Configurando as interfaces do Firepower Threat Defense no modo roteado

Contents

Introduction

Este documento descreve a configuração, a verificação e a operação em segundo plano de uma Interface de Par em Linha em um dispositivo Firepower Threat Defense (FTD).

Prerequisites

Requirements

Não há requisitos específicos para este documento.

Componentes Utilizados

- ASA5512-X - Código FTD 6.1.0.x
- Firepower Management Center (FMC) - código 6.1.0.x

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default)

configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

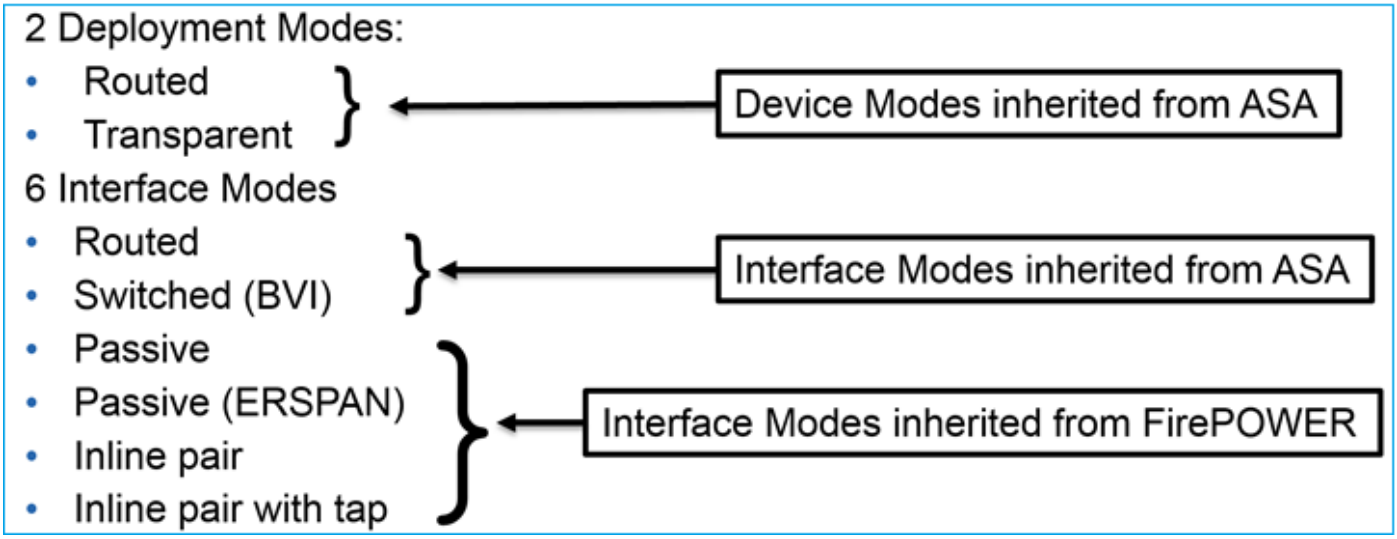
Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA555-X
- FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), máquina virtual baseada em kernel (KVM)
- Código de software FTD 6.2.x e posterior

Informações de Apoio

O FTD fornece dois modos de implantação e seis modos de interface, como mostrado nesta imagem:



Nota: Você pode combinar modos de interface em um único dispositivo FTD.

Visão geral de alto nível dos vários modos de implantação e interface do FTD:

interface FTD modo	modo de Implantação FTD	Descrição	O tráfego pode ser descartado
Roteado	Roteado	Verificações completas do mecanismo LINA e do mecanismo Snort	Yes
Comutado	Transparente	Verificações completas do mecanismo LINA e do	Yes

		mecanismo Snort	
Par em linha	Roteado ou Transparente	Mecanismo de LINA parcial e verificações completas do mecanismo de Snort	Yes
Par em linha com torneira	Roteado ou Transparente	Mecanismo de LINA parcial e verificações completas do mecanismo de Snort	No
Passivo	Roteado ou Transparente	Mecanismo de LINA parcial e verificações completas do mecanismo de Snort	No
Passivo (ERSPAN)	Roteado	Mecanismo de LINA parcial e verificações completas do mecanismo de Snort	No

