

在路由模式下配置Firepower威胁防御接口

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[相关产品](#)

[背景信息](#)

[配置](#)

[网络图](#)

[配置路由接口和子接口](#)

[步骤1:配置逻辑接口](#)

[第二步：配置物理接口](#)

[FTD路由接口操作](#)

[FTD路由接口概述](#)

[验证](#)

[跟踪FTD路由接口上的数据包](#)

[相关信息](#)

简介

本文档介绍Firepower威胁防御(FTD)设备上的内联接口的配置、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：

- ASA5512-X - FTD代码6.1.0.x
- Firepower管理中心(FMC) — 代码6.1.0.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。

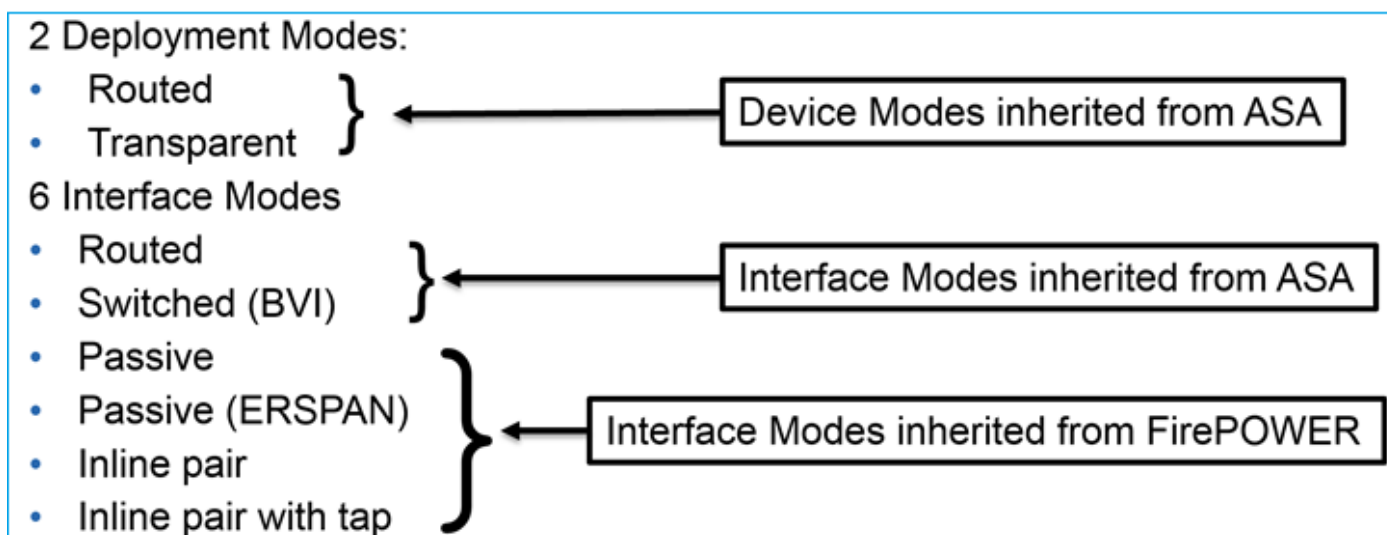
相关产品

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

Firepower威胁防御(FTD)提供两种部署模式和六种接口模式，如下图所示：



 注意：您可以在单个FTD设备上混合接口模式。

各种FTD部署和接口模式的高级概述：

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

配置

网络图



配置路由接口和子接口

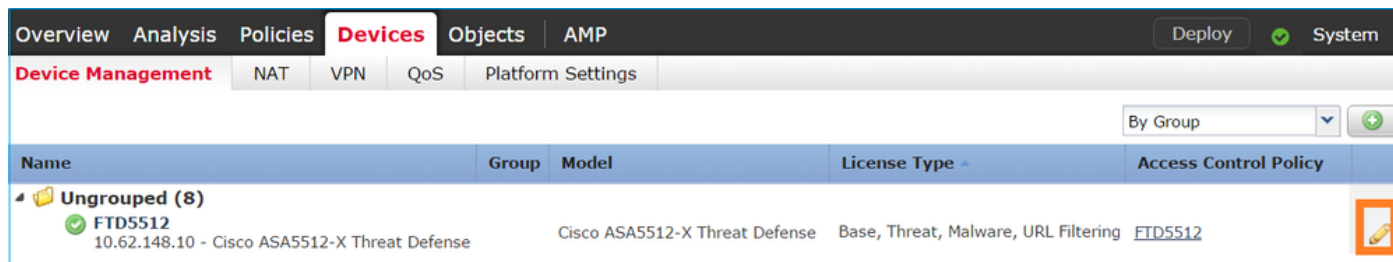
按照以下要求配置子接口G0/0.201和接口G0/1:

接口	G 0/0.201	G 0/1
名称	内部	外部
安全区域	INSIDE_ZONE	OUTSIDE_ZONE
描述	内部	外部
子接口Id	201	-
VLAN ID	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
双工/速度	自动	自动

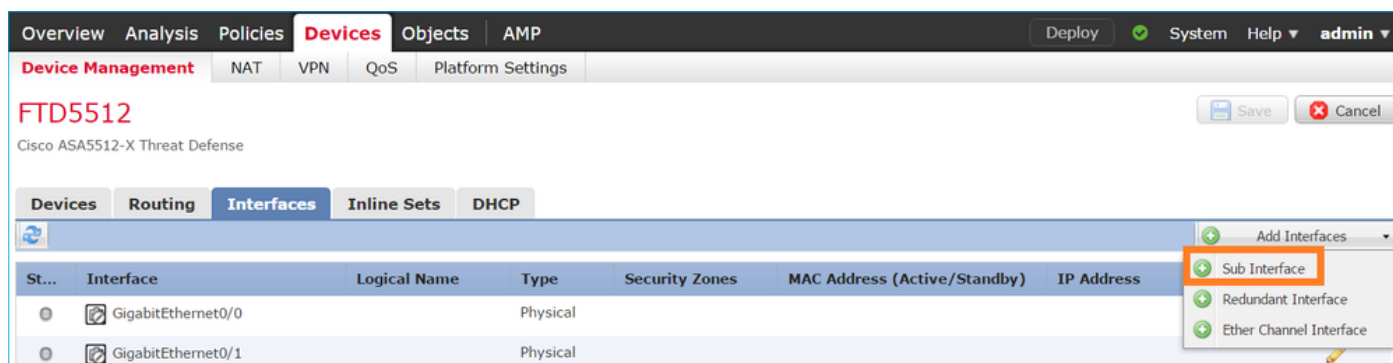
解决方案

步骤1:配置逻辑接口

导航到Devices > Device Management，选择适当的设备，然后选择Edit图标：



