配置Firepower威胁防御在已路由模式建立接口

目录

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。

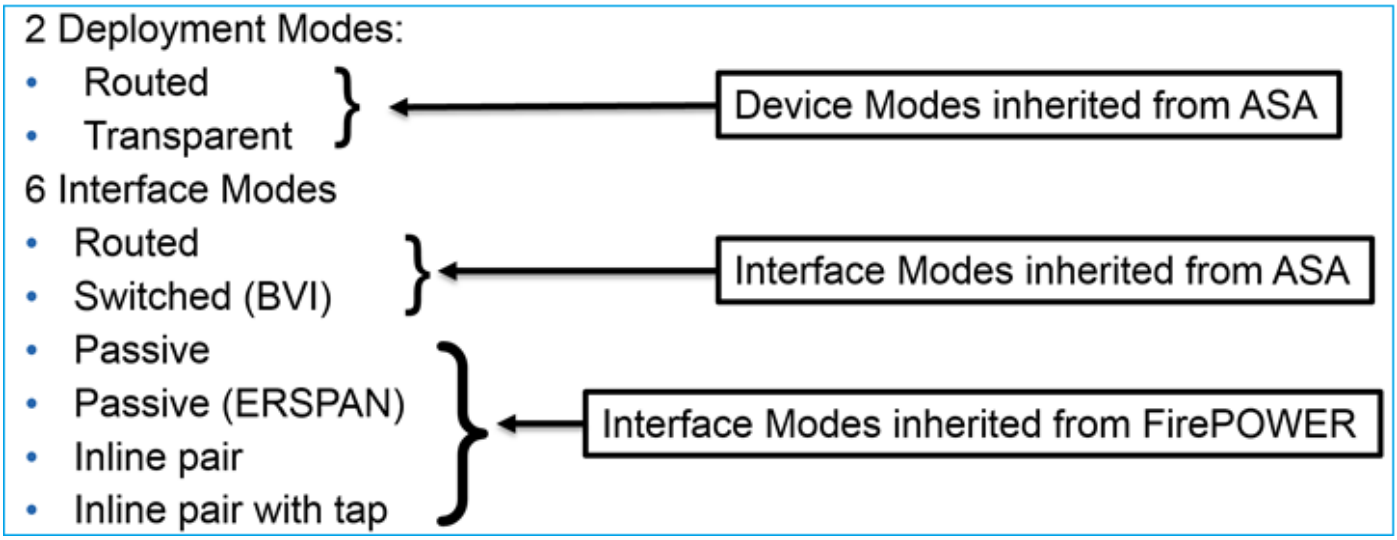
相关产品

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)，基于内核的虚拟机(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

