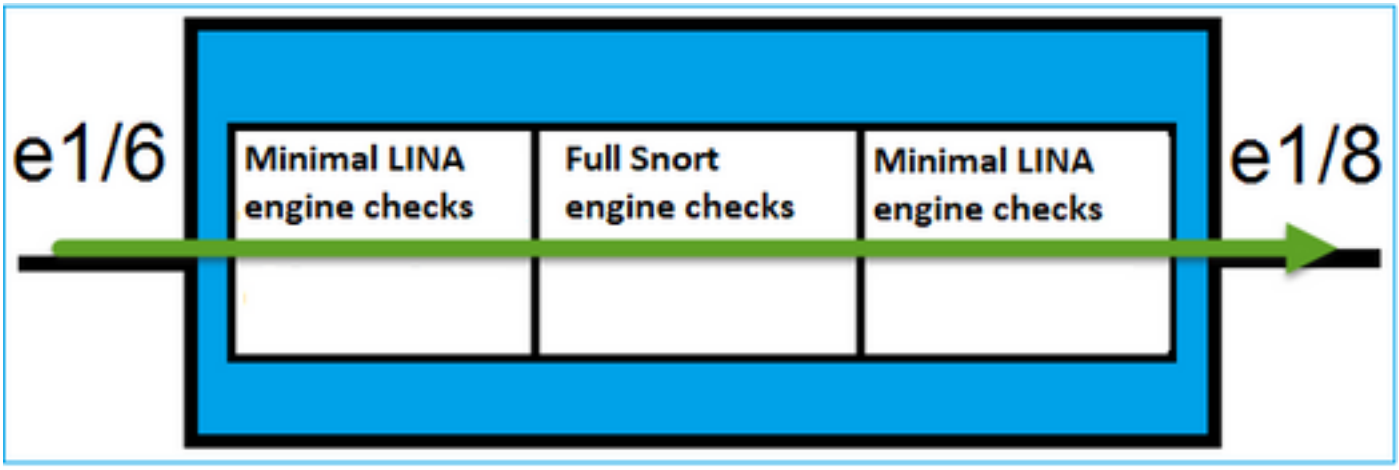


注意：只有物理接口才能成为内联对集的成员

基本原理

- 当您配置内联对2时，物理接口在内部桥接
- 非常类似于经典的内联入侵防御系统(IPS)
- 在路由或透明部署模式下可用
- 大多数LINA引擎功能（NAT、路由等）对于通过内联对的流不可用
- 可以丢弃中转流量
- 一些LINA引擎检查与完整的Snort引擎检查一起应用

最后一点可以可视化，如图所示：



验证1.使用Packet-Tracer

Packet Tracer输出模拟经过内联对的数据包，其中突出显示的重要点：

<#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 ingressed 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

>
```

验证2.通过内联对发送TCP SYN/ACK数据包

您可以使用可设计实用程序（如Scapy）的数据包生成TCP SYN/ACK数据包。此语法生成启用了SYN/ACK标志的3个数据包：

<#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)
```

在FTD CLI上启用此捕获并发送一些TCP SYN/ACK数据包：

<#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


>
```

通过FTD发送数据包后，您可以看到已创建的连接：

<#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

>
```

注意:b标志 — 传统ASA将丢弃未经请求的SYN/ACK数据包，除非启用TCP状态旁路。内联对模式下的FTD接口在TCP状态旁路模式下处理TCP连接，并且不丢弃不属于现有连接的TCP数据包。

注意：N标志 — 数据包由FTD Snort引擎进行检查。

捕获结果证明了这一点，因为您可以看到流经FTD的3个数据包：

<#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个数据包退出FTD设备：

<#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
>
```

通过跟踪第一个捕获数据包，可以揭示一些其他信息，如Snort引擎判定：

<#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
>
```