选择Add Interfaces > Sub Interface:



根据要求配置子接口设置：

Add Sub Interface

Name: Enabled Management Only

Security Zone: ▼

Description:

General IPv4 IPv6 Advanced

MTU: (64 - 9198)

Interface *: ▼ Enabled

Sub-Interface ID *: (1 - 4294967295)

VLAN ID: (1 - 4094)

接口IP设置：

Add Sub Interface

Name: Enabled Management Only

Security Zone: ▼

Description:

General **IPv4** IPv6 Advanced

IP Type: ▼

IP Address: eg. 1.1.1.1/255.255.255.228

在物理接口(GigabitEthernet0/0)下指定Duplex (双工) 和Speed (速度) 设置：

General	IPv4	IPv6	Advanced	Hardware Configuration
Duplex:	<input type="text" value="auto"/> ▼			
Speed:	<input type="text" value="auto"/> ▼			

启用物理接口（本例中为G0/0）：

Edit Physical Interface

Mode:	<input type="text" value="None"/> ▼	
Name:	<input type="text"/>	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Management Only
Security Zone:	<input type="text"/> ▼	
Description:	<input type="text"/>	

General	IPv4	IPv6	Advanced	Hardware Configuration
MTU:	<input type="text" value="1500"/>	(64 - 9198)		
Interface ID:	<input type="text" value="GigabitEthernet0/0"/>			