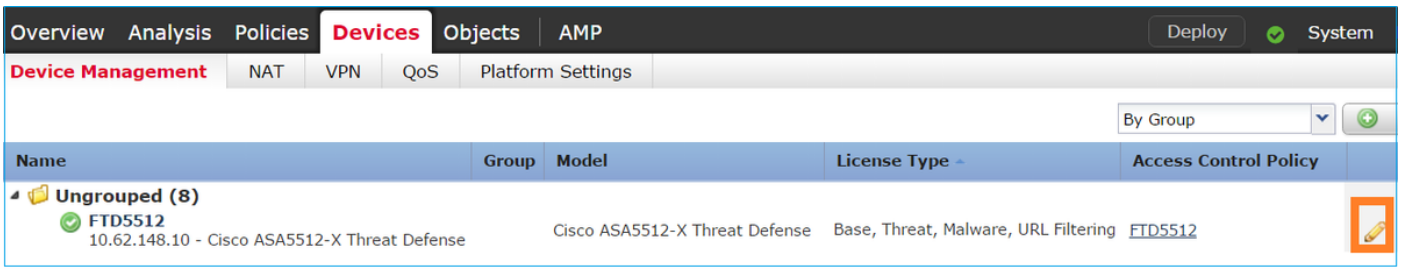
根据以下需求配置子接口G0/0.201和接口G0/1 ：

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

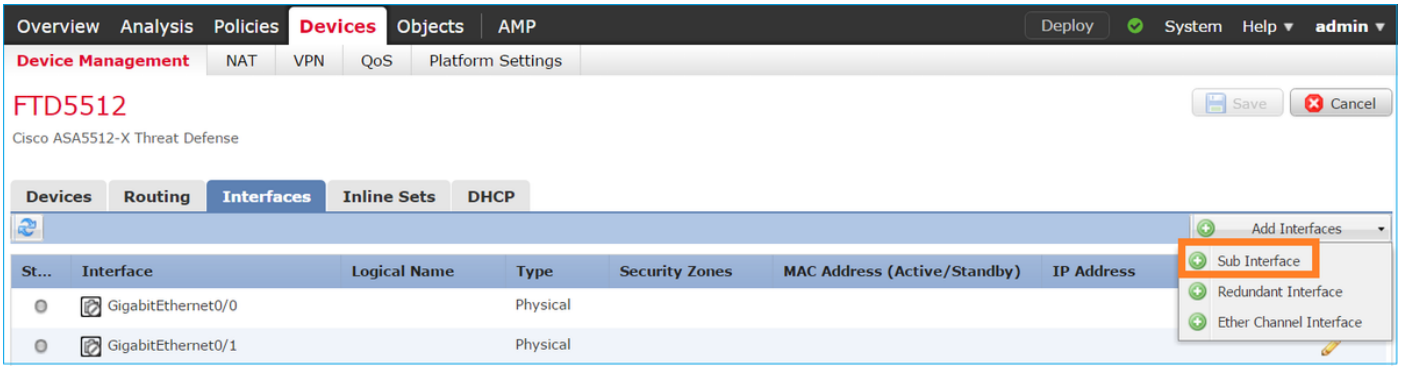
[解决方案]

