在内联对模式下配置FTD接口

目录

简介

先决条件

- 要求
- 使用的组件
- 相关产品

背景信息

在FTD上配置内联对接口

- 网络图

验证

检验FTD内联对接口操作

- 基本原理
- 验证1.使用Packet Tracer
- 验证2.通过内联对发送TCP SYN/ACK数据包
- 验证3.防火墙引擎调试允许的流量
- 验证4.验证链路状态传播
- 验证5.配置静态NAT
- 案例研究 — 通过内联集的不对称流量

内联对接口模式上的阻止数据包

使用Tap配置内联对模式

使用分路接口验证FTD内联对

内联对和Etherchannel

- Etherchannel在FTD上终止
- 通过FTD的Etherchannel

故障排除

比较：内联对与带分路的内联对

摘要

相关信息

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

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Firepower 4112 FTD（代码7.x）
- Firepower管理中心(FMC)（代码7.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

本文档还可与以下硬件和软件版本一起使用：

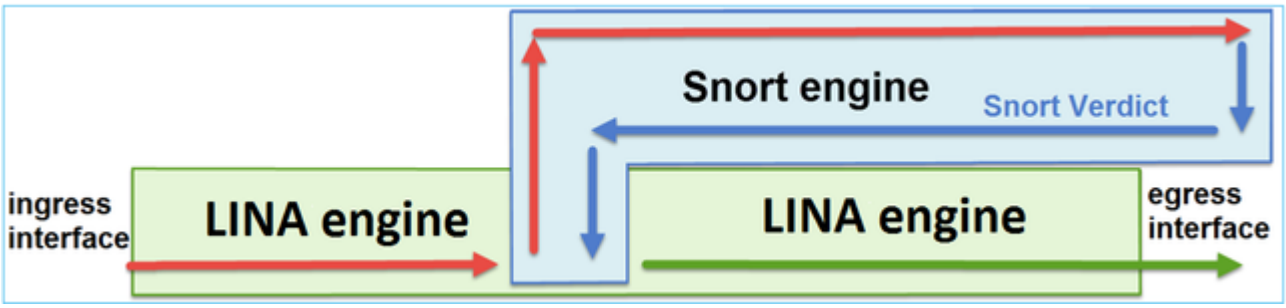
- FPR1000、FPR2100、FPR4100、FPR9300
- 安全防火墙3100和4200系列
- vFTD
- FTD软件代码6.2.x及更高版本

背景信息

FTD 是由两个主要引擎组成的统一软件映像：

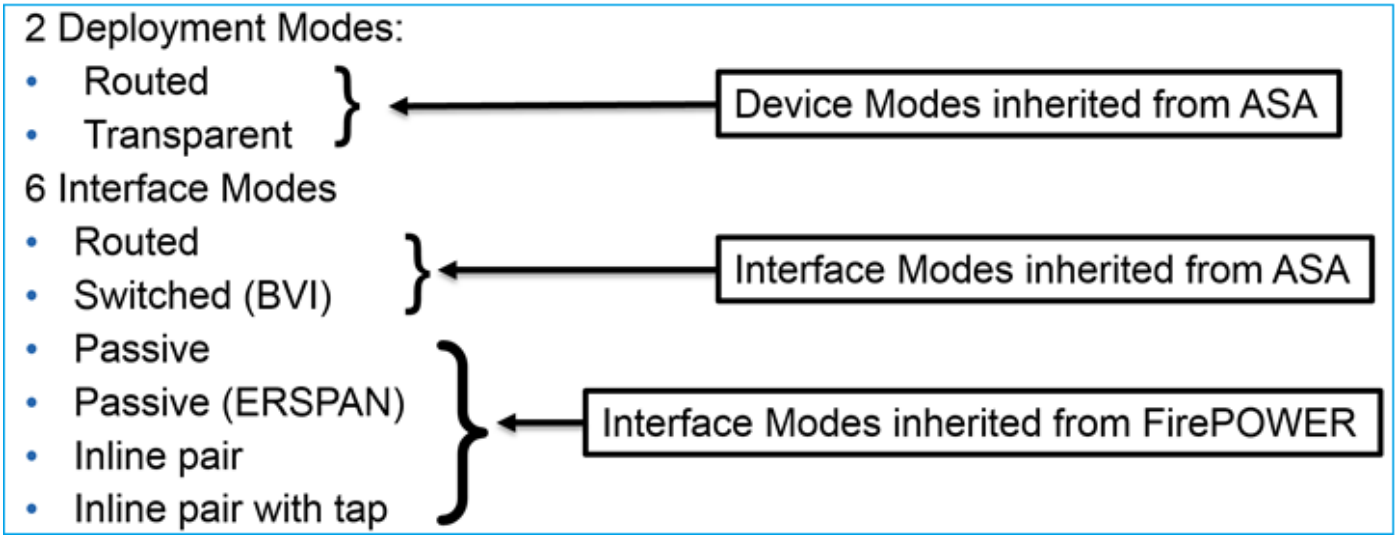
1. LINA 引擎
2. Snort 引擎

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策略需要该数据包，则由Snort引擎检查该数据包。
- 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引擎和完整Snort引擎检查。	Yes
带分路器的内联对	路由或透明	部分LINA引擎和完整Snort引擎检查。	无
被动	路由或透明	部分LINA引擎和完整Snort引擎检查。	无
被动(ERSPAN)	已路由	部分LINA引擎和完整Snort引擎检查。	无