第二步：配置物理接口

根据需要编辑GigabitEthernet0/1物理接口：

Edit Physical Interface

Mode: ▼

Name: Enabled Management Only

Security Zone: ▼

Description:

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: ▼

IP Address: eg. 1.1.1.1/255.255.255.228

- 对于路由接口，模式为：None
- Name等同于ASA接口名称
- 在FTD上，所有接口的安全级别均为0
- same-security-traffic不适用于FTD。默认情况下，允许FTD接口（内部）之间的流量

选择Save和Deploy。

确认

在FMC GUI中：

St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
	GigabitEthernet0/0		Physical			
	GigabitEthernet0/1	OUTSIDE	Physical	OUTSIDE_ZONE		192.168.202.1/24(Static)
	GigabitEthernet0/2		Physical			
	GigabitEthernet0/3		Physical			
	GigabitEthernet0/4		Physical			
	GigabitEthernet0/5		Physical			
	Diagnostic0/0		Physical			
	GigabitEthernet0/0.201	INSIDE	SubInterf...	INSIDE_ZONE		192.168.201.1/24(Static)

从FTD CLI:

<#root>

>

show interface ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	up	up
GigabitEthernet0/0.201	192.168.201.1	YES	manual	up	up
GigabitEthernet0/1	192.168.202.1	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
GigabitEthernet0/3	unassigned	YES	unset	administratively down	down
GigabitEthernet0/4	unassigned	YES	unset	administratively down	down
GigabitEthernet0/5	unassigned	YES	unset	administratively down	down
Internal-Contro0/0	127.0.1.1	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
Management0/0	unassigned	YES	unset	up	up

<#root>

>

show ip

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0.201	INSIDE	192.168.201.1	255.255.255.0	manual
GigabitEthernet0/1	OUTSIDE	192.168.202.1	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0.201	INSIDE	192.168.201.1	255.255.255.0	manual
GigabitEthernet0/1	OUTSIDE	192.168.202.1	255.255.255.0	manual

FMC GUI和FTD CLI关联 :

The image shows a screenshot of the FMC GUI configuration page for a sub-interface named 'INSIDE'. The 'Name' field is set to 'INSIDE', 'Security Zone' is 'INSIDE_ZONE', and 'Description' is 'INTERNAL'. Under the 'IPv4' tab, 'IP Type' is 'Use Static IP' and 'IP Address' is '192.168.201.1/24'. To the right, a terminal window shows the corresponding FTD CLI configuration: 'show running-config interface g0/0.201' followed by 'interface GigabitEthernet0/0.201', 'description INTERNAL', 'vlan 201', 'nameif INSIDE', 'cts manual', 'propagate sgt preserve-untag', 'policy static sgt disabled trusted', 'security-level 0', and 'ip address 192.168.201.1 255.255.255.0'. Arrows indicate the mapping from the GUI fields to the CLI commands.

<#root>

>

show interface g0/0.201

Interface GigabitEthernet0/0.201

"

INSIDE

",

is up, line protocol is up

Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec

VLAN identifier 201

Description: INTERNAL

MAC address a89d.21ce.fdea, MTU 1500

IP address 192.168.201.1, subnet mask 255.255.255.0

Traffic Statistics for "INSIDE":

1 packets input, 28 bytes

1 packets output, 28 bytes

0 packets dropped

>

show interface g0/1

Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up

Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec

Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)

Input flow control is unsupported, output flow control is off

Description: EXTERNAL

MAC address a89d.21ce.fde7, MTU 1500

IP address 192.168.202.1, subnet mask 255.255.255.0

0 packets input, 0 bytes, 0 no buffer

Received 0 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

0 pause input, 0 resume input

0 L2 decode drops

1 packets output, 64 bytes, 0 underruns

0 pause output, 0 resume output

0 output errors, 0 collisions, 12 interface resets

0 late collisions, 0 deferred

0 input reset drops, 0 output reset drops

input queue (blocks free curr/low): hardware (511/511)

output queue (blocks free curr/low): hardware (511/511)

Traffic Statistics for "OUTSIDE":

