

# Configurar interfaces do Firepower Threat Defense no modo roteado

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar uma interface roteada e uma subinterface](#)

[Etapa 1. Configurar a interface lógica](#)

[Etapa 2. Configurar a interface física](#)

[Operação de Interface Roteada de FTD](#)

[Visão Geral da Interface Roteada de FTD](#)

[Verificar](#)

[Rastrear um Pacote na Interface Roteada de FTD](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve a configuração, a verificação e a operação 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

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA5512-X - Código FTD 6.1.0.x
- Firepower Management Center (FMC) - código 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

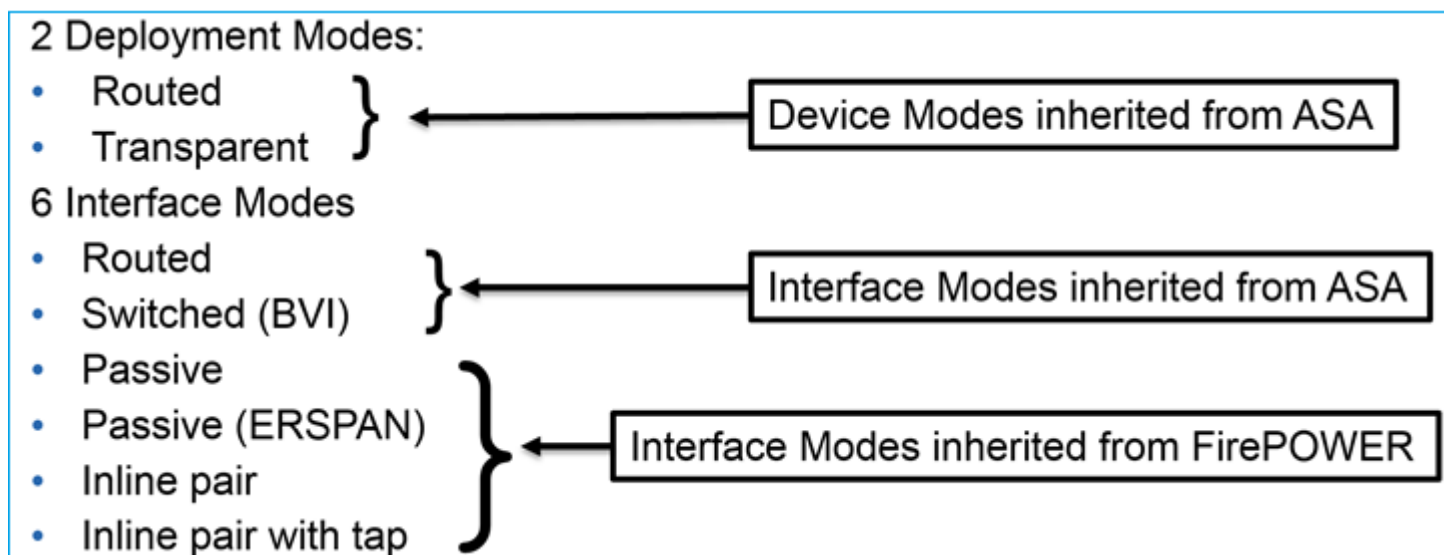
## Produtos Relacionados

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, ASA5555-X
- FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), Kernel-based Virtual Machine (KVM)
- Código de software FTD 6.2.x ou posterior

## Informações de Apoio

O Firepower Threat Defense (FTD) oferece dois modos de implantação e seis modos de interface, como mostrado nesta imagem:



**Observação:** você pode combinar modos de interface em um único dispositivo FTD.

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

interface FTD modo	Modo de Implantação de 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 mecanismo Snort	Yes

Par em linha	Roteado ou transparente	Verificações do motor LINA parcial e do motor Snort completo	Yes
Par em linha com torneira	Roteado ou transparente	Verificações do motor LINA parcial e do motor Snort completo	No
Passivo	Roteado ou transparente	Verificações do motor LINA parcial e do motor Snort completo	No
Passivo (ERSPAN)	Roteado	Verificações do motor LINA parcial e do motor Snort completo	No