在FTD上配置内联对接口

网络图



要求

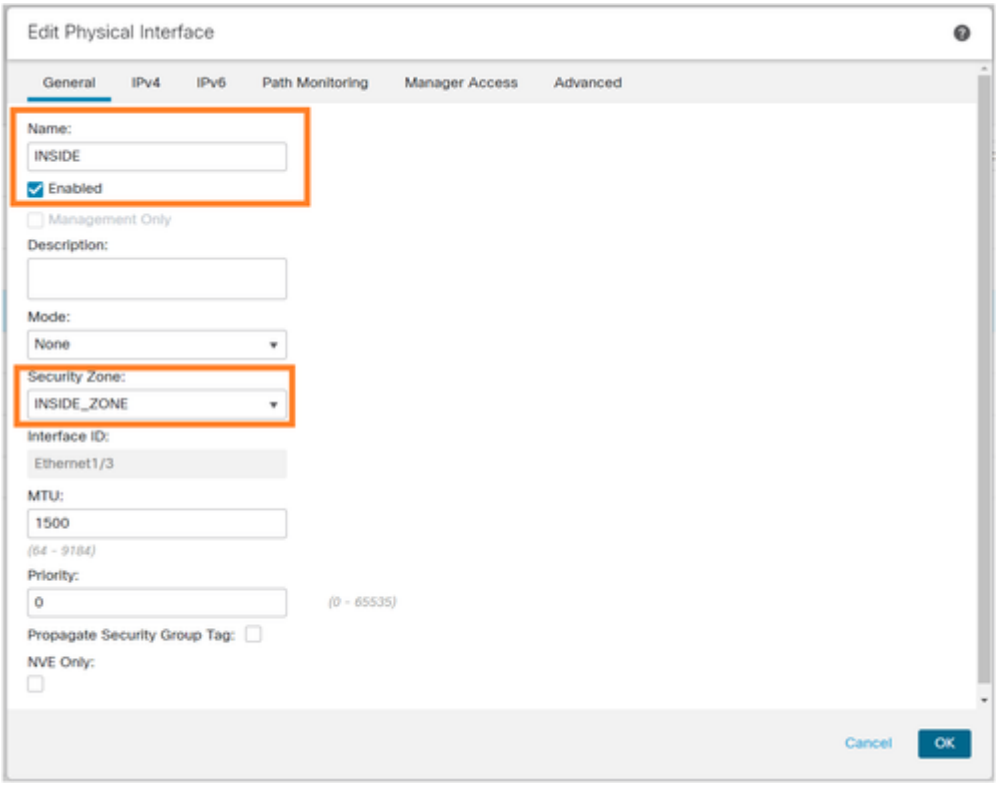
按照以下要求在内联对模式下配置物理接口e1/3和e1/4:

接口	e1/3	e1/4
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	
传播链路状态	启用	

解决方案

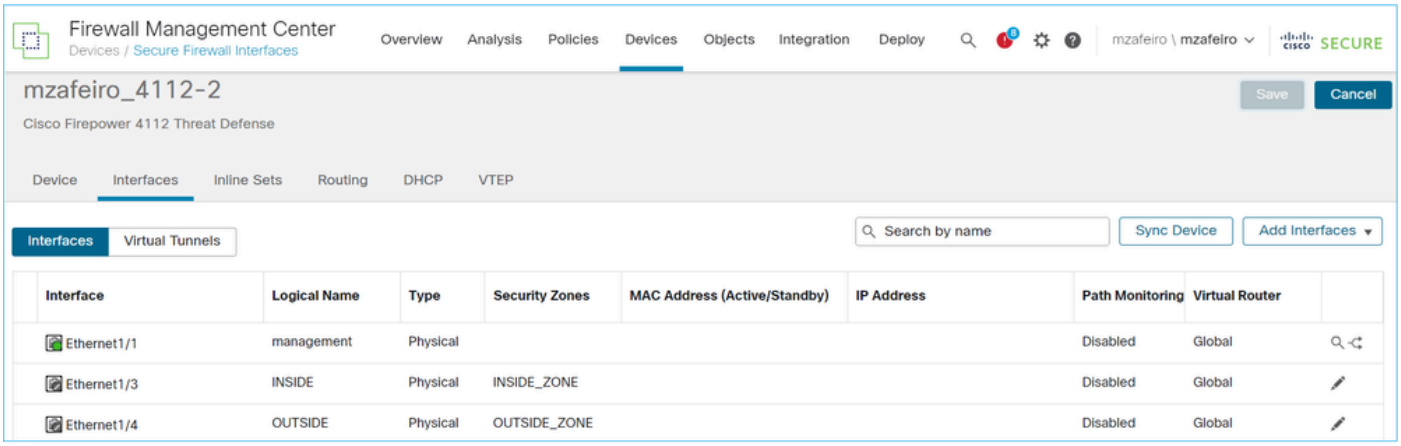
步骤1.要配置到各个接口，请导航到Devices > Device Management，选择适当的设备，然后选择Edit:

接下来，为接口指定Name和Enabled，如图所示。



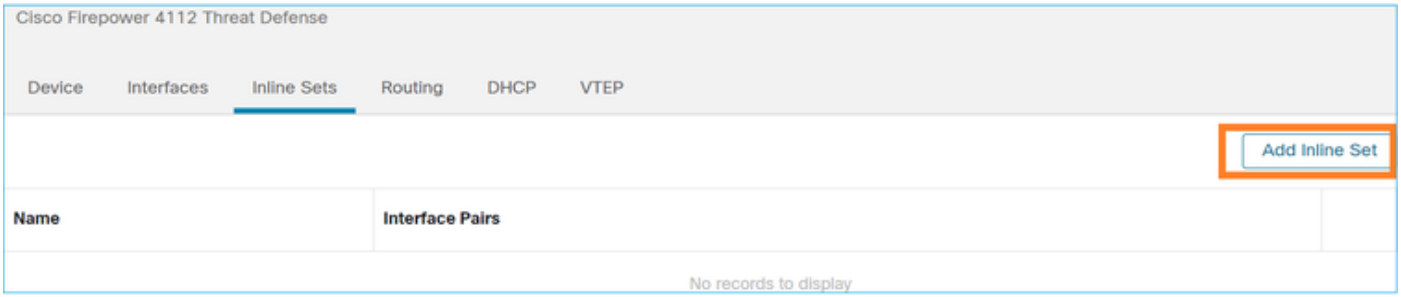
注意：Name是接口的名称。

同样，对于接口Ethernet1/4。最后结果如下所示：

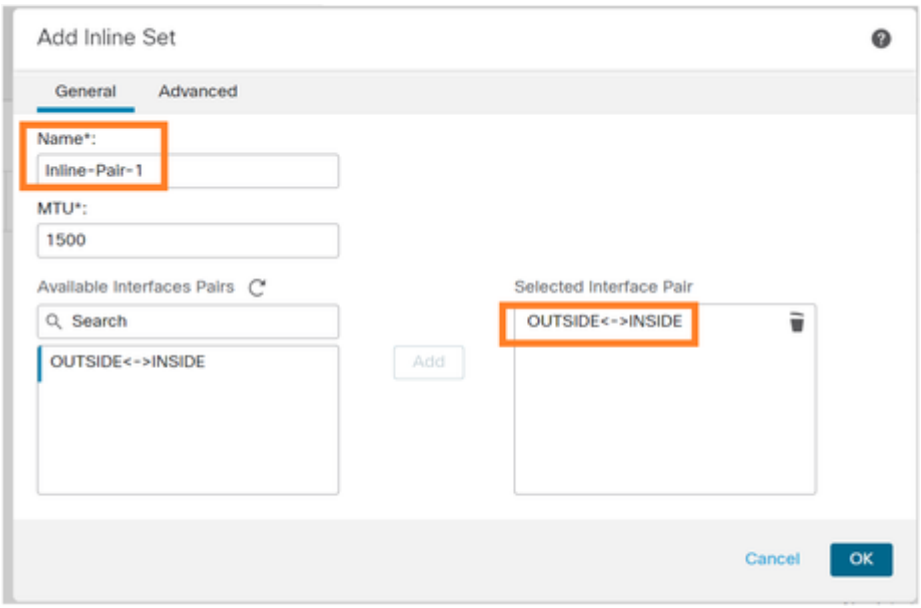


步骤2.配置内联对。

导航到内联集>添加内联集，如图所示。



步骤3.按照图中所示的要求配置General设置。



步骤4.在Advanced Settings中启用Propagate Link State选项，如图所示。



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。

步骤5.保存更改并进行部署。

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：

<#root>

```
firepower#

show inline-set



Inline-set Inline-Pair-1
  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 on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/4 "OUTSIDE"
      Current-Status: UP
    Interface: Ethernet1/3 "INSIDE"
      Current-Status: UP
    Bridge Group ID: 507
```

注意：网桥组ID是一个不同于0的值。如果“分路模式”为“打开”，则它为0。

接口和名称信息：

<#root>

```
firepower#
```

```
show nameif

Interface       Name             Security
Ethernet1/1     management        0
Ethernet1/3     INSIDE            0
Ethernet1/4     OUTSIDE           0
```

检验接口状态：

```
<#root>
firepower#
 show interface ip brief

Interface             IP-Address    OK? Method Status Protocol
Internal-Control0/0   unassigned    YES unset  up     up
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
Internal-Data0/3      unassigned    YES unset  up     up
Internal-Data0/4      unassigned    YES unset  down   up
Ethernet1/1           203.0.113.130 YES unset  up     up

Ethernet1/3           unassigned    YES unset  up     up



Ethernet1/4           unassigned    YES unset  up     up
```

检验物理接口信息：

```
<#root>
firepower#
show interface e1/3

Interface Ethernet1/3 "INSIDE", is up, line protocol is up

  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
```

```
        MAC address ac4a.670e.641e, MTU 1500

IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1

        IP address unassigned
  Traffic Statistics for "INSIDE":
        170 packets input, 12241 bytes
         41 packets output, 7881 bytes
          9 packets dropped
    1 minute input rate 0 pkts/sec, 37 bytes/sec
    1 minute output rate 0 pkts/sec, 19 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec, 34 bytes/sec
    5 minute output rate 0 pkts/sec, 23 bytes/sec
    5 minute drop rate, 0 pkts/sec
```

检验FTD内联对接口操作

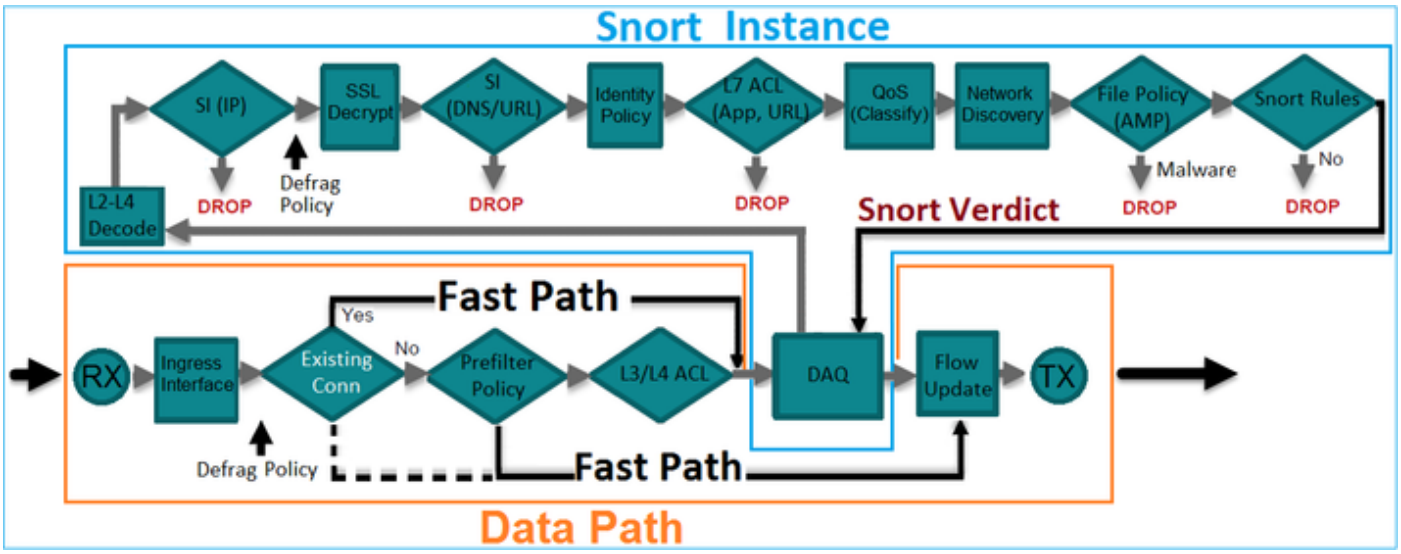
本节介绍以下验证检查以验证内联对操作：

- 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.验证链路状态传播功能。
- 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，会处理数据包，如图所示。

