

# 配置Firepower威胁防御在已路由模式建立接口

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[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](#)

[步骤2.配置物理接口](#)

[FTD路由接口操作](#)

[FTD路由接口概述](#)

[验证](#)

[跟踪在FTD路由接口的一数据包](#)

[相关信息](#)

## 简介

本文描述配置，验证，并且一个轴向对的背景操作在Firepower威胁防御(FTD)设备建立接口。

## 先决条件

### 要求

没有本文的特定需求。

### 使用的组件

- 运行FTD代码6.1.0.x的ASA5512-X
- 运行6.1.0.x的Firepower管理中心(FMC)

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。如果您的网络实际，请保证您了解所有命令潜在影响。

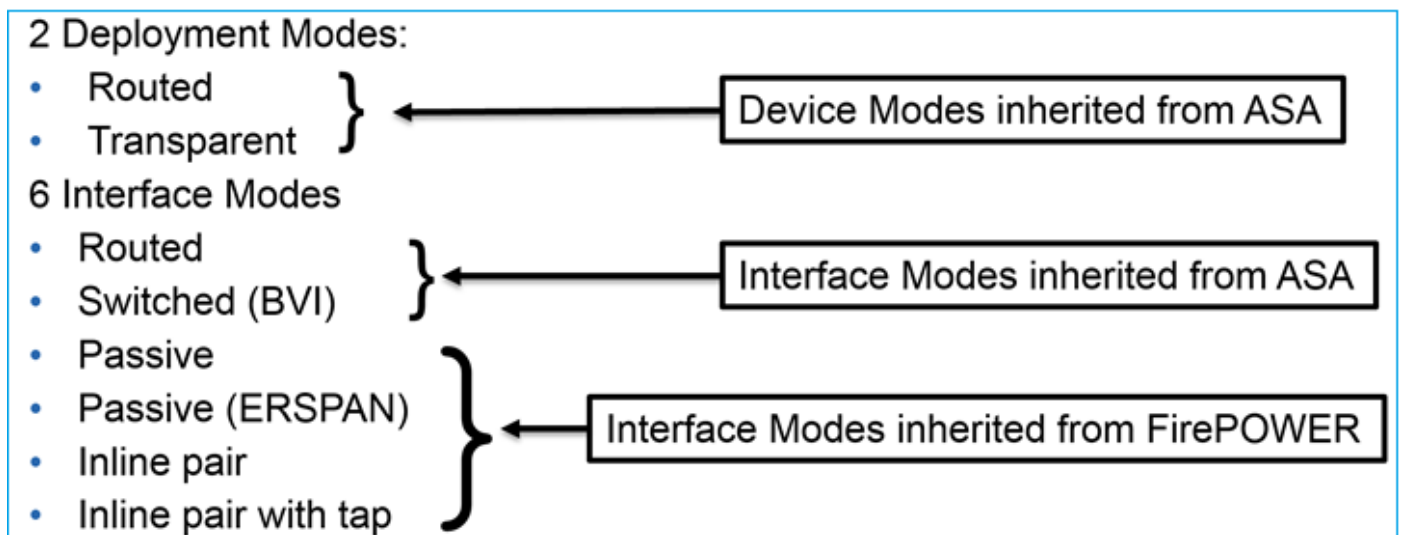
## 相关产品

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) , 亚马逊网站服务(AW) , 键盘/视频/鼠标(KVM)
- FTD软件代码6.2.x和以后。

## 背景信息

FTD提供两个部署模式和六个接口模式如以下镜像所显示：



**Note:**您能混合在单个FTD设备的接口模式。

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	全双工莉娜引擎和喷鼻息引擎检查	是
交换式	透明	全双工莉娜引擎和喷鼻息引擎检查	是
轴向对	已路由或透明	部分莉娜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	部分莉娜引擎和全双工喷鼻息引擎检查	无
被动	已路由或透明	部分莉娜引擎和全双工喷鼻息引擎检查	无
被动(ERSPAN)	已路由	部分莉娜引擎和全双工喷鼻息引擎检查	无