通过跟踪第二个捕获的数据包，可以显示数据包与当前连接匹配，因此它会绕过ACL检查，但仍会由Snort引擎进行检查：

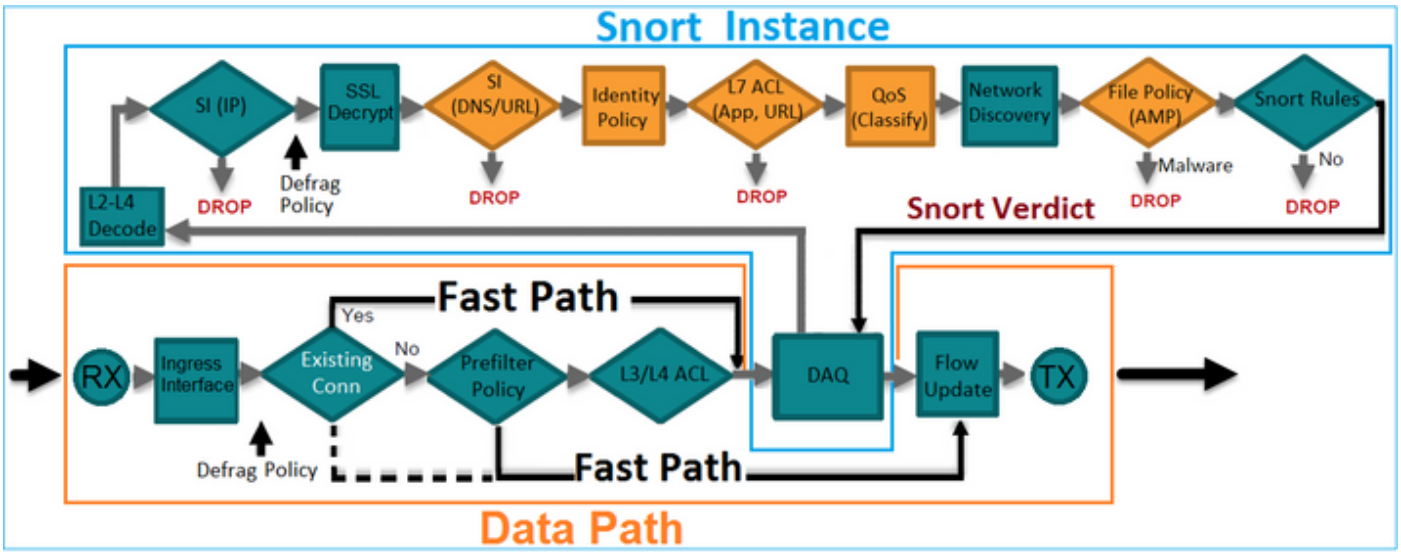
<#root>

```
>
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
>
```

验证3.允许流量的防火墙引擎调试

防火墙引擎调试针对FTD Snort引擎的特定组件（如图中所示的访问控制策略）运行：



通过内联对发送TCP SYN/ACK数据包时，可以在调试输出中看到：

<#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
```

验证4.检验链路状态传播

启用FTD上的缓冲区日志并关闭连接到e1/6接口的交换机端口。在FTD CLI上，您必须看到两个接口都关闭：

<#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日志显示：

<#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

>
```

内联集状态显示两个接口成员的状态：

<#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
>
```

注意2个接口状态的差异：

<#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
>
```

对于Ethernet1/8接口：

<#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
>
```

重新启用交换机端口后，FTD日志显示：

<#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) brin

>
```