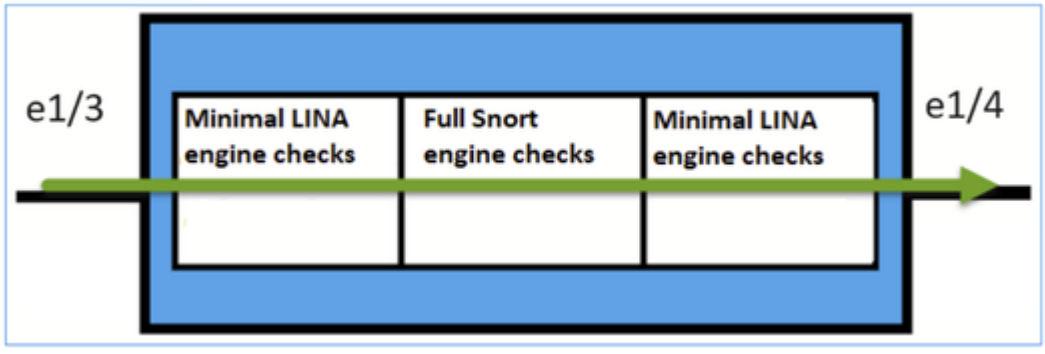


注意：只有物理接口可以成为内联对集的成员。

基本原理

- 当您配置内联对2物理时，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>

firepower#

packet-tracer input INSIDE tcp 192.168.201.50 1111 192.168.202.50 80

Phase: 1

Type: NGIPS-MODE

Subtype: ngips-mode

Result: ALLOW

Elapsed time: 11834 ns

Config:

Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 11834 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.201.50 host 192.168.202.50 rule-id 268451044
access-list CSM_FW_ACL_ remark rule-id 268451044: ACCESS POLICY: mzafeiro_2m - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268451044: L7 RULE: New-Rule-#1303-ALLOW
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 3

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Elapsed time: 2440 ns

Config:

Additional Information:

Ingress interface INSIDE is in NGIPS inline mode.

Egress interface OUTSIDE is determined by inline-set configuration

Phase: 4
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 68320 ns
Config:
Additional Information:
New flow created with id 1801, packet dispatched to next module

Phase: 5
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 18056 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 6
Type: SNORT
Subtype: identity
Result: ALLOW
Elapsed time: 13668 ns
Config:
Additional Information:
user id: no auth, realm id: 0, device type: 0, auth type: invalid, auth proto: basic, username: none, A
src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, abp src: none, abp dst: none, loc

Phase: 7
Type: SNORT
Subtype: firewall
Result: ALLOW
Elapsed time: 67770 ns
Config:
Network 0, Inspection 0, Detection 0, Rule ID 268451044
Additional Information:
Starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt:
Matched rule ids 268451044 - Allow

Phase: 8
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 11002 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Result:

input-interface: INSIDE(vrfid:0)

input-status: up

input-line-status: up

output-interface: OUTSIDE(vrfid:0)

output-status: up

output-line-status: up

```
Action: allow


Time Taken: 204924 ns
```

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>

firepower#

capture CAPI interface INSIDE trace match ip host 192.168.201.60 any


firepower#

capture CAPO interface OUTSIDE match ip host 192.168.201.60 any
```

捕获显示3个SYN/ACK数据包经过FTD:

```
<#root>

firepower#

show capture CAPI



3 packets captured

1: 09:20:18.206440 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
2: 09:20:18.208180 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3: 09:20:18.210026 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3 packets shown
firepower#

show capture CAPO



3 packets captured

1: 09:20:18.206684 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
2: 09:20:18.208210 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3: 09:20:18.210056 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3 packets shown
```

第一个捕获数据包的Trace显示一些附加信息，如Snort引擎判定：

```
<#root>

firepower#
```

show capture CAPI packet-number 1 trace

```
3 packets captured

1: 09:20:18.206440 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Elapsed time: 5978 ns
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 5978 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.201.50 object-group FMC_INLINE_dst_rule_2684510
access-list CSM_FW_ACL_ remark rule-id 268451044: ACCESS POLICY: mzafeiro_2m - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268451044: L7 RULE: New-Rule-#1303-ALLOW
object-group network FMC_INLINE_dst_rule_268451044
network-object 192.168.202.50 255.255.255.255
network-object 192.168.201.60 255.255.255.255
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 3
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 1952 ns
Config:
Additional Information:
Ingress interface INSIDE is in NGIPS inline mode.
Egress interface OUTSIDE is determined by inline-set configuration

Phase: 4
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 45872 ns
Config:
Additional Information:
New flow created with id 1953, packet dispatched to next module

Phase: 5
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 18544 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 6
Type: SNORT
```

Subtype: identity
Result: ALLOW
Elapsed time: 25182 ns
Config:
Additional Information:
user id: no auth, realm id: 0, device type: 0, auth type: invalid, auth proto: basic, username: none, A
src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, abp src: none, abp dst: none, loc

Phase: 7

Type: SNORT

Subtype: firewall

Result: ALLOW

Elapsed time: 50924 ns

Config:

Network 0, Inspection 0, Detection 0, Rule ID 268451044

Additional Information:

Starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 0

Matched rule ids 268451044 - Allow

Phase: 8
Type: SNORT
Subtype: appid

```
Result: ALLOW
Elapsed time: 17722 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 172152 ns


1 packet shown
```

第二个捕获的数据包的跟踪显示数据包与当前连接匹配，因此它会绕过ACL检查，但仍由Snort引擎进行检查：

```
<#root>

firepower#

show capture CAPI packet-number 2 trace



3 packets captured

2: 09:20:18.208180 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 1952 ns
Config:
Additional Information:

Found flow with id 1953, using existing flow



Phase: 2
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 7320 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 3
Type: SNORT
```

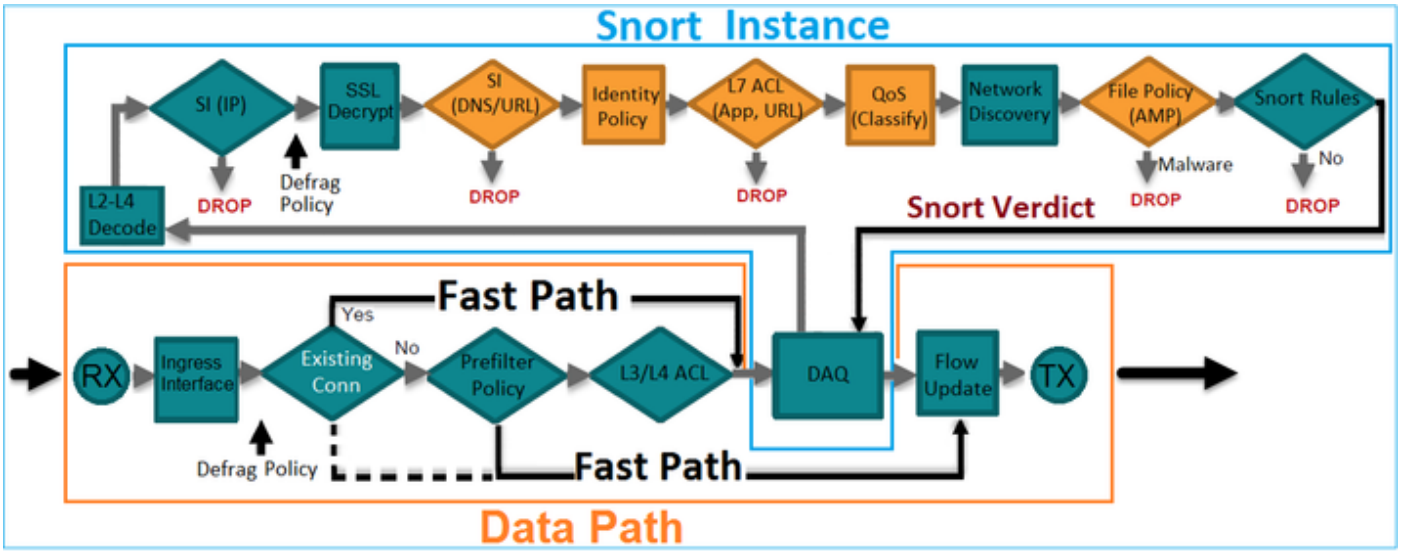
```
Subtype: appid
Result: ALLOW
Elapsed time: 1860 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
Action: allow
Time Taken: 11132 ns


1 packet shown
```

验证3.防火墙引擎调试允许的流量

防火墙引擎调试针对FTD Snort引擎的特定组件（如访问控制策略）运行，如图所示：



通过内联对发送TCP SYN/ACK数据包时，可以在debug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.验证链路状态传播

启用FTD上的缓冲区日志并关闭连接到e1/4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>

firepower#

show interface ip brief


Interface              IP-Address    OK? Method Status     Protocol
Internal-Control0/0    unassigned    YES unset  up         up
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
Internal-Data0/3        unassigned    YES unset  up         up
Internal-Data0/4        unassigned    YES unset  down       up
Ethernet1/1             203.0.113.130 YES unset  up         up

Ethernet1/3             unassigned    YES unset  admin down down



Ethernet1/4             unassigned    YES unset  down       down
```

FTD日志显示：

```
<#root>

firepower#

show log

...

May 28 2024 07:35:10: %FTD-4-411002: Line protocol on Interface Ethernet1/4, changed state to down



May 28 2024 07:35:10: %FTD-4-411004: Interface INSIDE, changed state to administratively down



May 28 2024 07:35:10: %FTD-4-411004: Interface Ethernet1/3, changed state to administratively down



May 28 2024 07:35:10: %FTD-4-812005: Link-State-Propagation activated on inline-pair due to failure of i



May 28 2024 07:35:10: %FTD-4-411002: Line protocol on Interface Ethernet1/3, changed state to down
```

内联集状态显示两个接口成员的状态：

```
<#root>

firepower#
```

show inline-set

```
Inline-set Inline-Pair-1
  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 on

```
  hardware-bypass mode is disabled
    Interface-Pair[1]:
    Interface: Ethernet1/4 "OUTSIDE"
```

Current-Status: Down(Propagate-Link-State-Activated)

```
    Interface: Ethernet1/3 "INSIDE"
```

Current-Status: Down(Administrative-Down-By-Propagate-Link-State)

```
Bridge Group ID: 507
```

注意两个接口状态的差异：

<#root>

firepower#

show interface e1/3

Interface Ethernet1/3 "INSIDE", is admin down, line protocol is down

```
  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
        MAC address ac4a.670e.641e, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1
```

Administrative-Down-By-Propagate-Link-State

```
        IP address unassigned
```

```
  Traffic Statistics for "INSIDE":
        2400 packets input, 165873 bytes
        1822 packets output, 178850 bytes
        17 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,  32 bytes/sec
      5 minute output rate 0 pkts/sec,  57 bytes/sec
      5 minute drop rate, 0 pkts/sec
firepower#
```

show interface e1/4

Interface Ethernet1/4 "OUTSIDE", is down, line protocol is down

```
  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
        MAC address ac4a.670e.640e, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1
```

Propagate-Link-State-Activated

```
        IP address unassigned
  Traffic Statistics for "OUTSIDE":
        1893 packets input, 158046 bytes
        2386 packets output, 213997 bytes
        67 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,  51 bytes/sec
      5 minute output rate 0 pkts/sec,  39 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>

May 28 2024 07:38:04: %FTD-4-411001: Line protocol on Interface Ethernet1/4, changed state to up

May 28 2024 07:38:04: %FTD-4-411003: Interface Ethernet1/3, changed state to administratively up

May 28 2024 07:38:04: %FTD-4-411003: Interface INSIDE, changed state to administratively up

```
May 28 2024 07:38:04: %FTD-4-812006: Link-State-Propagation de-activated on inline-pair due to recovery

May 28 2024 07:38:05: %FTD-4-411002: Line protocol on Interface Ethernet1/4, changed state to down
```