步骤1.配置逻辑接口

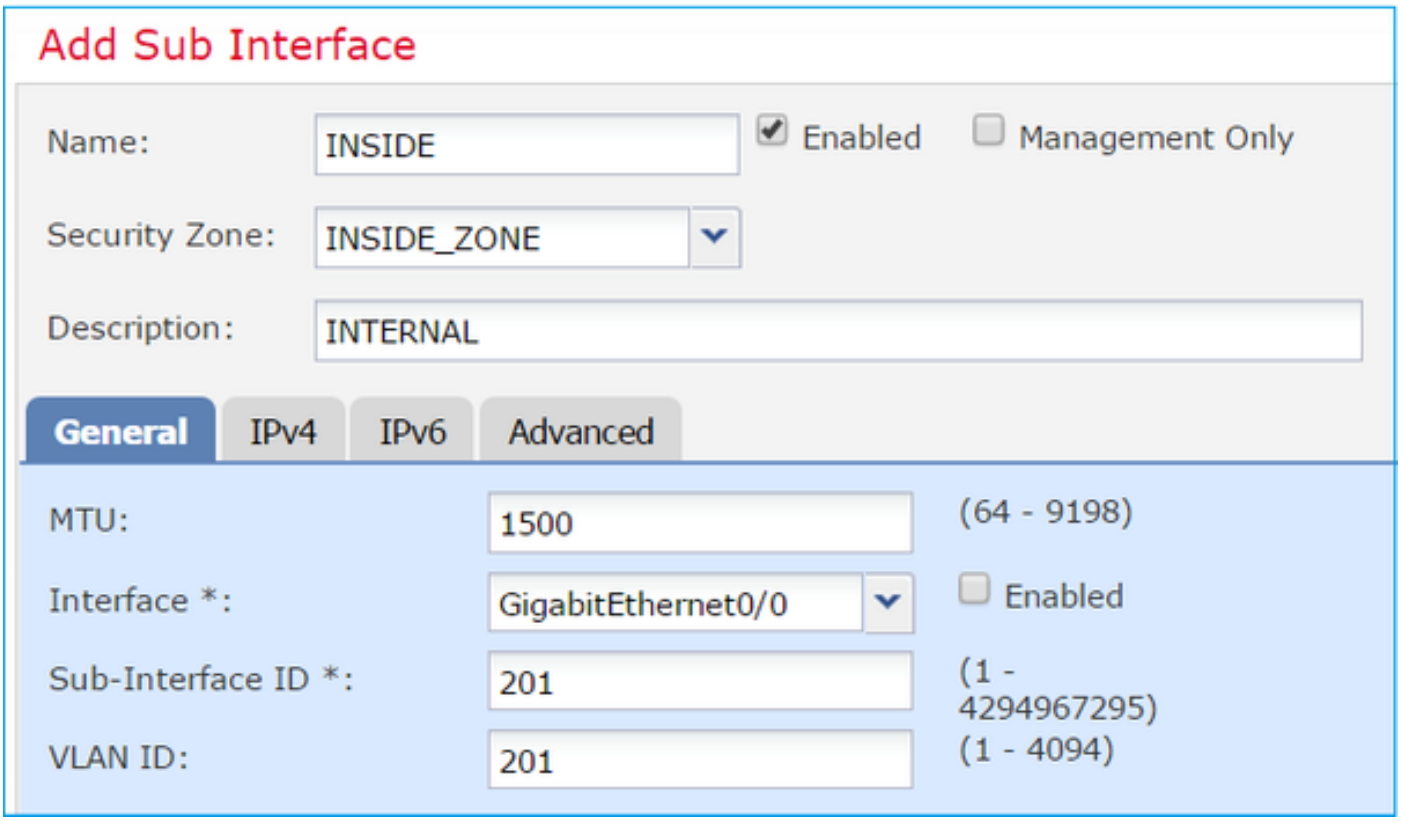
导航对**设备>设备管理**，选择适当的设备并且选择**Edit图标**：



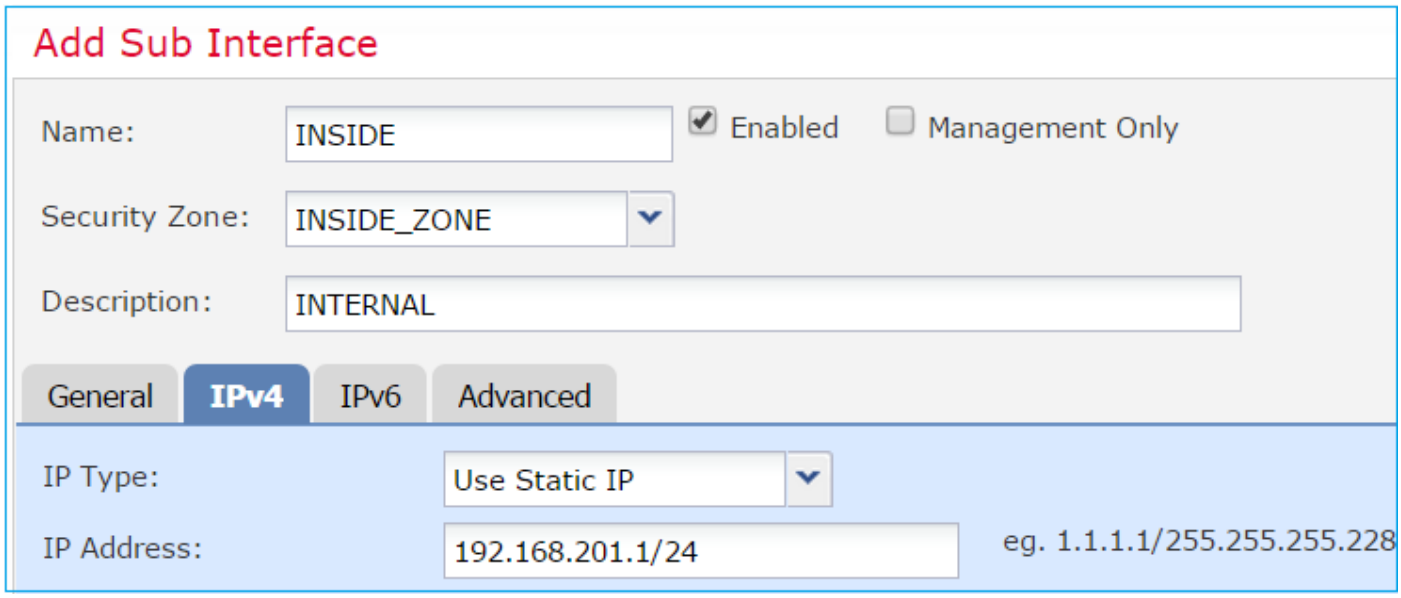
选择**添加接口> Sub接口**：



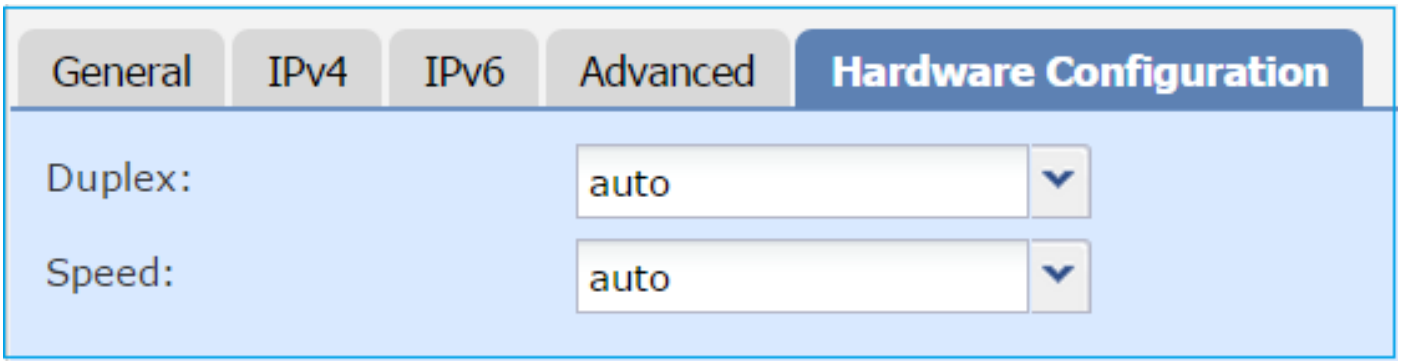
