

配置Firepower威胁防御在路由的模式下建立接口

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[背景信息](#)

[Configure](#)

[Network Diagram](#)

[配置一个路由接口和一个子接口](#)

[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](#)

[Verify](#)

[跟踪在FTD路由接口的一个信息包](#)

[Related Information](#)

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)工具上建立接口。

Prerequisites

Requirements

没有本文的特定需求。

Components Used

- ASA5512-X - FTD代码6.1.0.x
- Firepower管理中心(FMC) -请编码6.1.0.x

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.如果您的网络实际，请保证您了解所有命令的潜在影响。

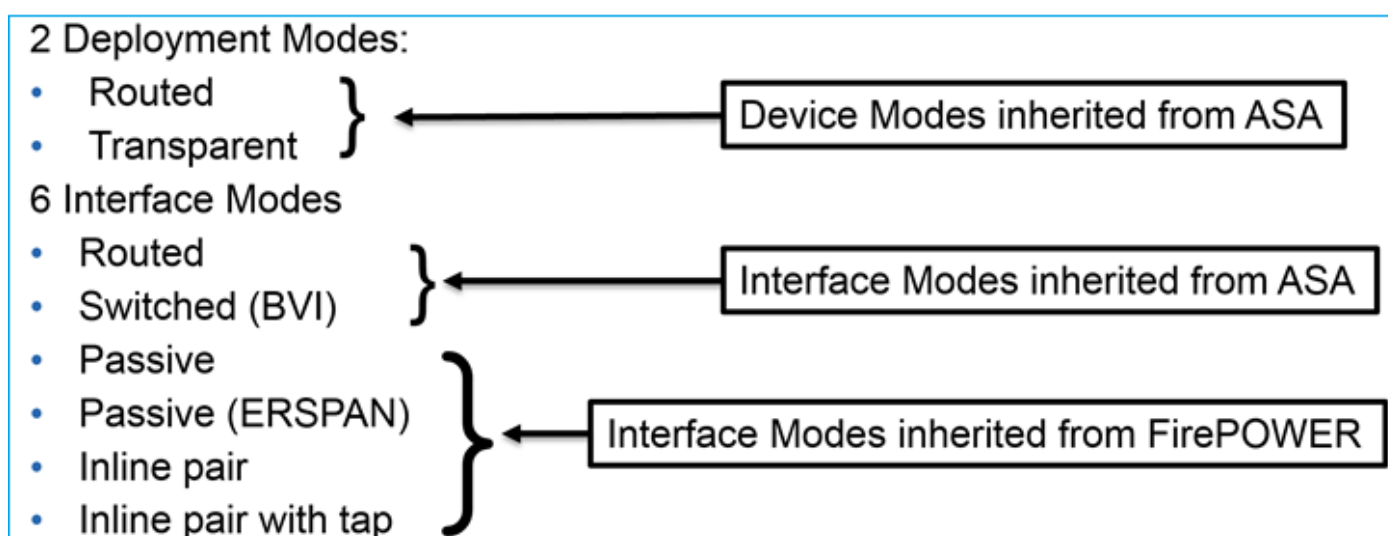
相关产品

本文可能也与这些一起使用硬件和软件版本：

- 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) , 基于内核的虚拟机(KVM)
- FTD软件代码6.2.x和以后

背景信息

如此镜像所显示，FTD提供两个配置模式和六个接口模式：



Note: 您能混合在单个FTD工具上的接口模式。

多种FTD配置和接口模式高级概述：

FTD接口模式	FTD配置模式	说明	数据流可以降低
路由	路由	充分的莉娜引擎和喷鼻息引擎检查	是
交换式	透明	充分的莉娜引擎和喷鼻息引擎检查	是
轴向对	路由或透明	部分莉娜引擎和充分的喷鼻息引擎检查	是
与轻拍的轴向对	路由或透明	部分莉娜引擎和充分的喷鼻息引擎检查	无
被动	路由或透明	部分莉娜引擎和充分的喷鼻息引擎检查	无
被动(ERSPAN)	路由	部分莉娜引擎和充分的喷鼻息引擎检查	无