0 packets input, 0 bytes

0 packets output, 0 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, 0 bytes/sec
 5 minute output rate 0 pkts/sec, 0 bytes/sec
 5 minute drop rate, 0 pkts/sec

>

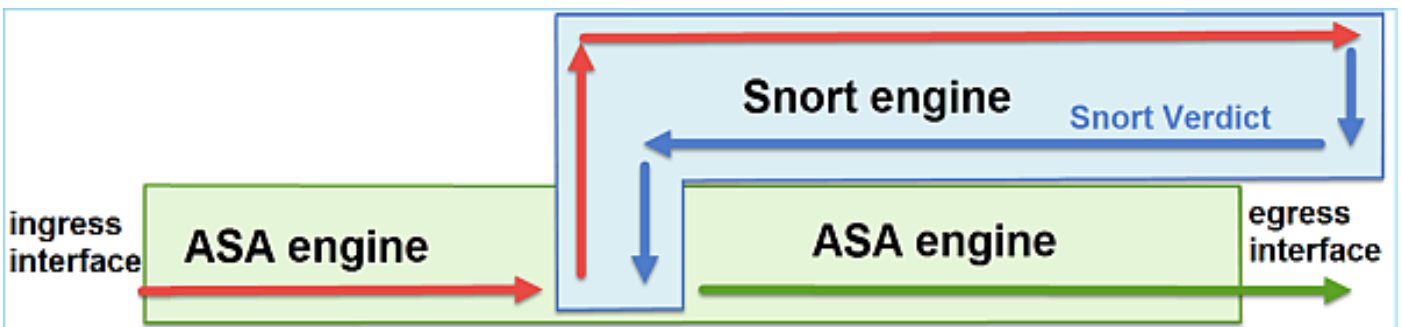
FTD路由接口操作

使用路由接口时，检验FTD数据包流。

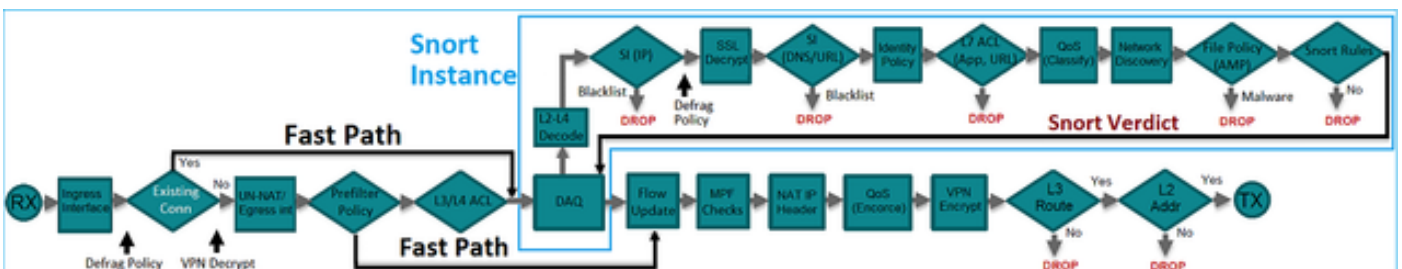
解决方案

FTD架构概述

FTD数据平面的简要概述：



此图显示了每个引擎内发生的一些检查：



要点

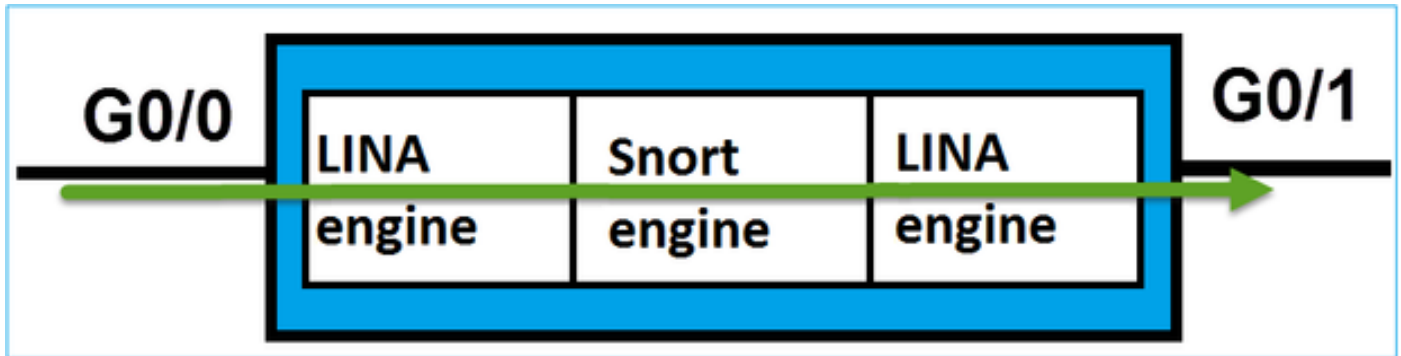
- 底部检查与FTD LINA引擎数据路径相对应

- 蓝色方框内的检查与FTD Snort引擎实例相对应

FTD路由接口概述

- 仅在路由部署中可用
- 传统L3防火墙部署
- 一个或多个物理或逻辑(VLAN)可路由接口
- 允许配置NAT或动态路由协议等功能
- 根据路由查找转发数据包，并根据ARP查找解决下一跳
- 实际流量 可以丢弃
- 完整的LINA引擎检查与完整的Snort引擎检查一起应用

最后一点可以直观地显示为：



验证

跟踪FTD路由接口上的数据包

网络图



使用以下参数使用Packet Tracer查看应用的策略：

输入界面	内部
协议/服务	TCP端口80

源 IP	192.168.201.100
目的 IP	192.168.202.100

解决方案

当使用路由接口时，数据包的处理方式类似于传统ASA路由接口。在LINA引擎数据路径中执行路由查找、模块化策略框架(MPF)、NAT、ARP查找等检查。此外，如果访问控制策略有此要求，数据包将由Snort引擎 (Snort实例之一) 进行检查，并在其中生成判定并返回到LINA引擎：

```
<#root>
```

```
>  
packet-tracer input INSIDE tcp 192.168.201.100 11111 192.168.202.100 80
```

```
Phase: 1
```

```
Type: ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
found next-hop 192.168.202.100 using egress ifc OUTSIDE
```

```
Phase: 2
```

```
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 268437505
```

```
access-list CSM_FW_ACL_ remark rule-id 268437505: ACCESS POLICY: FTD5512 - Default/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268437505: L4 RULE: DEFAULT ACTION RULE