验证5.配置静态NAT

解决方案

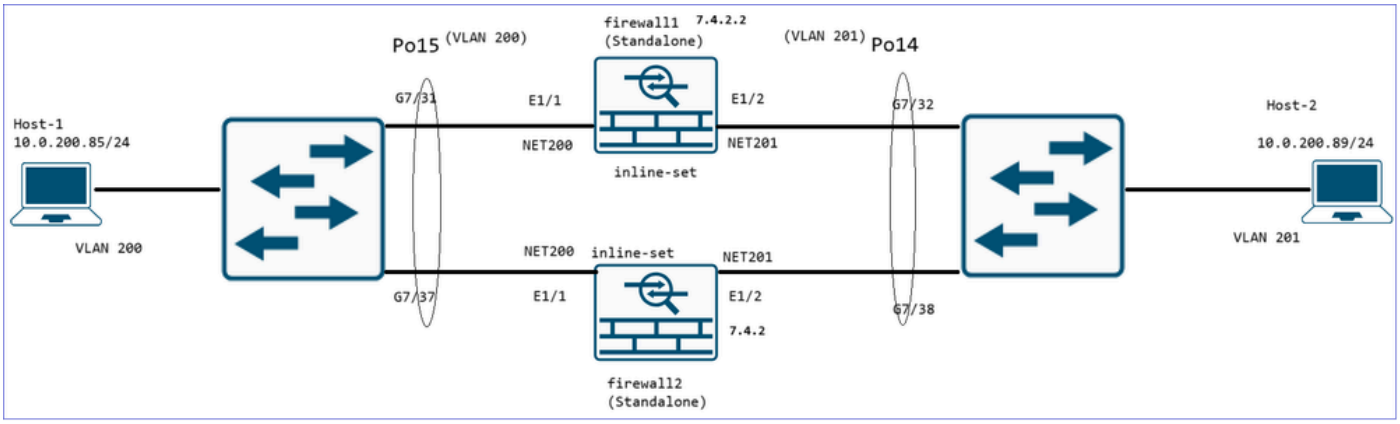
内联、内联分路器或被动模式下运行的接口不支持NAT:

Firepower管理中心配置指南，版本6.0.1

案例研究 — 通过内联集的不对称流量

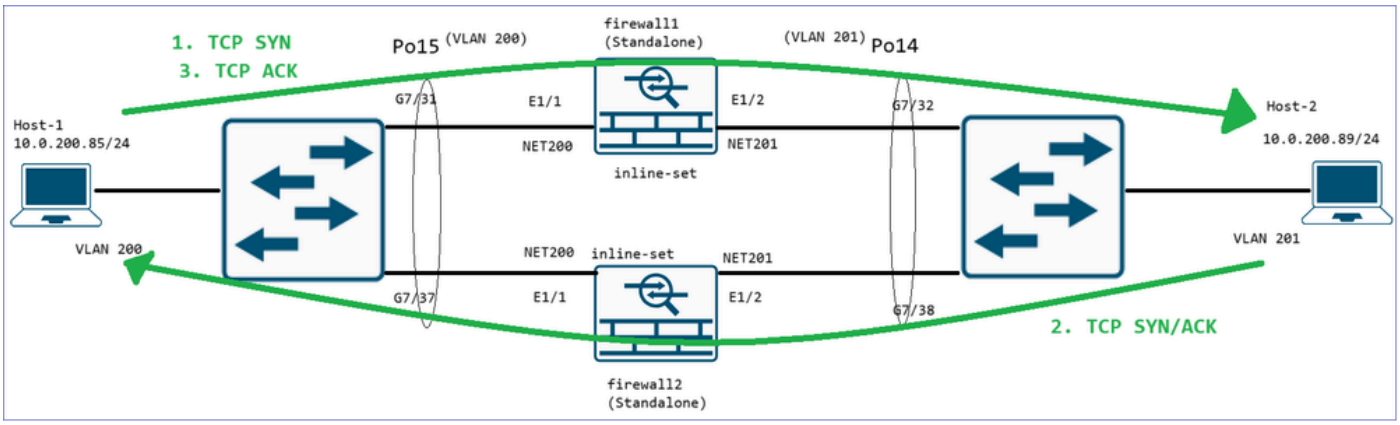
> 警告：在内联集（IPS模式）接口上，默认启用TCP状态旁路。如果在ACP Advanced Settings中配置了TSID或TLS解密策略，则它会以静默方式覆盖/禁用此默认TCP状态绕行行为，因此会实施TCP状态检查而不是绕过。
> 可观察症状：对于流经内联集的TCP状态旁路符合条件的流量（例如，流量流出并进入不同内联集的非对称流量场景），可以使用ASP drop tcp-not-syn(syslog 106015)丢弃数据包。

请考虑以下场景：



两个防火墙在独立模式下运行（它们甚至运行不同的软件版本），但处理来自相同端口通道接口的流量。

在这种情况下，由于端口通道负载均衡算法，可以具有非对称流量：



1. Host-1(10.0.200.85)向Host-2(10.0.200.89)发送TCP SYN。 此数据包通过firewall1。
2. Host-2(10.0.200.89)向Host-2(10.0.200.85)发送TCP SYN/ACK。 此数据包通过firewall2。
3. TCP三次握手完成，Host-1向Host-2发送TCP ACK。此数据包通过firewall1。

从Host-1的角度来看，已成功建立连接：

<#root>

```
root@kali:/ #

wget -O - http://10.0.200.89/10K


--2025-05-06 08:20:28--  http://10.0.200.89/10K
Connecting to 10.0.200.89:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10240 (10K)
Saving to: ‘STDOUT’
-                                                   100%[=============================================================
2025-05-06 08:20:28 (99.8 MB/s) - written to stdout [10240/10240]
```

firewall1上的数据包捕获仅显示从Host1到Host2的流量：

<#root>

```
firepower#

show capture
```

```
capture CAPI type raw-data trace interface NET200 [Capturing - 875 bytes]
  match ip host 10.0.200.85 host 10.0.200.89
capture CAPO type raw-data trace interface NET201 [Capturing - 875 bytes]
  match ip host 10.0.200.85 host 10.0.200.89
```