验证5.配置静态 NAT

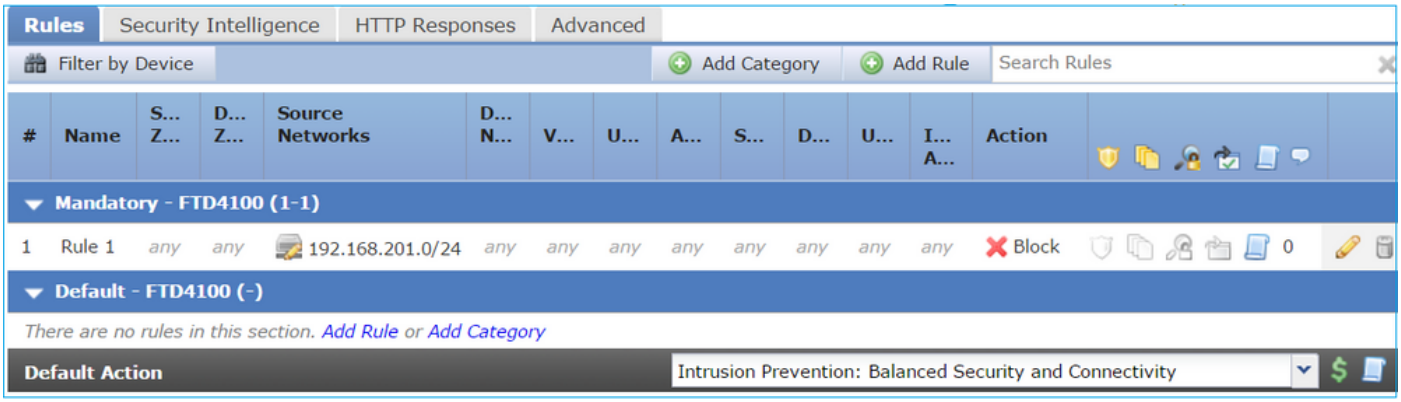
解决方案

内联、内联分路器或被动模式下运行的接口不支持NAT:

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

内联对接口模式上的阻止数据包

创建阻止规则，通过FTD内联对发送流量并观察行为，如图所示。



解决方案

通过跟踪启用捕获，并通过FTD内联对发送SYN/ACK数据包。流量被阻止：

<#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
```

通过跟踪，数据包可以显示：

<#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 ingressed 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
```

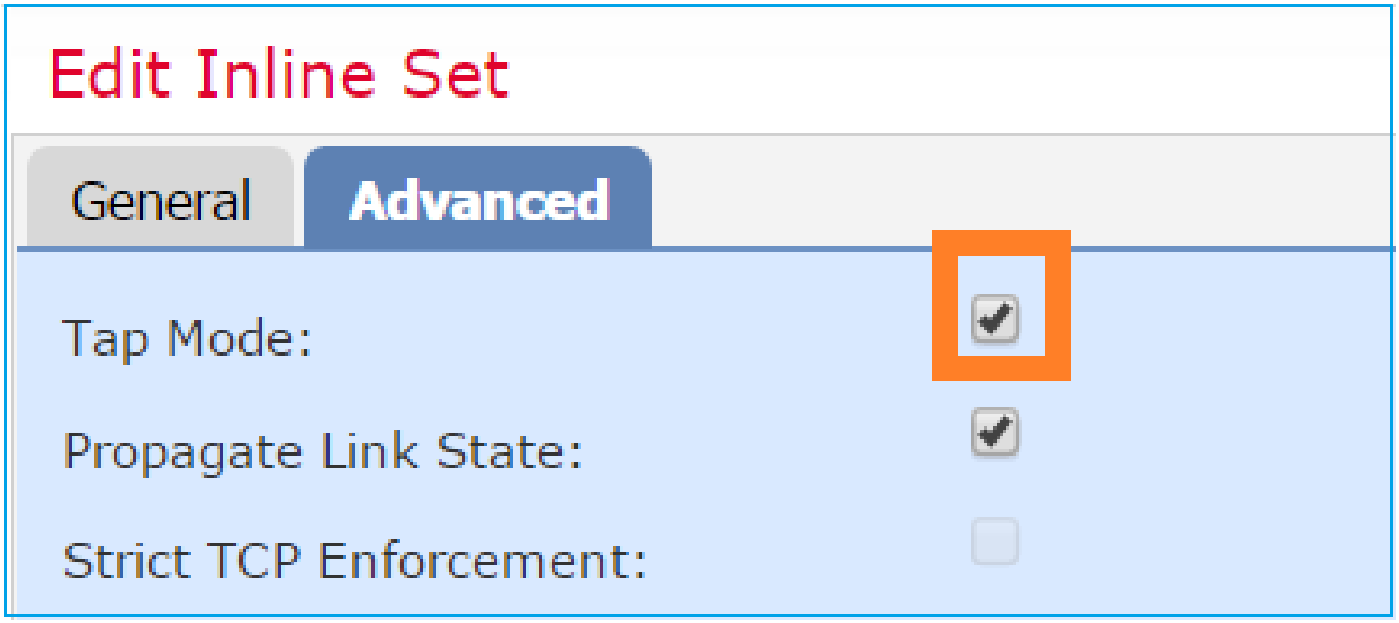
在此跟踪中，可以看到，数据包被FTD LINA引擎丢弃，并且未转发到FTD Snort引擎。