根据需求配置子接口设置：



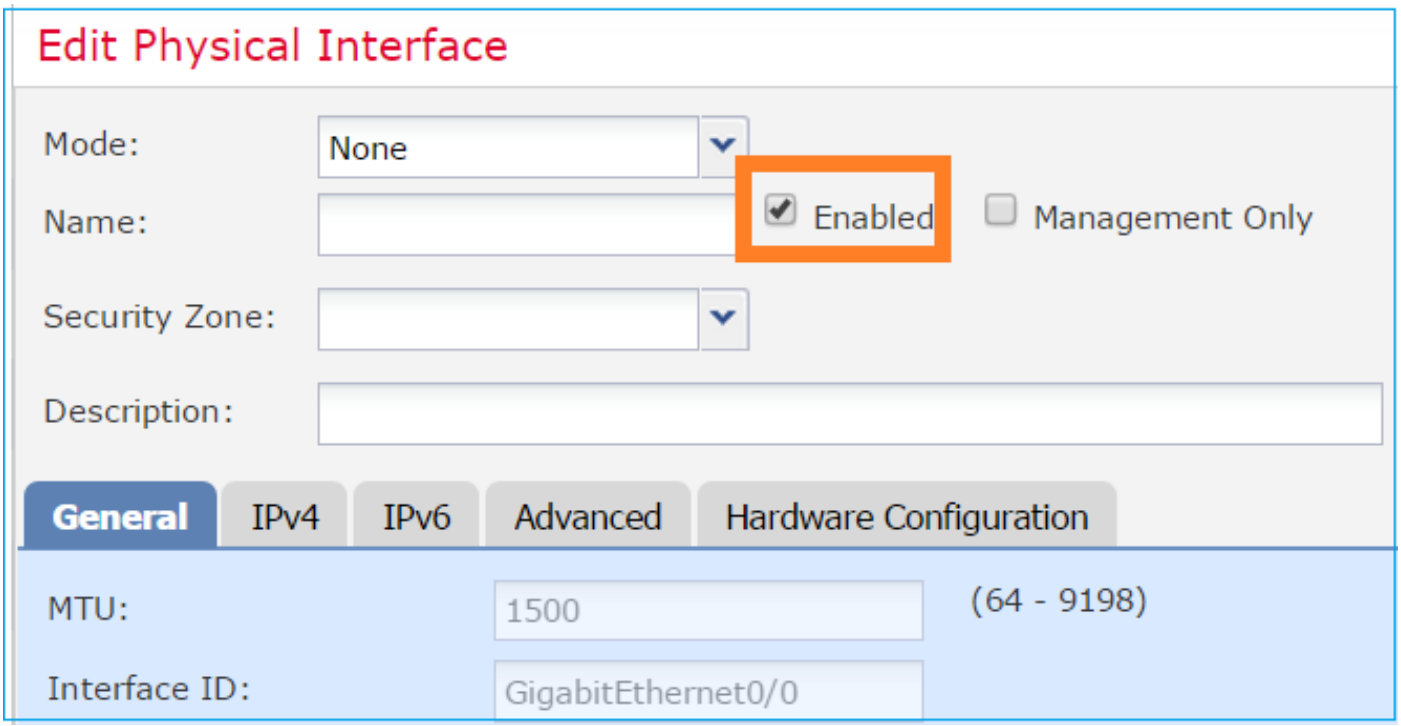
建立接口IP设置：



在物理接口(GigabitEthernet0/0)下请指定双工和速度设置：

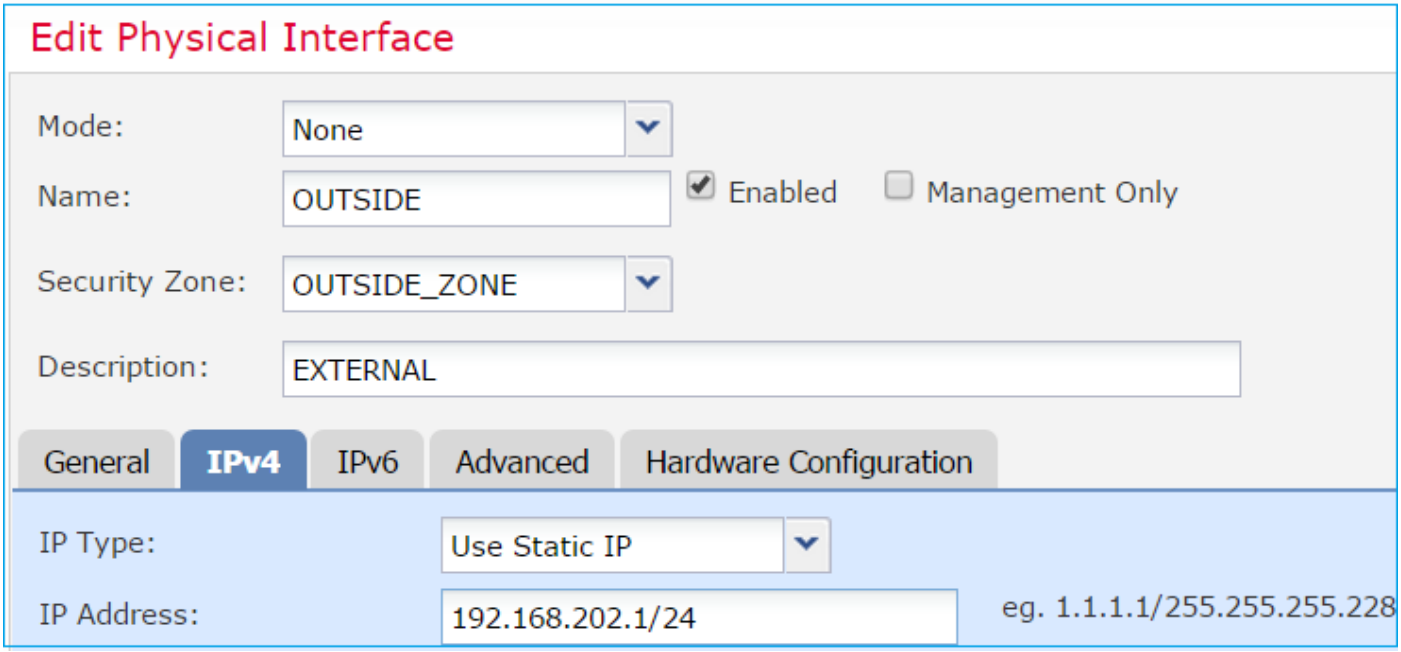


启用物理接口(G0/0在这种情况下)：



步骤2.配置物理接口

根据需求编辑GigabitEthernet0/1物理接口：