捕获内容：

```
<#root>

firepower#

show capture CAPI



9 packets captured

   1: 12:21:14.161689       10.0.200.85.44806 > 10.0.200.89.80:

S

1877376557:1877376557(0) win 64240 <mss 1460,sackOK,timestamp 2133104674 0,nop,wscale 7>
   2: 12:21:14.162924       10.0.200.85.44806 > 10.0.200.89.80: .

ack

 3274105192 win 502 <nop,nop,timestamp 2133104676 1658009126>
   3: 12:21:14.163077       10.0.200.85.44806 > 10.0.200.89.80: P 1877376558:1877376687(129) ack 327410
   4: 12:21:14.164801       10.0.200.85.44806 > 10.0.200.89.80: . ack 3274106640 win 501 <nop,nop,times
   5: 12:21:14.164908       10.0.200.85.44806 > 10.0.200.89.80: . ack 3274108088 win 494
...
```

firewall2上的数据包捕获仅显示从Host2到Host1的流量：

```
<#root>

FTD1010-12#

show capture CAPI



11 packets captured

   1: 12:21:14.198949       10.0.200.89.80 > 10.0.200.85.44806:
```

```
S

 3274105191:3274105191(0)

ack

 1877376558 win 65160 <mss 1460,sackOK,timestamp 1658009126 2133104674,nop,wscale 7>
   2: 12:21:14.200001       10.0.200.89.80 > 10.0.200.85.44806: . ack 1877376687 win 509 <nop,nop,times
   3: 12:21:14.200825       10.0.200.89.80 > 10.0.200.85.44806: . 3274105192:3274106640(1448) ack 18773
   4: 12:21:14.200947       10.0.200.89.80 > 10.0.200.85.44806: . 3274106640:3274108088(1448) ack 18773
   5: 12:21:14.200963       10.0.200.89.80 > 10.0.200.85.44806: . 3274108088:3274109536(1448) ack 18773
   6: 12:21:14.200978       10.0.200.89.80 > 10.0.200.85.44806: . 3274109536:3274110984(1448) ack 18773
   7: 12:21:14.200993       10.0.200.89.80 > 10.0.200.85.44806: P 3274110984:3274112432(1448) ack
...
```

firewall1上的Syslogs显示，TCP SYN数据包创建了TCP状态旁路连接：

<#root>

```
firepower#

show logging


...
May 06 2025 12:21:14: %FTD-6-302303:

Built TCP state-bypass connection

 106977 from NET200:10.0.200.85/44806 (10.0.200.85/44806) to NET201:10.0.200.89/80 (10.0.200.89/80)
```

在firewall2上，TCP SYN/ACK数据包还创建了TCP状态旁路连接：

<#root>

```
FTD1010-12#

show logging


...
May 06 2025 12:21:14: %FTD-6-302303:
```

```
Built TCP state-bypass
```

```
connection
```

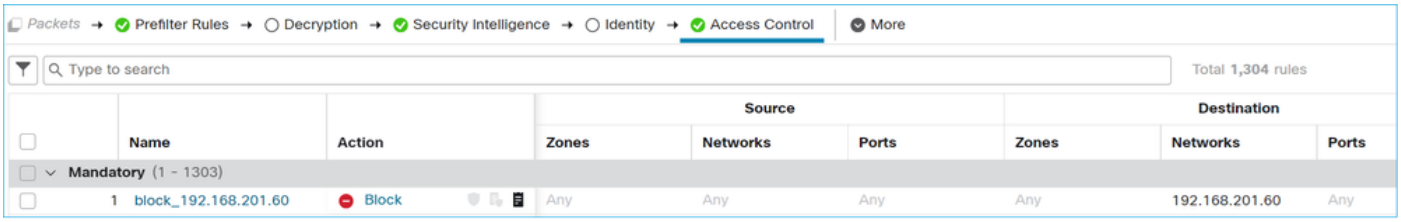
```
 325 from NET201:10.0.200.89/80 (10.0.200.89/80) to NET200:10.0.200.85/44806 (10.0.200.85/44806)
```

要点

- 由于两台设备都在TCP状态旁路模式下处理TCP连接，因此非对称流量通过一组不同的防火墙设备内联运行。
- 请注意，防火墙上未手动配置TCP状态旁路，但它是内联集接口操作的结果。

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>

```
firepower#
```

```
show capture
```

```
capture CAPI type raw-data trace interface INSIDE
```

```
[Capturing - 270 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
```

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

```
<#root>

firepower#

show capture CAPI packet-number 1 trace



4 packets captured

   1: 09:41:54.562547       192.168.201.50.59144 > 192.168.201.60.80: S 3817586151:3817586151(0) win 64
Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Elapsed time: 10126 ns
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Elapsed time: 10126 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip any host 192.168.201.60 rule-id 268451045 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268451045: ACCESS POLICY: mzafeiro_2m - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268451045: L4 RULE: block_192.168.201.60
Additional Information:

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
Action: drop

Time Taken: 20252 ns

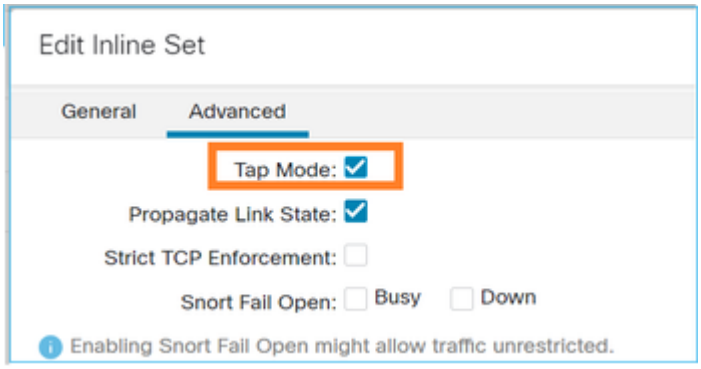
1 packet shown
```

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>

```
firepower#

 show inline-set



Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Fail-open for snort down is off
  Fail-open for snort busy is off


Tap mode is on


  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/4 "OUTSIDE"
      Current-Status: UP
    Interface: Ethernet1/3 "INSIDE"
      Current-Status: UP
```

```
   Bridge Group ID: 0
```

使用分路接口验证FTD内联对

基本原理

- 使用分路器配置内联对时，物理接口在内部桥接。
- 它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。