使用Tap配置内联对模式

在内联对上启用分路模式。

解决方案

导航到设备>设备管理>内联集>编辑内联集>高级并启用分路模式，如图所示。



确认

<#root>

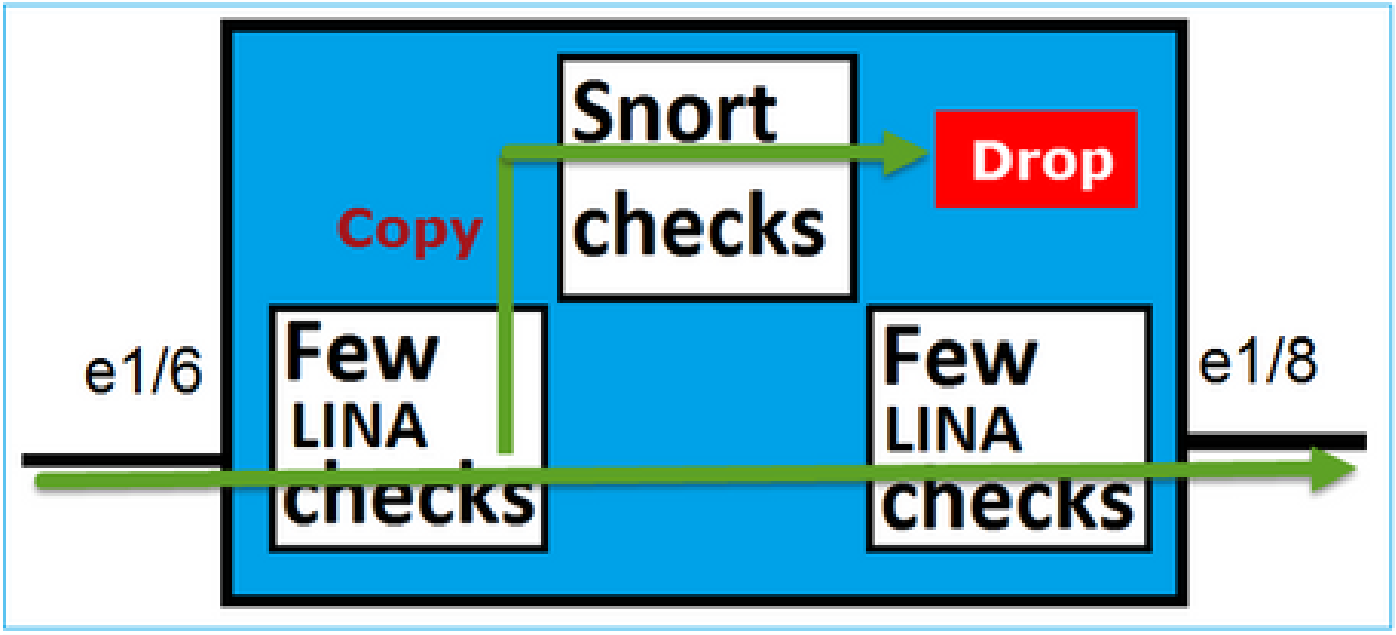
```
>

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
>
```

使用分路接口验证FTD内联对

基本原理

- 使用分路2配置内联对时，物理接口在内部桥接
- 在路由或透明部署模式下可用
- 大多数LINA引擎功能（NAT、路由等）对于通过内联对的流不可用
- 无法丢弃实际流量
- 一些LINA引擎检查与完整的Snort引擎检查一起应用于实际流量的副本