```

```
Additional Information:
```

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 3

Type: CONN-SETTINGS

Subtype:
Result: ALLOW
Config:

class-map class-default

match any

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Phase: 4

Type: NAT

Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 11336, packet dispatched to next module

Result:


input-interface: INSIDE

input-status: up
input-line-status: up

output-interface: OUTSIDE

output-status: up
output-line-status: up
Action: allow

>

 注：在第4阶段，将根据UM_STATIC_TCP_MAP的TCP映射检查数据包。这是FTD上的默认TCP映射。

<#root>

firepower#

show run all tcp-map

```
!  
tcp-map UM_STATIC_TCP_MAP  
  no check-retransmission  
  no checksum-verification  
  exceed-mss allow  
  queue-limit 0 timeout 4  
  reserved-bits allow  
  syn-data allow  
  synack-data drop  
  invalid-ack drop  
  seq-past-window drop  
  tcp-options range 6 7 allow  
  tcp-options range 9 18 allow  
  tcp-options range 20 255 allow  
  tcp-options selective-ack allow  
  tcp-options timestamp allow
```

```
tcp-options window-scale allow
tcp-options mss allow
tcp-options md5 clear
ttl-evasion-protection
urgent-flag allow
window-variation allow-connection
!
>
```

相关信息

- [适用于Firepower设备管理器的思科Firepower威胁防御配置指南，版本6.1](#)
- [在ASA 55xx-X设备上安装和升级Firepower威胁防御](#)
- [思科安全防火墙威胁防御](#)
- [思科技术支持和下载](#)

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）。