Configure

Network Diagram



配置路由接口和子接口

配置子接口G0/0.201并且根据这些需求建立接口G0/1：

接口	G0/0.201	G0/1
名字	里面	从外部
安全区	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

连接对设备>设备管理，选择适当的设备并且选择Edit图标：

The screenshot shows the 'Devices' tab in the management console. The 'Device Management' section is active, displaying a table of devices. The table has columns for Name, Group, Model, License Type, and Access Control Policy. One device is listed: 'FTD5512' with IP '10.62.148.10', model 'Cisco ASA5512-X Threat Defense', license type 'Base, Threat, Malware, URL Filtering', and ID 'FTD5512'. An edit icon is visible next to the device entry.

选择添加接口> Sub接口：

The screenshot shows the Cisco ASA5512 configuration page for 'FTD5512'. The 'Interfaces' tab is active, displaying a table of existing interfaces:

St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
<input type="checkbox"/>	GigabitEthernet0/0		Physical			
<input type="checkbox"/>	GigabitEthernet0/1		Physical			

The 'Add Interfaces' dropdown menu is open, showing options: 'Sub Interface' (highlighted with an orange box), 'Redundant Interface', and 'Ether Channel Interface'.

根据需求配置子接口设置：

The 'Add Sub Interface' configuration form is shown with the following fields:

- Name: Enabled Management Only
- Security Zone:
- Description:

Below the form are tabs for 'General', 'IPv4', 'IPv6', and 'Advanced'. The 'General' tab is selected, showing the following settings:

- 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"/>		
General IPv4 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：

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

Enable (event)物理接口(G0/0在这种情况下)：

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"/>

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
- 名字与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接口之间的数据流(相互)和(内部)默认情况下允许

选择保存并且配置。

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
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

```
> 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相关性 :

The screenshot shows the 'Edit Sub Interface' configuration page in the FMC GUI. The 'Name' field is set to 'INSIDE', 'Security Zone' is 'INSIDE_ZONE', and 'Description' is 'INTERNAL'. The 'IP Type' is set to 'Use Static IP' and the 'IP Address' is '192.168.201.1/24'. A callout box on the right shows the CLI configuration for the same interface:

```
> 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

>

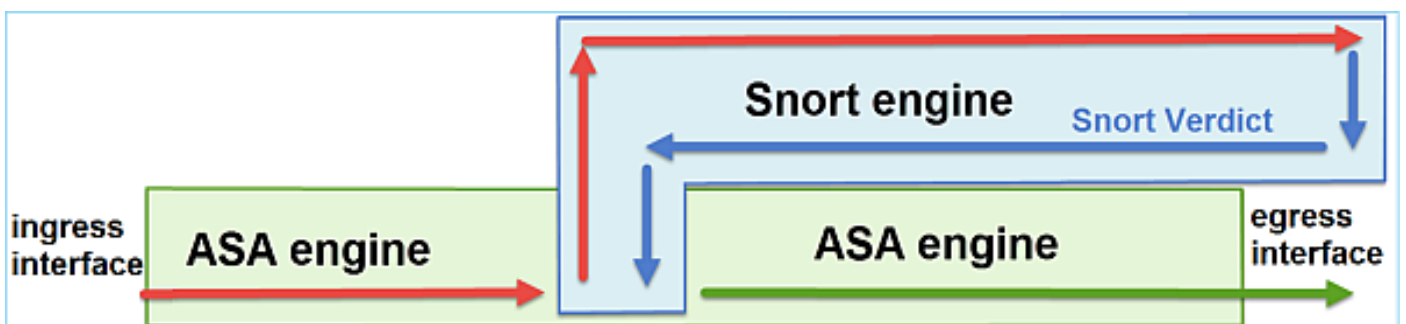
FTD路由接口操作

当路由接口是在使用中的时，请验证FTD信息包流。

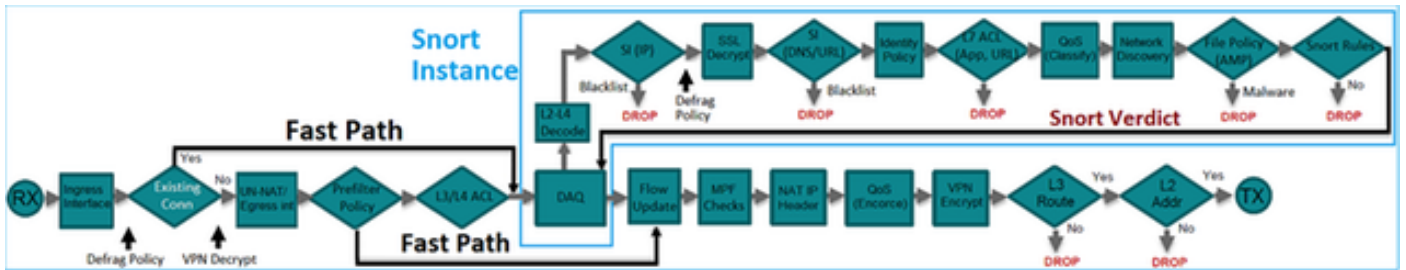
解决方案

FTD体系结构概述

FTD数据层面高级概述：



此图片显示在每个引擎内发生的某些检查：



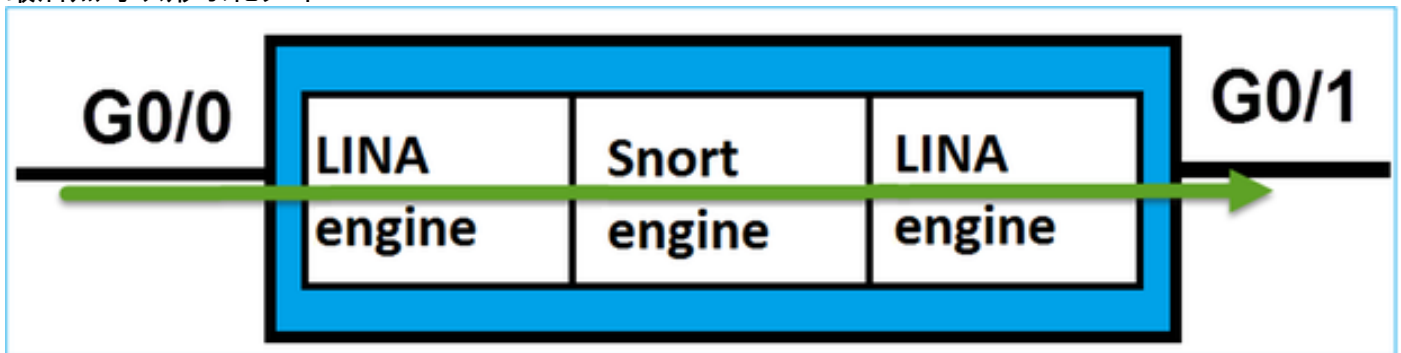
关键点

- 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

- 仅可用在路由的配置
- 传统L3防火墙配置
- 一个或更多物理或逻辑(VLAN)路由可达接口
- 允许功能类似将被配置的NAT或动态路由协议
- 信息包根据路由查找转发，并且根据ARP查找是解决的下一跳
- 实际数据流可以降低
- 充分的莉娜引擎检查与充分的喷鼻息引擎检查一起适用

最后点可以形象化如下：



Verify

跟踪在FTD路由接口的信息包

Network Diagram



以这些参数使用信息包跟踪程序发现应用的策略：

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

解决方案

当使用时路由接口信息包在对一个经典ASA路由接口的一此类似被处理。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得，信息包由喷鼻息引擎(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返回莉娜引擎：

```
> 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
```

```
lt/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

```
l 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:在第4阶段信息包根据称为UM_STATIC_TCP_MAP的TCP映射核对。这是在FTD的默认TCP映射。

```
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  
!  
>
```

Related Information

- [Cisco Firepower威胁防御Firepower设备管理器配置指南，版本6.1](#)
- [安装和升级Firepower威胁防御在ASA 55xx-X设备](#)
- [Firepower威胁防御\(FTD\)捕获和信息包跟踪程序的使用](#)
- [Technical Support & Documentation - Cisco Systems](#)