最后一点如图所示：



带分路模式的内联对不会丢弃中转流量。通过数据包的跟踪，可以确认以下情况：

<#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
```

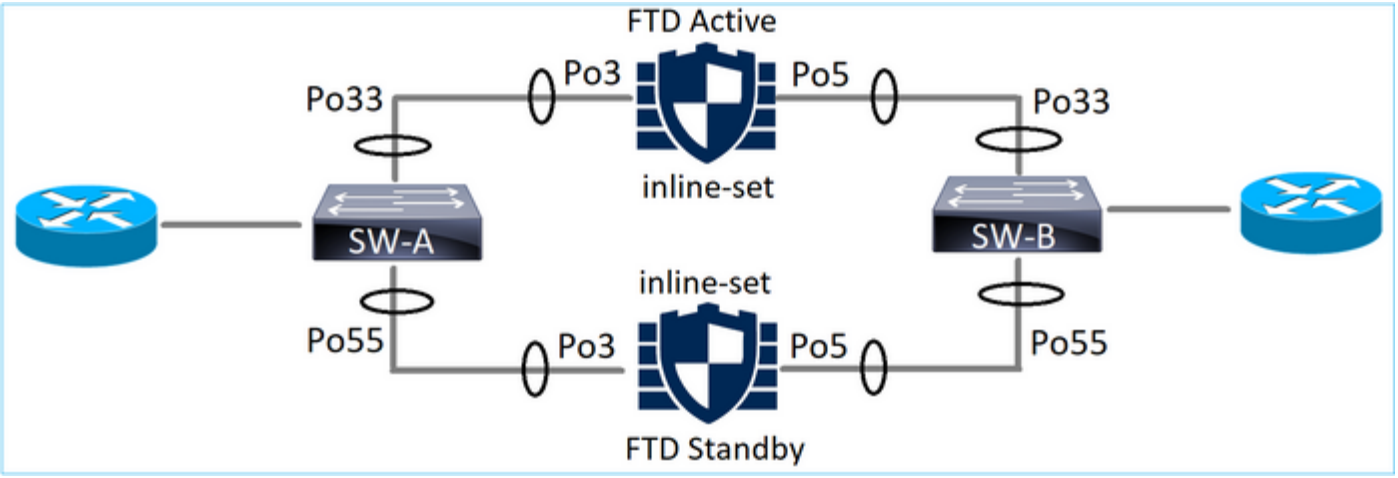
```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list


Phase: 3
Type: NGIPS-MODE
Subtype: ngips-mode

Result: ALLOW
Config:
Additional Information:

The flow ingressed 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
>
```

内联对和Etherchannel

您可以通过两种方式配置与etherchannel的内联对：

1. Etherchannel在FTD上终止
2. Etherchannel通过FTD（需要FXOS代码2.3.1.3及更高版本）

Etherchannel在FTD上终止



SW-A上的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上的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)
```

根据MAC地址学习，通过活动FTD转发流量：

<#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
```

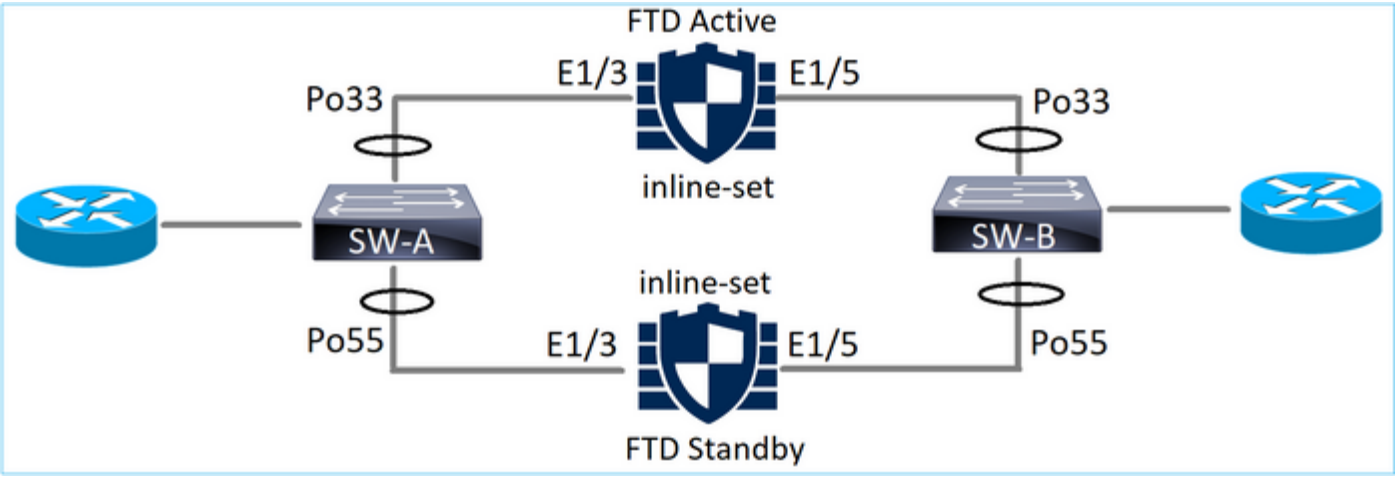
FTD上的内联集：

<#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：在FTD故障切换事件中，流量中断主要取决于交换机获取远程对等体的MAC地址所用的时间。

通过FTD的Etherchannel



SW-A上的Etherchannel:

<#root>