Configurar

Diagrama de Rede

Configurar uma interface roteada e uma subinterface

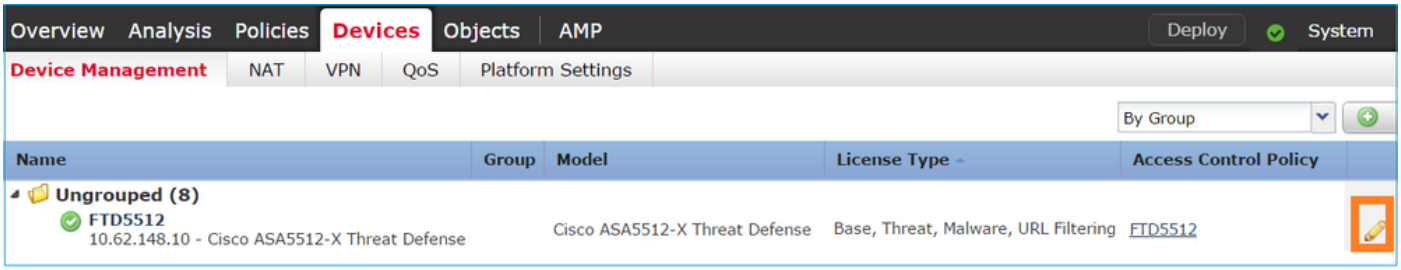
Configure a subinterface G0/0.201 e a interface G0/1 de acordo com estes requisitos:

Interface	G0/0,201	G0/1
Nome	INTERNA	EXTERNA
Zona de segurança	INSIDE_ZONE	OUTSIDE_ZONE
Descrição	INTERNO	EXTERNO
ID da subinterface	201	-
ID da VLAN	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
Duplex/Velocidade	Auto	Auto