# 配置

## 网络图



## 配置路由接口和子接口

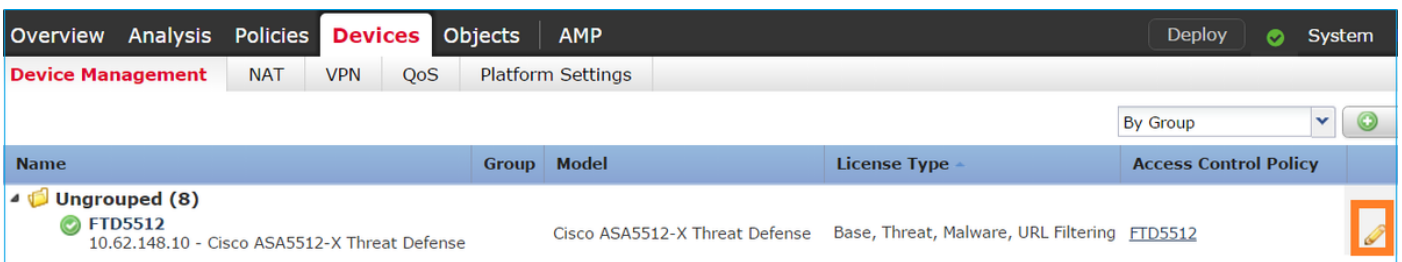
根据以下需求配置子接口G0/0.201和接口G0/1：

接口	G0/0.201	G0/1
名称	里面	从外部
安全区域	INSIDE_ZONE	OUTSIDE_ZONE
说明	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

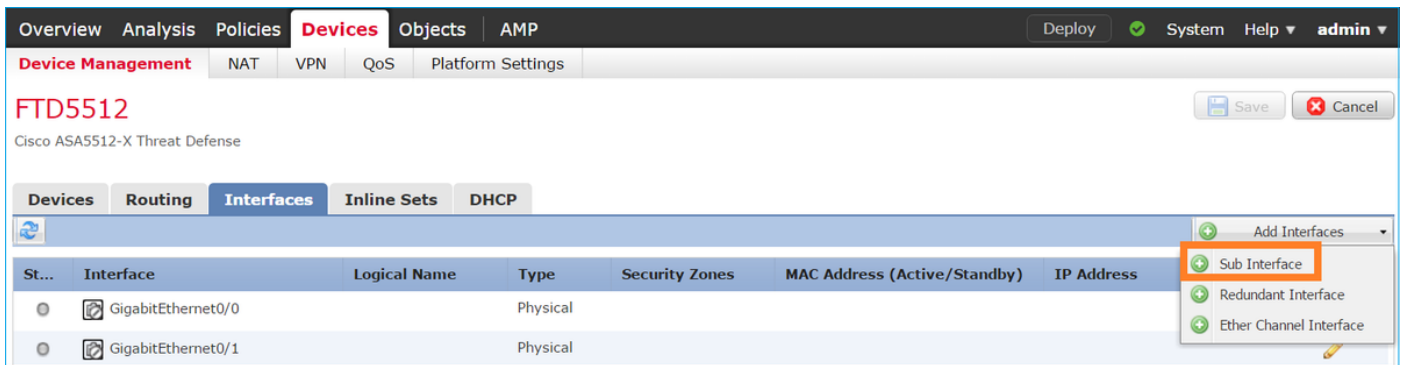
## 解决方案

### 步骤1.配置逻辑接口

导航对设备>设备管理，选择适当的设备并且选择Edit图标：



选择添加接口> Sub接口：



根据需求配置子接口设置：

### 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)

建立接口IP设置：

## Add Sub Interface

Name:	<input type="text" value="INSIDE"/>	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Management Only
Security Zone:	<input type="text" value="INSIDE_ZONE"/>		
Description:	<input type="text" value="INTERNAL"/>		
<b>General</b>   <b>IPv4</b>   IPv6   Advanced			
IP Type:	<input type="text" value="Use Static IP"/>		
IP Address:	<input type="text" value="192.168.201.1/24"/>	eg. 1.1.1.1/255.255.255.228	