## Configurar

### Diagrama de Rede



### Configurar uma interface roteada e uma subinterface

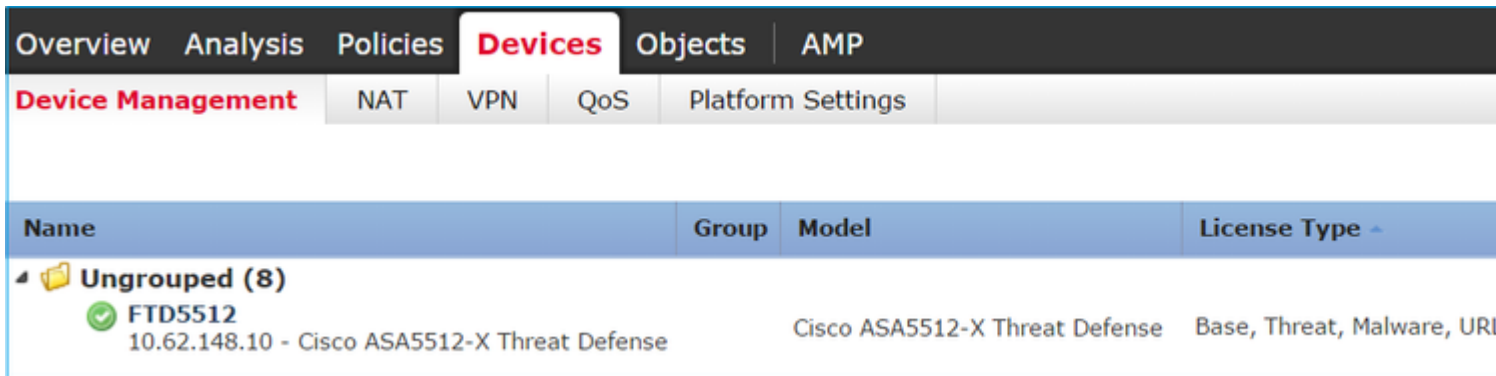
Configure a subinterface G0/0.201 e a interface G0/1 de acordo com estes requisitos:

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

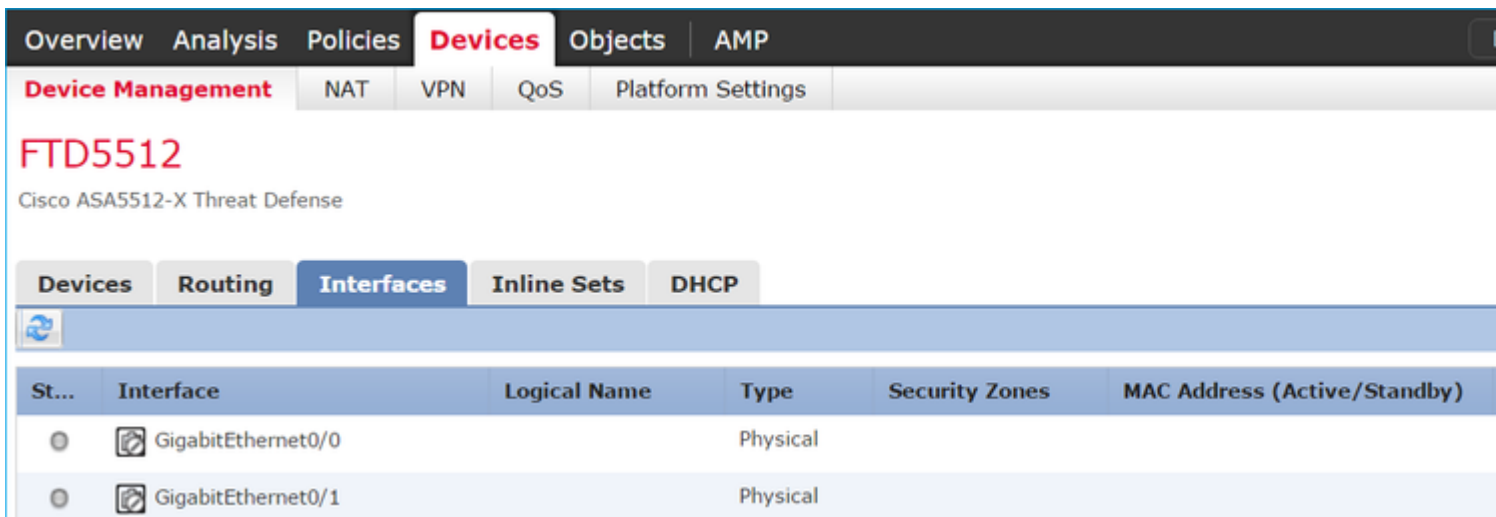
Navegue até **Devices > Device Management**, selecione o dispositivo apropriado e selecione o ícone **Edit**:



The screenshot shows the 'Devices' tab in the Palo Alto Networks management console. The navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices' (selected), 'Objects', and 'AMP'. Below the navigation bar, there are sub-tabs for 'Device Management', 'NAT', 'VPN', 'QoS', and 'Platform Settings'. The main content area displays a table of devices:

Name	Group	Model	License Type
Ungrouped (8)			
FTD5512 10.62.148.10 - Cisco ASA5512-X Threat Defense		Cisco ASA5512-X Threat Defense	Base, Threat, Malware, UR

Selecione **Add Interfaces > Sub Interface**:



The screenshot shows the 'Sub Interfaces' configuration page for device FTD5512. The navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices' (selected), 'Objects', and 'AMP'. Below the navigation bar, there are sub-tabs for 'Device Management', 'NAT', 'VPN', 'QoS', and 'Platform Settings'. The main content area displays the device name 'FTD5512' and the model 'Cisco ASA5512-X Threat Defense'. Below this, there are sub-tabs for 'Devices', 'Routing', 'Interfaces' (selected), 'Inline Sets', and 'DHCP'. The main content area displays a table of interfaces:

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

Defina as configurações de subinterface de acordo com os requisitos:

### 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)

Configurações IP da interface:

### 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

Na interface física (GigabitEthernet0/0) especifique as configurações de Duplex e Velocidade:

General | IPv4 | IPv6 | Advanced | **Hardware Configuration**

Duplex:  ▼

Speed:  ▼

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

### Edit Physical Interface

Mode:  ▼

Name:   Enabled  Management Only

Security Zone:  ▼

Description:

**General** | IPv4 | IPv6 | Advanced | Hardware Configuration

MTU:  (64 - 9198)

Interface ID:

## Etapa 2. Configurar a interface física

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

### Edit Physical Interface

Mode:  ▼

Name:   Enabled  Management Only

Security Zone:  ▼

Description:

General | **IPv4** | IPv6 | Advanced | Hardware Configuration

IP Type:  ▼

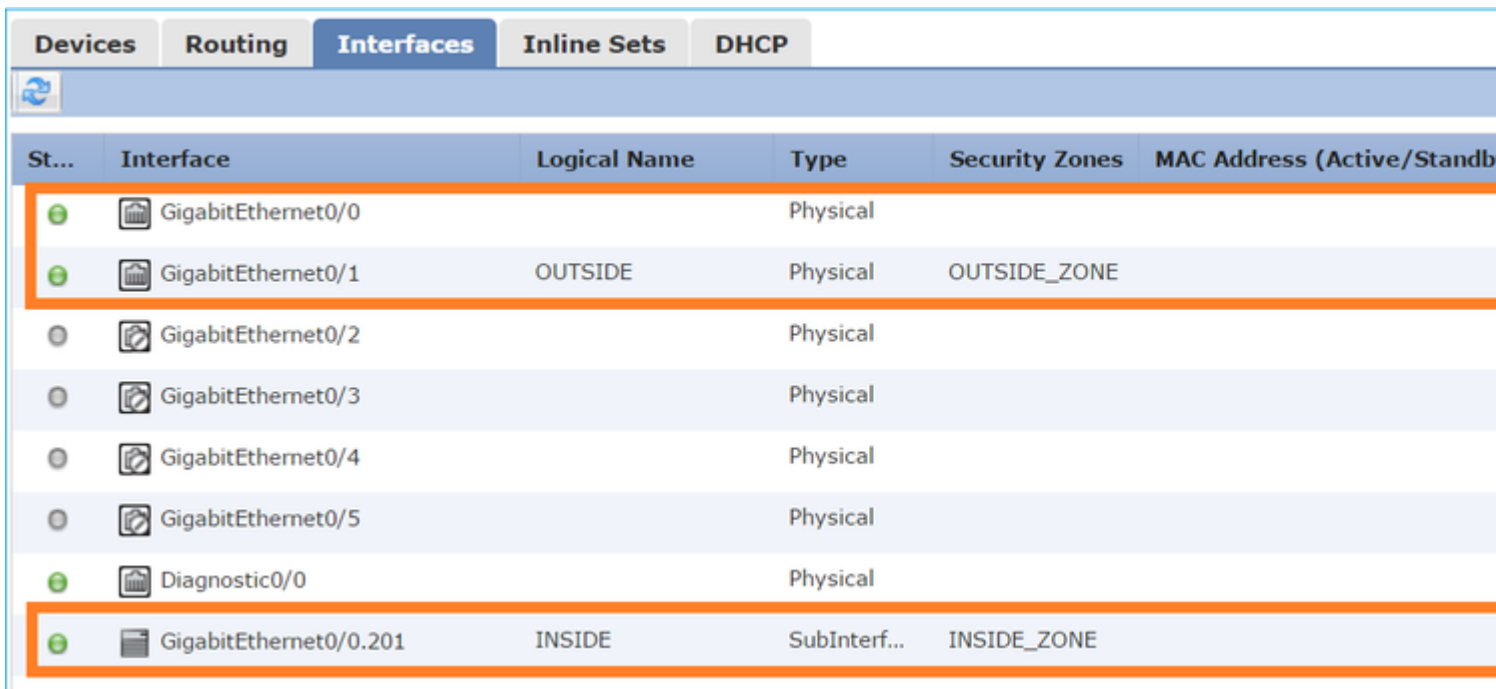
IP Address:  eg. 1.1.1.1/255.255.255.228

- 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:



St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standb
	GigabitEthernet0/0		Physical		
	GigabitEthernet0/1	OUTSIDE	Physical	OUTSIDE_ZONE	
	GigabitEthernet0/2		Physical		
	GigabitEthernet0/3		Physical		
	GigabitEthernet0/4		Physical		
	GigabitEthernet0/5		Physical		
	Diagnostic0/0		Physical		
	GigabitEthernet0/0.201	INSIDE	SubInterf...	INSIDE_ZONE	

Na CLI do FTD:

```
<#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-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

```
<#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

Correlação entre a GUI do FMC e a CLI do FTD:

**Edit Sub Interface**

Name:   Enabled  Management Only

Security Zone:  ▾

Description:

General **IPv4** IPv6 Advanced

IP Type:  ▾

IP Address:  eg. 1.1.1.1/255.255.255.0

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

<#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
>

```

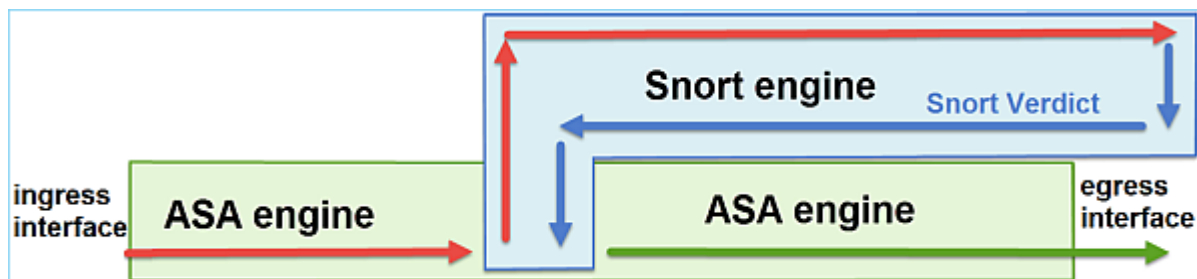
## Operação de Interface Roteada de FTD

Verifique o fluxo de pacotes FTD quando as interfaces roteadas estiverem em uso.

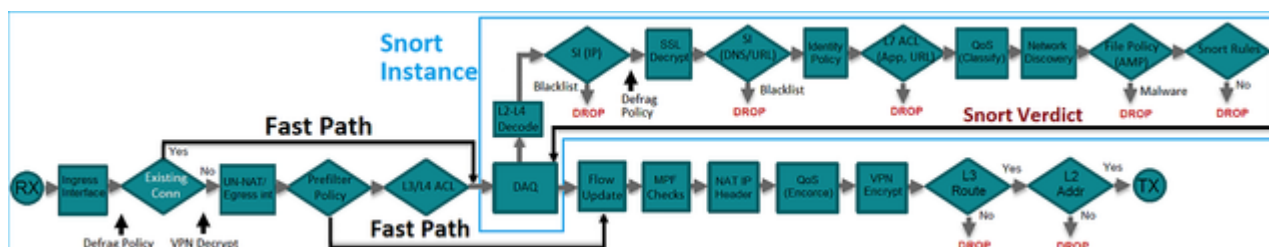
## Solução

### Visão geral da arquitetura do FTD

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



Esta figura mostra algumas das verificações que ocorrem dentro de cada mecanismo:



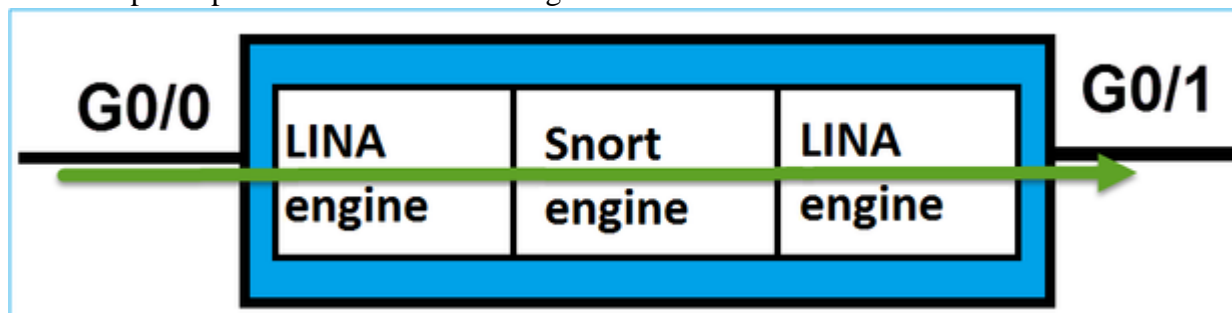
### Pontos principais

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

### Visão Geral da Interface Roteada de FTD

- Disponível somente na Implantação de **Roteamento**
- **Implantação de firewall L3** tradicional
- 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 de FTD

### Diagrama de Rede



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

<b>Interface de entrada</b>	INTERNA
<b>Protocolo/Serviço</b>	Porta TCP 80
<b>IP origem</b>	192.168.201.100
<b>IP de Destino</b>	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 Route Lookup, Modular Policy Framework (MPF), NAT, ARP lookup 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 do Snort), onde um veredito será gerado e retornará ao mecanismo LINA:

```
<#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
```

```
>
```

---

**Observação:** na fase 4, o pacote é comparado a um mapa TCP chamado UM\_STATIC\_TCP\_MAP. Este é o mapa TCP padrão no FTD.

---

```
<#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
!
```

```
>
```

## Informações Relacionadas

- [Guia de configuração do Cisco Firepower Threat Defense para Firepower Device Manager, versão 6.1](#)
- [Instalar e atualizar o Firepower Threat Defense em dispositivos ASA 55xx-X](#)
- [Defesa contra ameaças do Cisco Secure Firewall](#)
- [Suporte técnico e downloads da Cisco](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.