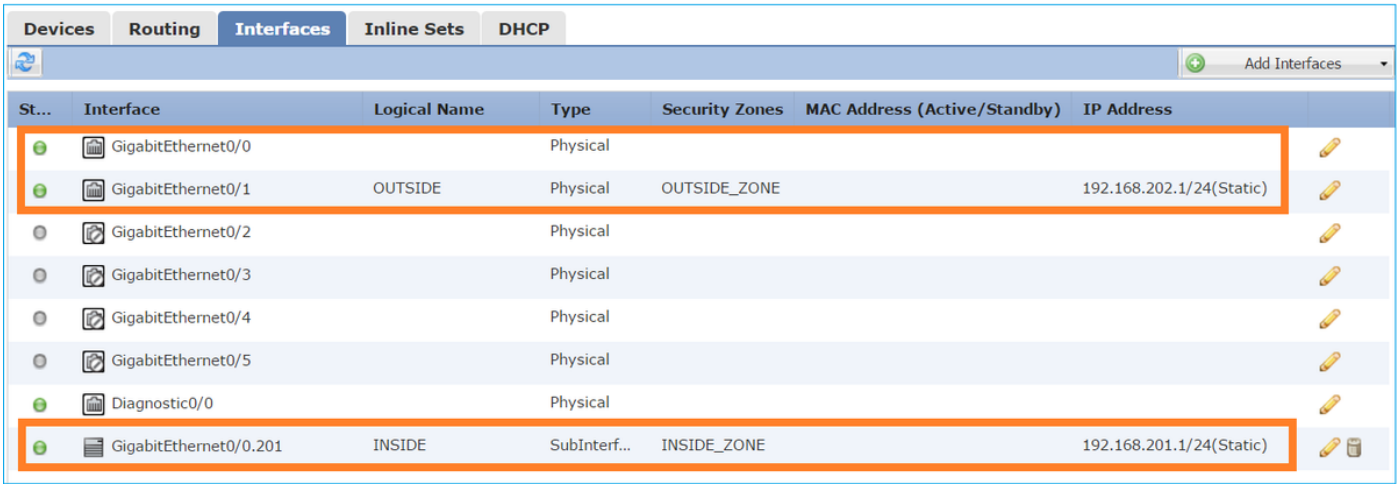


- 对于路由接口模式是：**无**
- 名称与ASA接口**nameif**是等同的
- 在FTD所有接口有安全等级= 0
- **same-security-traffic**不是可适用的在FTD。FTD接口(相互)和发夹之间的流量(内部)默认情况下允许

选择**保存**并且**部署。**

验证