在物理接口(GigabitEthernet0/0)下请指定双工和速度设置：

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

启用物理接口(G0/0在这种情况下)：

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

## 步骤2.配置物理接口

根据需求编辑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

- 对于路由接口模式是：无
- 名称与ASA接口nameif是等同的
- 在FTD所有接口有安全等级= 0
- **same-security-traffic**不是可适用的在FTD。FTD接口(相互)和发夹之间的流量(内部)默认情况下允许

选择保存并且部署。

## 验证

从FMC GUI：

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 :

> **show interface ip brief**

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	up	up
<b>GigabitEthernet0/0.201</b>	<b>192.168.201.1</b>	<b>YES</b>	<b>manual</b>	<b>up</b>	<b>up</b>
<b>GigabitEthernet0/1</b>	<b>192.168.202.1</b>	<b>YES</b>	<b>manual</b>	<b>up</b>	<b>up</b>
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

> **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
<b>GigabitEthernet0/0.201</b>	<b>INSIDE</b>	<b>192.168.201.1</b>	<b>255.255.255.0</b>	<b>manual</b>
<b>GigabitEthernet0/1</b>	<b>OUTSIDE</b>	<b>192.168.202.1</b>	<b>255.255.255.0</b>	<b>manual</b>

## FMC GUI和FTD CLI相关性 :

**Edit Sub Interface**

Name:   Enabled  Management Only

Security Zone:  ▼

Description:

General **IPv4** IPv6 Advanced

IP Type:  ▼

IP Address:

```
> show running-config interface g0/0.201
!
interface GigabitEthernet0/0.201
description INTERNAL
vlan 201
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.201.1 255.255.255.0
```