```
SW-A#
show etherchannel summary | i Po33|Po55

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

阻止通过备用FTD的LACP数据包：

<#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上的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)
```

根据MAC地址学习，通过活动FTD转发流量：

<#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上的内联集：

<#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：在本场景中，如果发生一个FTD故障切换事件，收敛时间主要取决于Etherchannel LACP协商，而根据中断时间，收敛时间可能会相当长。如果Etherchannel模式为ON(no LACP)，则收敛时间取决于MAC地址学习。

故障排除

当前没有可用于此配置的特定信息。

比较：内联对与带分路的内联对

	内联对	带分路器的内联对
show inline-set	> show inline-set 内联集内联对1 MTU is 1500 bytes 打开/激活故障安全模式 Failsecure模式关闭 分路模式关闭 Propagate-link-state选项为on 已禁用硬件旁路模式 接口对[1]: 接口：Ethernet1/6“内部” 当前状态：UP 接口：Ethernet1/8“OUTSIDE” 当前状态：UP 网桥组ID:509 >	> show inline-set 内联集内联对1 MTU is 1500 bytes 打开/激活故障安全模式 Failsecure模式关闭 分路模式已打开 Propagate-link-state选项为on 已禁用硬件旁路模式 接口对[1]: 接口：Ethernet1/6“内部” 当前状态：UP 接口：Ethernet1/8“OUTSIDE” 当前状态：UP 网桥组ID:0 >
show interface	> show interface e1/6 接口Ethernet1/6“INSIDE”，启用，线路协议启用 硬件为EtherSVI，BW 1000 Mbps，DLY 1000 usec MAC地址5897.bdb9.770e，MTU 1500 IPS接口模式：内联，内联集：内联对–1 未分配IP地址 “INSIDE”的流量统计信息： 3957个数据包输入，264913字节 144个数据包输出，58664字节 4个数据包被丢弃 1分钟输入速率0数据包/秒，26字节/秒 1分钟输出速率0 pkts/sec，7字节/sec 1分钟丢弃率，0数据包/秒 5分钟输入速率0数据包/秒，28字节/秒 5分钟输出速率0 pkts/sec，9字节/sec	> show interface e1/6 接口Ethernet1/6“INSIDE”，启用，线路协议启用 硬件为EtherSVI，BW 1000 Mbps，DLY 1000 usec MAC地址5897.bdb9.770e，MTU 1500 IPS接口模式：inline-tap，Inline-Set:Inline-Pair-1 未分配IP地址 “INSIDE”的流量统计信息： 24个数据包输入，1378字节 0个数据包输出，0个字节 丢弃了24个数据包 1分钟输入速率0数据包/秒，0字节/秒 1分钟输出速率0 pkts/sec，0字节/sec 1分钟丢弃率，0数据包/秒 5分钟输入速率0数据包/秒，0字节/秒 5分钟输出速率0 pkts/sec，0字节/sec 5分钟丢弃率，0数据包/秒 > show interface e1/8