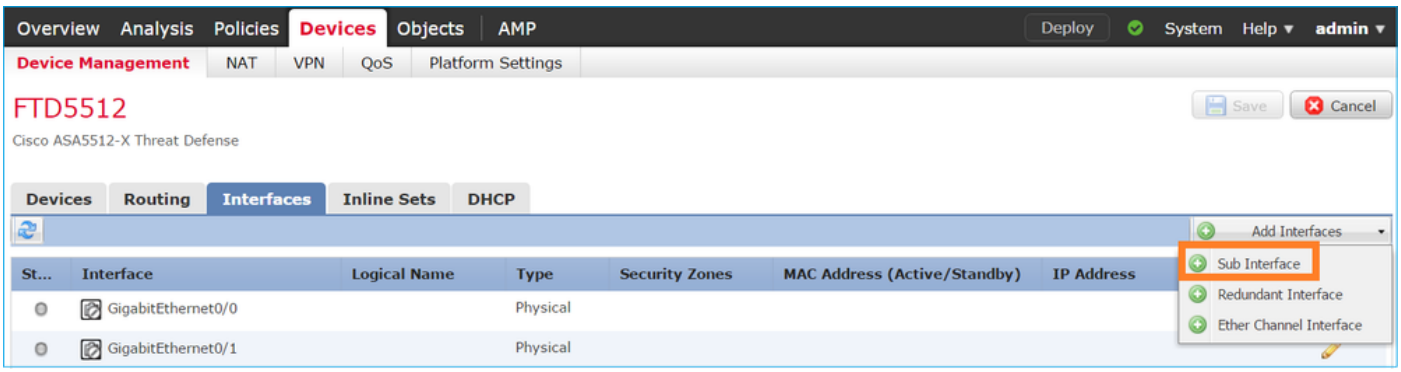
Solução

Etapa 1. Configurar a interface lógica

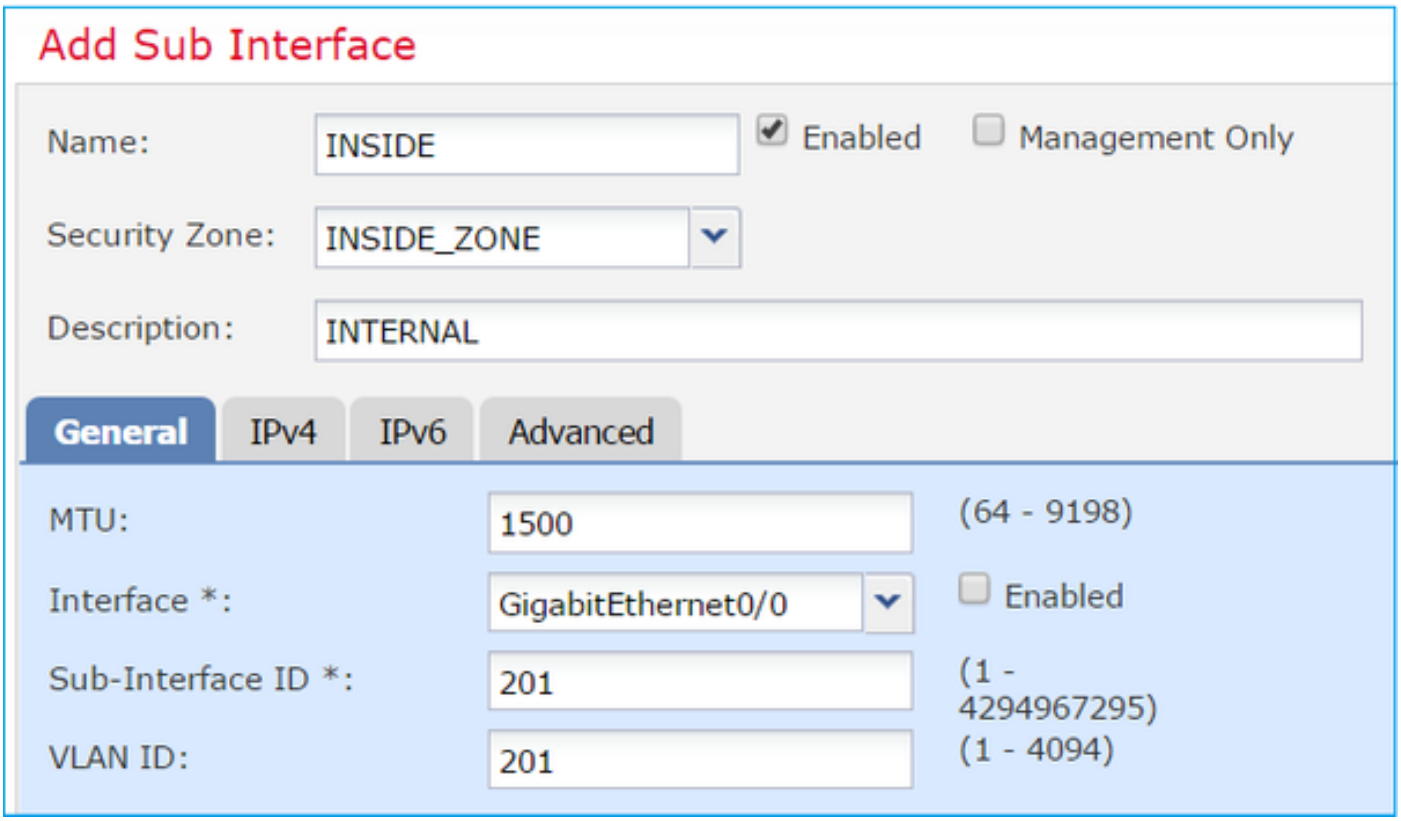
Navegue até **Dispositivos > Gerenciamento de dispositivos,** selecione o dispositivo apropriado e selecione o ícone **Editar**:



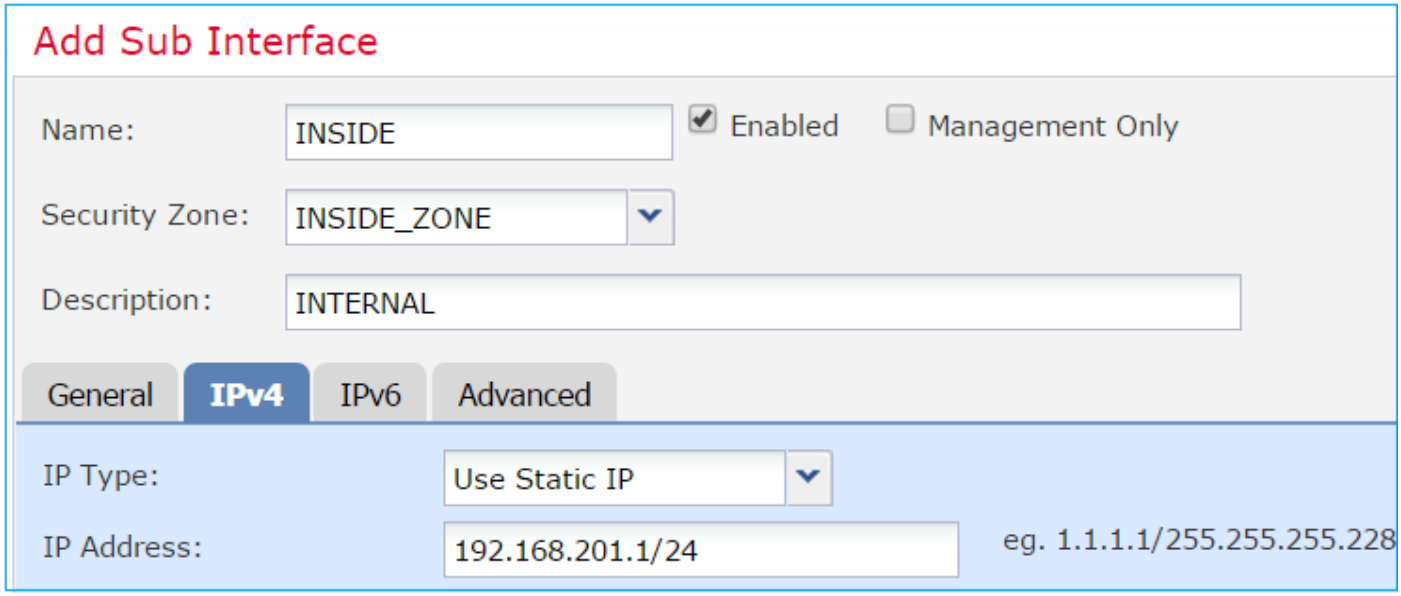
Selecione **Add Interfaces > Sub Interface**:



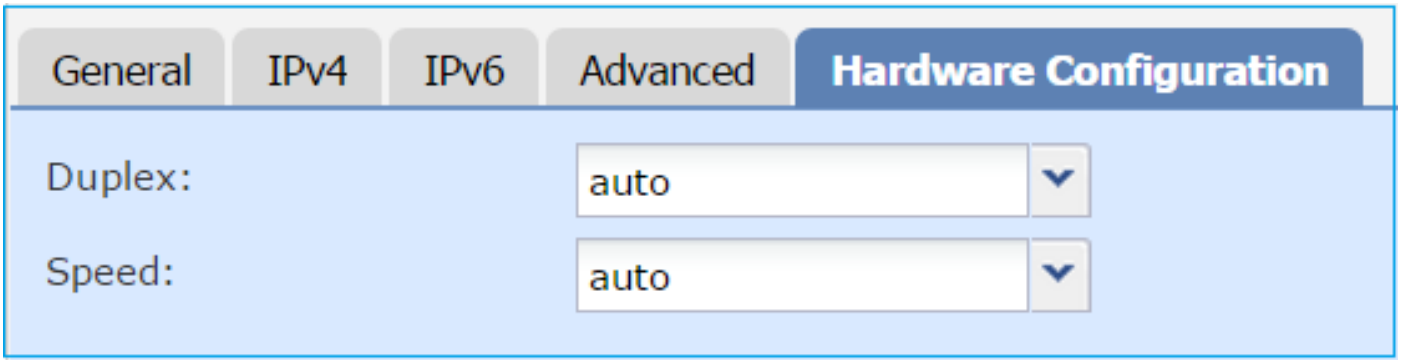
Defina as configurações da subinterface de acordo com os requisitos:



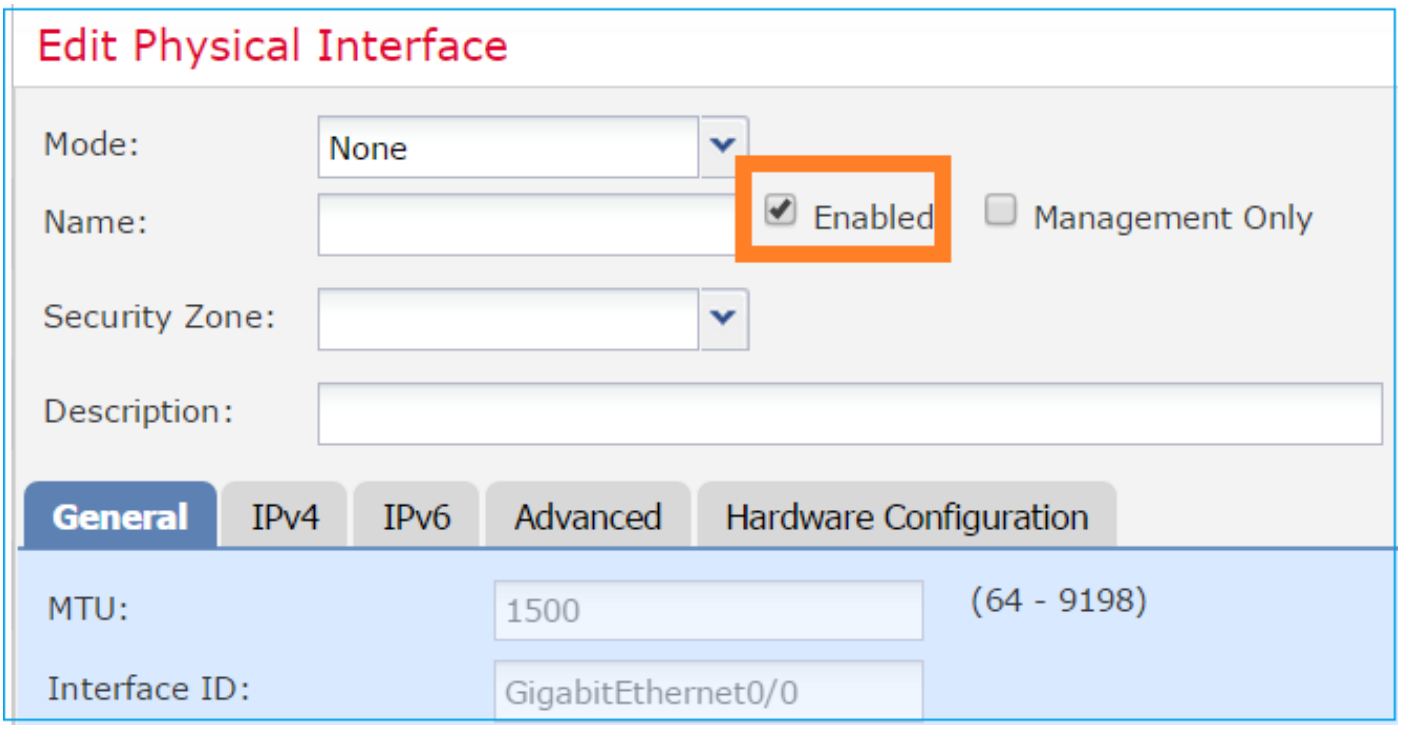
Configurações de IP da interface:



Na interface física (GigabitEthernet0/0), especifique as configurações Duplex e Speed:

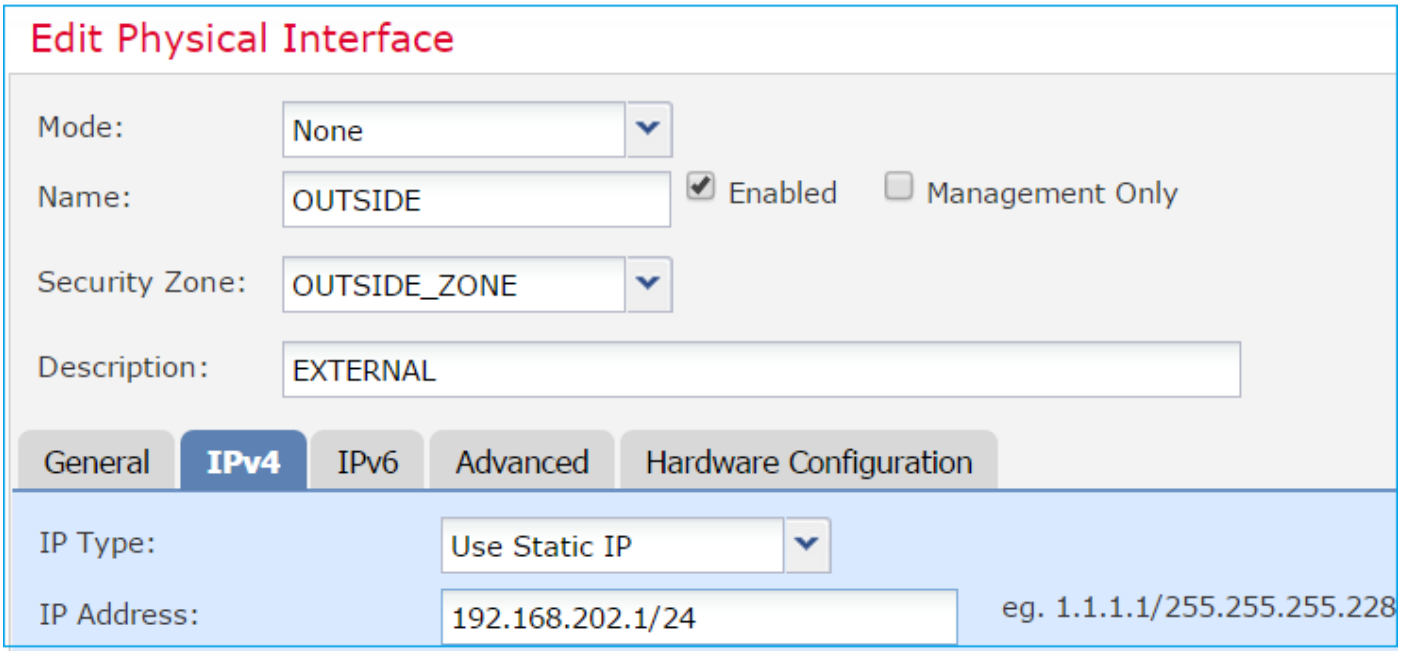


Ative a interface física (G0/0 neste caso):



Etapa 2. Configurar a interface física

Edite a interface física GigabitEthernet0/1 de acordo com os requisitos:

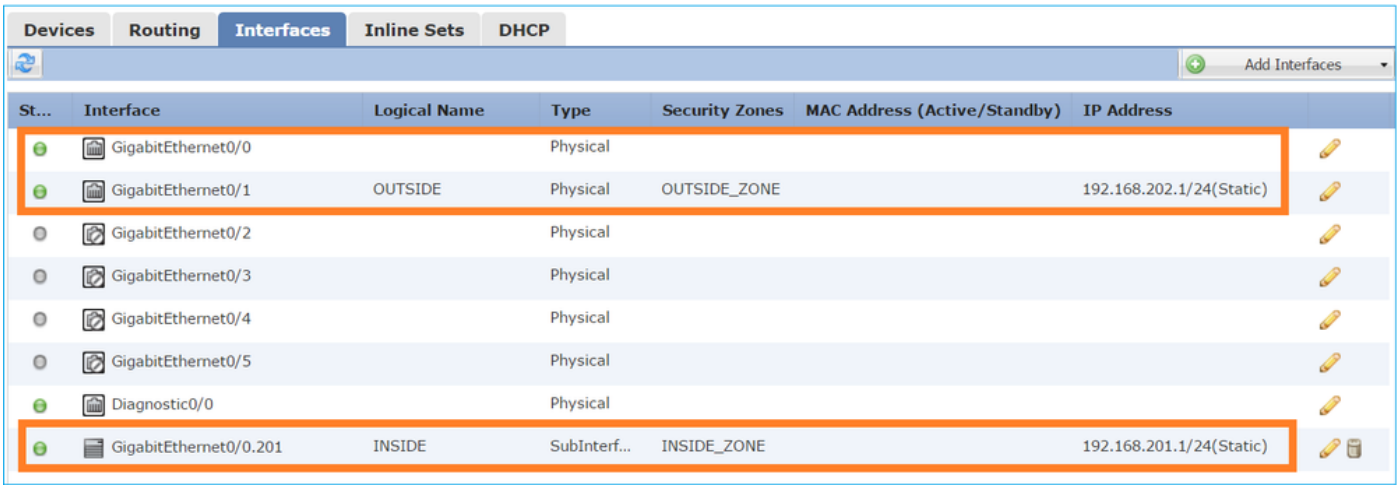


- Para a interface roteada, o modo é: **Nenhum**
- O nome é equivalente ao **nome** da interface ASA **se**
- No FTD, todas as interfaces têm nível de segurança = 0
- **same-security-traffic** não é aplicável no FTD. O tráfego entre interfaces FTD (inter) e (intra) é permitido por padrão

Selecione **Salvar** e **implantar.**

Verificação

Na GUI do FMC:

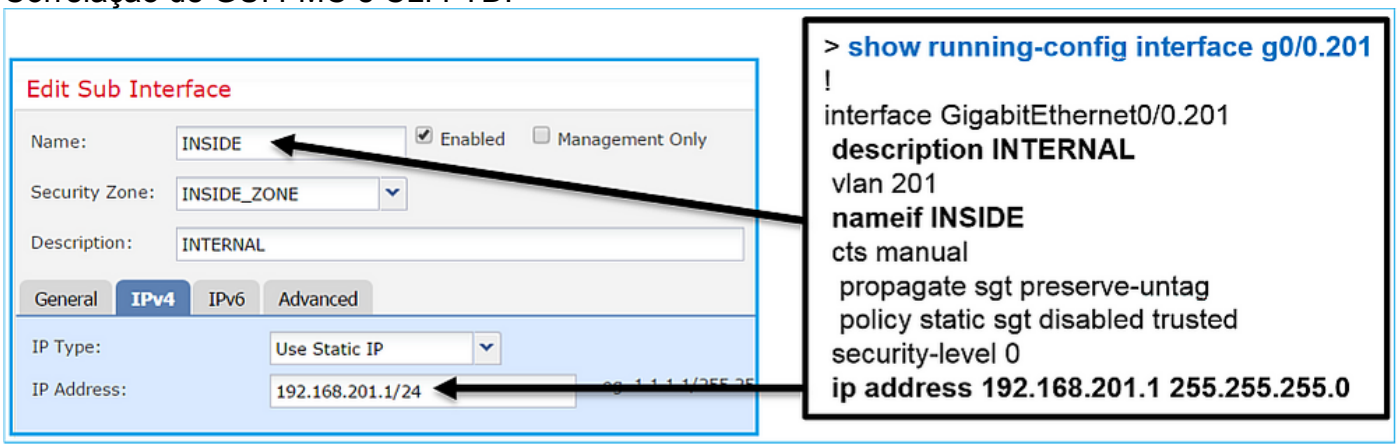


Na CLI do FTD:

```
> 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
```

Correlação de GUI FMC e CLI FTD:



```
> 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
>
```

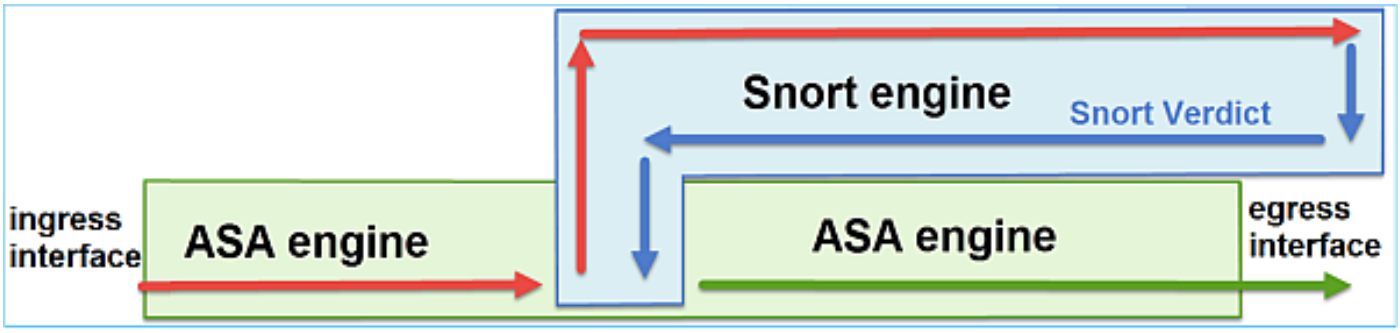
Operação da Interface Roteada FTD

Verifique o fluxo do pacote FTD quando as interfaces roteadas estão em uso.

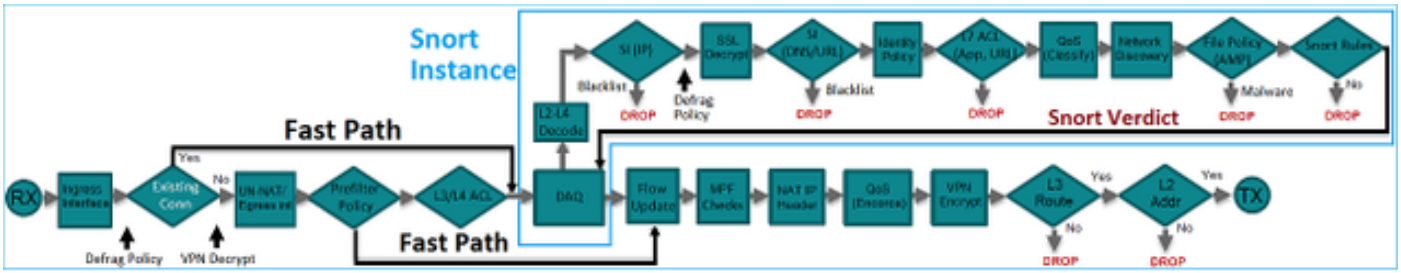
Solução

Resumo da arquitetura do FTD

Uma visão geral de alto nível do plano de dados FTD:



Esta imagem mostra algumas das verificações que ocorrem em cada mecanismo:



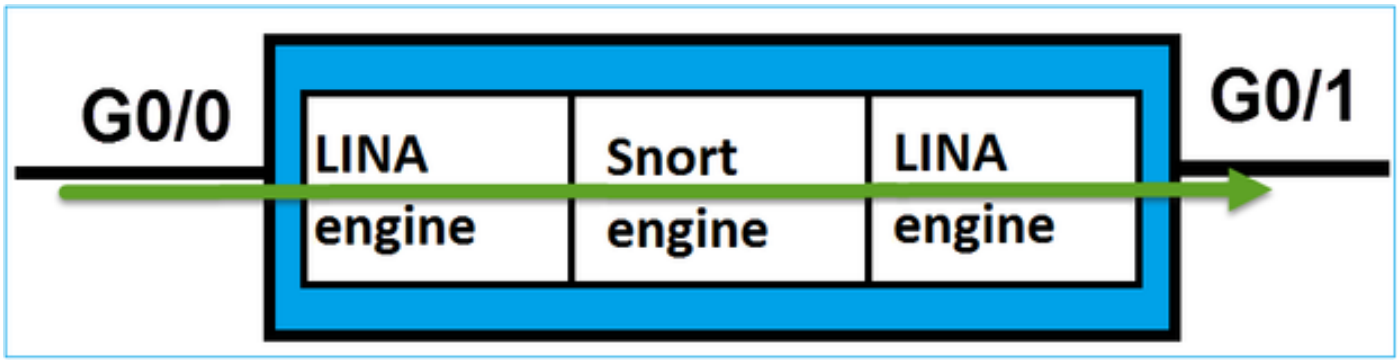
Pontos principais

- As verificações inferiores correspondem ao caminho de dados do mecanismo de LINA do FTD
- As verificações dentro da caixa azul correspondem à instância do mecanismo Snort FTD

Visão geral da interface roteada FTD

- Disponível somente na Implantação **Roteada**
- **Implantação de firewall** tradicional **L3**
- Uma ou mais interfaces roteáveis físicas ou lógicas (VLAN)
- Permite que recursos como NAT ou protocolos de roteamento dinâmico sejam configurados
- Os pacotes são encaminhados com base na **pesquisa de rota** e o próximo salto é resolvido com base na **pesquisa ARP**
- Tráfego real **pode ser descartado**
- As verificações **completas do mecanismo LINA** são aplicadas juntamente com verificações **completas do mecanismo Snort**

O último ponto pode ser visualizado da seguinte forma:



Verificar

Rastrear um pacote na interface roteada FTD

Diagrama de Rede

Use o packet-tracer com estes parâmetros para ver as políticas aplicadas:

Interface de entrada	INTERNA
Protocolo/serviço	Porta TCP 80
IP de origem	192.168.201.100
IP de Destino	192.168.202.100

Solução

Quando uma interface roteada é usada, o pacote é processado de maneira semelhante a uma interface roteada ASA clássica. Verificações como pesquisa de rota, Estrutura de política modular (MPF), NAT, pesquisa ARP etc. ocorrem no caminho de dados do mecanismo LINA. Além disso, se a política de controle de acesso exigir, o pacote será inspecionado pelo mecanismo Snort (uma das instâncias Snort), onde um veredito é gerado e retornado ao mecanismo LINA:

```
> 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

>
```

Nota: Na fase 4, o pacote é comparado a um mapa TCP chamado UM_STATIC_TCP_MAP. Este é o mapa TCP padrão no FTD.

```
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
!
>
```

Informações Relacionadas

- Guia de configuração do Cisco Firepower Threat Defense para o Firepower Device Manager, versão 6.1
- Instalação e atualização do Firepower Threat Defense em dispositivos ASA 55xx-X
- Trabalhando com capturas do Firepower Threat Defense (FTD) e do Packet Tracer
- Suporte Técnico e Documentação - Cisco Systems