> **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

>

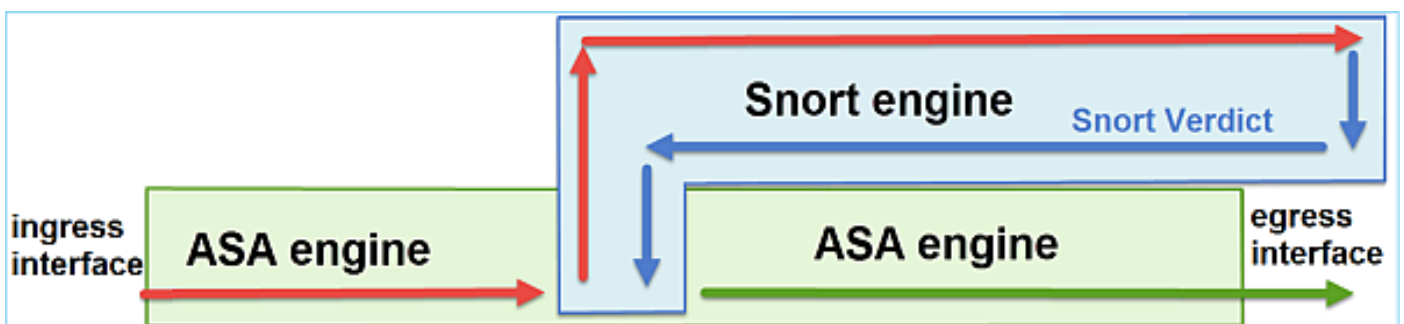
## FTD路由接口操作

当路由接口是在使用中的时，请验证处理FTD的数据包。

### [解决方案](#)

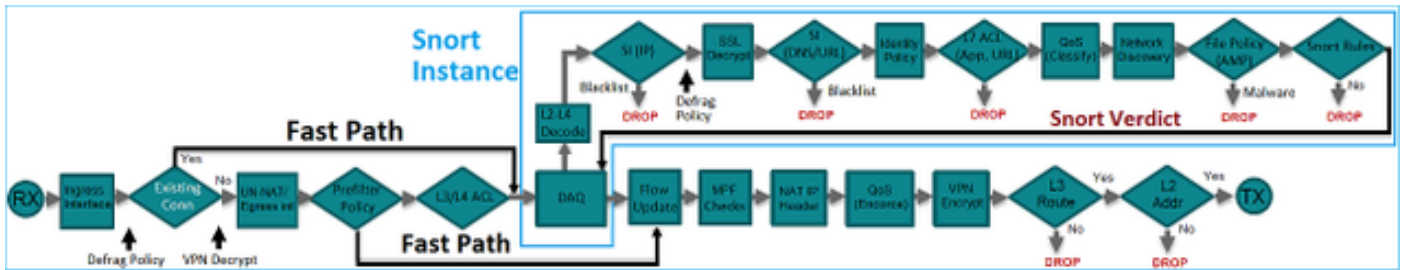
## FTD架构概述

FTD数据层面的高水平概述：





以下图片显示在每个引擎内发生的某些检查：



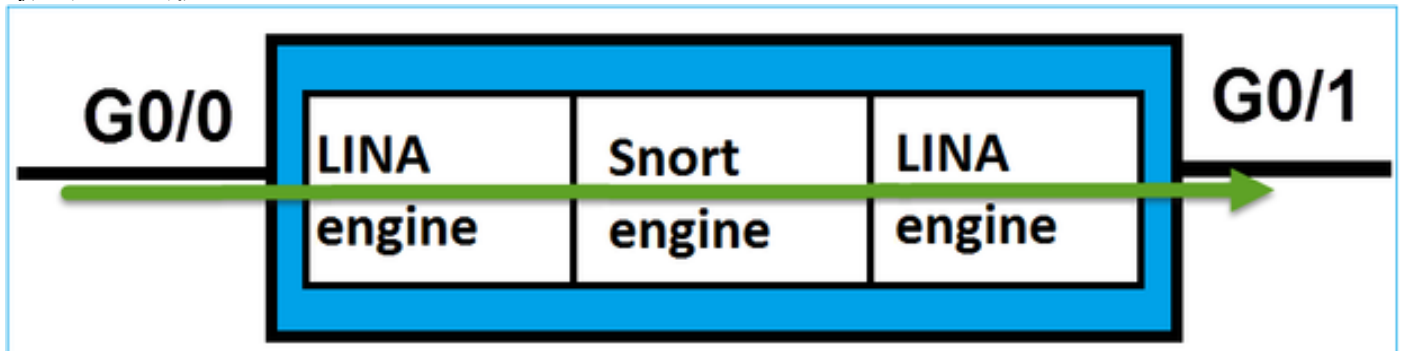
### 关键点

- 底下检查对应于FTD莉娜引擎数据路径
- 检查在蓝色框里面对应于FTD喷鼻息引擎实例

### FTD路由接口概述

- 仅联机在已路由部署
- 传统L3防火墙部署
- 一个或更多物理或逻辑(VLAN)路由可达接口
- 允许功能类似将配置的NAT或动态路由协议
- 数据包根据路由查找转发，并且根据ARP查找是解决的下一跳
- 实际流量可以丢弃
- 全双工莉娜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

跟踪在FTD路由接口的数据包

网络图



以下参数使用数据包追踪器发现已应用策略：

输入接口	里面
协议/服务	TCP端口80
源 IP	192.168.201.1 00
目的 IP	192.168.202.1 00

## 解决方案

当使用时路由接口数据包在对一个经典ASA路由接口的一此类似处理。检查类似路由查找，模块化政策架构(MPF)， NAT， ARP查找等在莉娜引擎数据路径发生。另外，如果访问控制策略如此要求，数据包乘喷鼻息引擎(其中一个喷鼻息实例)检查判决(黑名单， Whitelist)的地方生成并且返回回到莉娜引擎：

```
> 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 -

Defau

1t/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**

1 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

>

**Note:**在相位4数据包根据呼叫UM\_STATIC\_TCP\_MAP的TCP地图核对。这是在FTD的默认TCP地图。

```
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

- [Cisco Firepower威胁Firepower设备管理器的防御配置指南，版本6.1](#)
- [安装和升级Firepower在ASA 55xx-X设备的威胁防御](#)
- [工作用Firepower威胁防御\(FTD\)捕获和数据包追踪器](#)
- [技术支持和文档 - Cisco Systems](#)