从FMC GUI ：

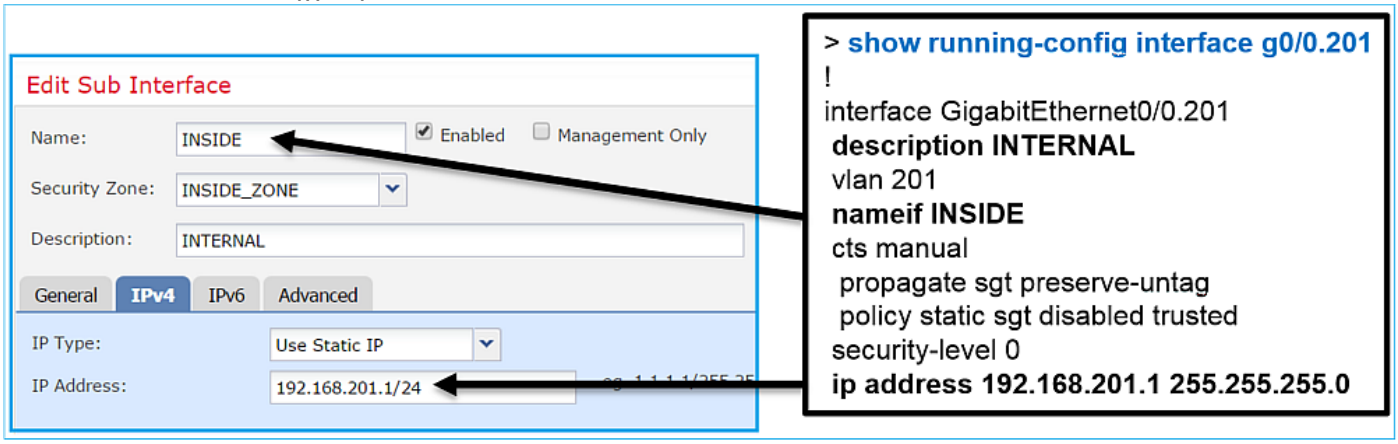


从FTD CLI ：

```
> 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-Control0/0        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：