	5分钟丢弃率，0数据包/秒 > show interface e1/8 Ethernet1/8接口“OUTSIDE”，启用，线路协议启用 硬件为EtherSVI，BW 1000 Mbps，DLY 1000 usec MAC地址5897.bdb9.774d，MTU 1500 IPS接口模式：内联，内联集：内联对–1 未分配IP地址 “OUTSIDE”的流量统计信息： 输入144个数据包，55634字节 3954数据包输出，339987字节 0个数据包被丢弃 1分钟输入速率0数据包/秒，7字节/秒 1分钟输出速率0 pkts/sec，37字节/sec 1分钟丢弃率，0数据包/秒 5分钟输入速率0数据包/秒，8字节/秒 5分钟输出速率0 pkts/sec，39字节/sec 5分钟丢弃率，0数据包/秒 >	Ethernet1/8接口“OUTSIDE”，启用，线路协议启用 硬件为EtherSVI，BW 1000 Mbps，DLY 1000 usec MAC地址5897.bdb9.774d，MTU 1500 IPS接口模式：inline-tap，Inline-Set:Inline-Pair-1 未分配IP地址 “OUTSIDE”的流量统计信息： 输入1个数据包，441字节 0个数据包输出，0个字节 1个数据包被丢弃 1分钟输入速率0数据包/秒，0字节/秒 1分钟输出速率0 pkts/sec，0字节/sec 1分钟丢弃率，0数据包/秒 5分钟输入速率0数据包/秒，0字节/秒 5分钟输出速率0 pkts/sec，0字节/sec 5分钟丢弃率，0数据包/秒 >
使用阻止规则处理数据包	> show capture CAPI packet-number 1 trace 捕获了3个数据包 1:16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80:S 0:0(0)ack 0 win 8192 阶段：1 类型：CAPTURE 子类型： 结果：允许 Config : 其它信息： MAC访问列表 阶段：2 类型：ACCESS-LIST 子类型： 结果：允许	> show capture CAPI packet-number 1 trace 捕获了3个数据包 1:16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80:S 0:0(0)win 8192 阶段：1 类型：CAPTURE 子类型： 结果：允许 Config : 其它信息： MAC访问列表 阶段：2 类型：ACCESS-LIST 子类型： 结果：允许 Config :

	Config : 隐式规则 其它信息： MAC访问列表 阶段：3 类型：NGIPS-MODE 子类型：ngips-mode 结果：允许 Config : 其它信息： 流进入配置为NGIPS模式的接口并应用NGIPS服务 阶段：4 类型：ACCESS-LIST 子类型：日志 结果：丢弃 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：访问策略：FTD4100 — 必备/1 access-list CSM_FW_ACL_ remark rule-id 268441600: L4规则：规则1 其它信息： 结果： input-interface:INSIDE input-status: up input-line-status: up 操作：丢弃 丢弃原因：(acl-drop)流被配置的规则拒绝 1个数据包显示 >	隐式规则 其它信息： MAC访问列表 阶段：3 类型：NGIPS-MODE 子类型：ngips-mode 结果：允许 Config : 其它信息： 流进入配置为NGIPS模式的接口并应用NGIPS服务 阶段：4 类型：ACCESS-LIST 子类型：日志 结果：本应已丢弃 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：访问策略：FTD4100 — 必备/1 access-list CSM_FW_ACL_ remark rule-id 268441600: L4规则：规则1 其它信息： 结果： input-interface:INSIDE input-status: up input-line-status: up 操作：访问列表已丢弃，但由于内联分路而转发数据包 1个数据包显示 >

摘要

- 当您使用内联对模式时，数据包主要通过FTD Snort引擎
- TCP连接在TCP状态旁路模式下处理
- 从FTD LINA引擎的角度来看，应用ACL策略
- 当内联对模式处于使用状态时，由于数据包是内联处理的，因此可以阻止它们
- 启用分路模式时，数据包副本会在内部进行检测并丢弃，同时实际流量不会经过修改的FTD

相关信息

- Cisco Firepower NGFW
- 技术支持和文档 - Cisco Systems

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。