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



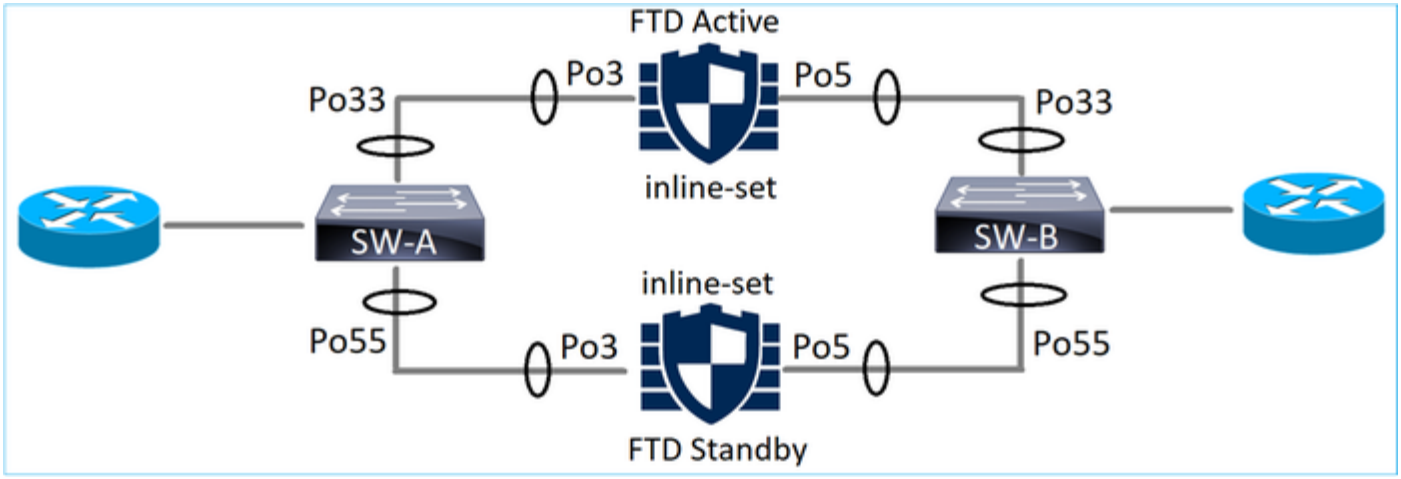
1 packet shown
>
```

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 Po55(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

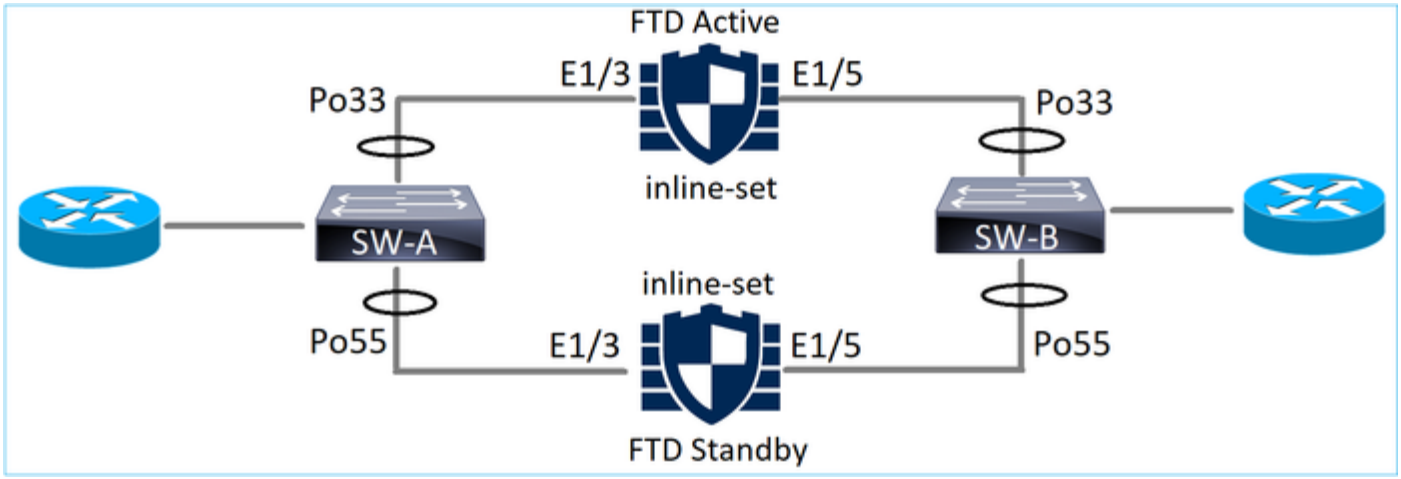

Interface-Pair[1]:
    Interface: Port-channel3 "INSIDE"
      Current-Status: UP
    Interface: Port-channel5 "OUTSIDE"
      Current-Status: UP

    Bridge Group ID: 775
```



注意：如果发生FTD故障切换事件，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
```

⚠ 警告：在此场景中，在FTD故障切换事件中，收敛时间主要取决于Etherchannel LACP协商，以及中断所需的时间，后者可能更长。如果Etherchannel模式为ON（无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	> 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“外部” 当前状态： UP 网桥组ID:509 >	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“外部” 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 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	> 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:内联对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 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:内联对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，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 >	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 type：捕获 子类型： 结果：允许 Config： 其它信息： MAC访问列表 阶段：2 type：访问列表 子类型： 结果：允许 Config： 隐式规则 其它信息： MAC访问列表 阶段：3 type：NGIPS模式 子类型：ngips模式 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 type：访问列表 子类型：日志 结果：丢弃	> 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 type：捕获 子类型： 结果：允许 Config： 其它信息： MAC访问列表 阶段：2 type：访问列表 子类型： 结果：允许 Config： 隐式规则 其它信息： MAC访问列表 阶段：3 type：NGIPS模式 子类型：ngips模式 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 type：访问列表 子类型：日志 结果：会掉下来的 Config：

	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： 输入接口：内部 输入状态： 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 >	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： 输入接口：内部 输入状态： up input-line-status: up 操作：访问列表已丢弃，但由于内联分路器而转发数据包 1个数据包显示 >

摘要

- 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，会应用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）。