```
> 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
>
```

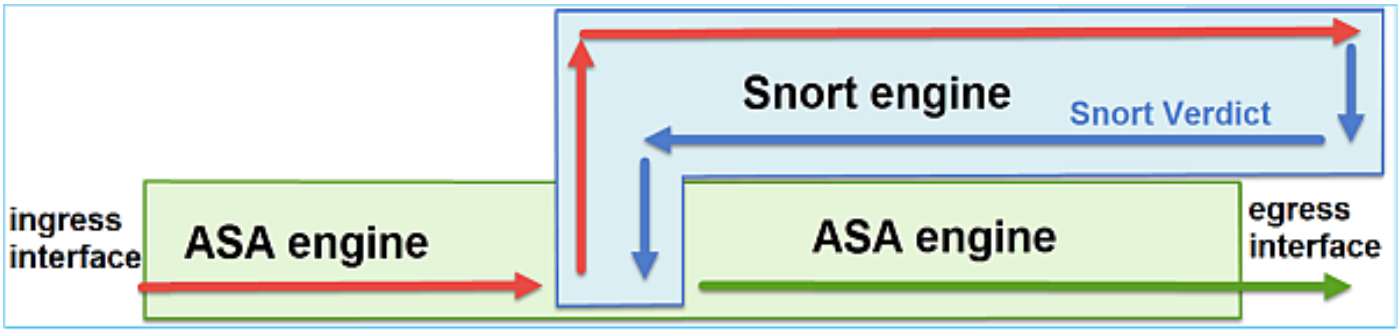
FTD路由接口操作

当路由接口是在使用中的时，请验证处理FTD的数据包。

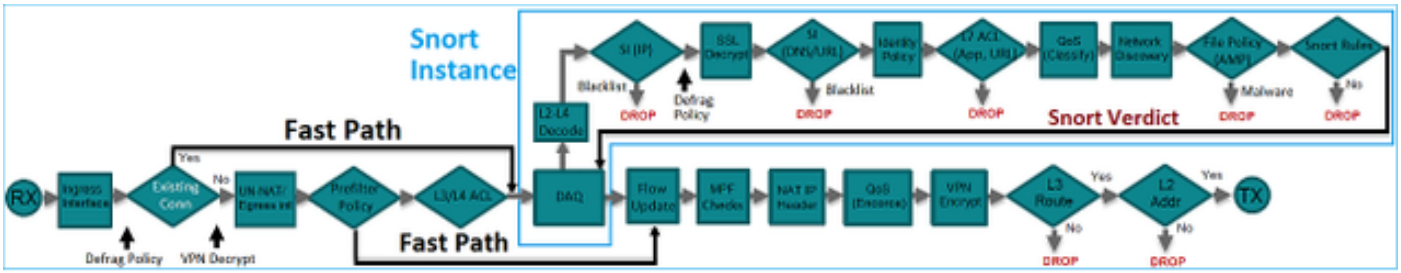
[解决方案]

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：



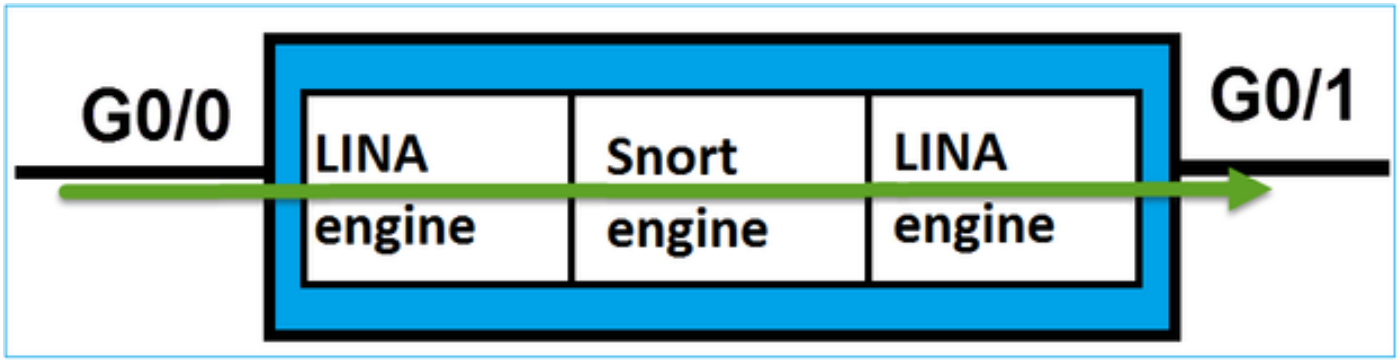
关键点

- 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	192.168.201.100
目的 IP	192.168.202.100

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

                   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
wil

                  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**