

Configurar a defesa da ameaça de FirePOWER conecta no modo roteado

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[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 da interface roteada FTD](#)

[Vista geral da interface roteada FTD](#)

[Verificar](#)

[Siga um pacote na interface roteada FTD](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a configuração, verificação e a operação de fundo de um par Inline conecta em um dispositivo da defesa da ameaça de FirePOWER (FTD).

Pré-requisitos

Requisitos

Não há umas exigências específicas para este documento.

Componentes Utilizados

- ASA5512-X que executa o código 6.1.0.x FTD
- Centro de gerenciamento de FirePOWER (FMC) 6.1.0.x sendo executado

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

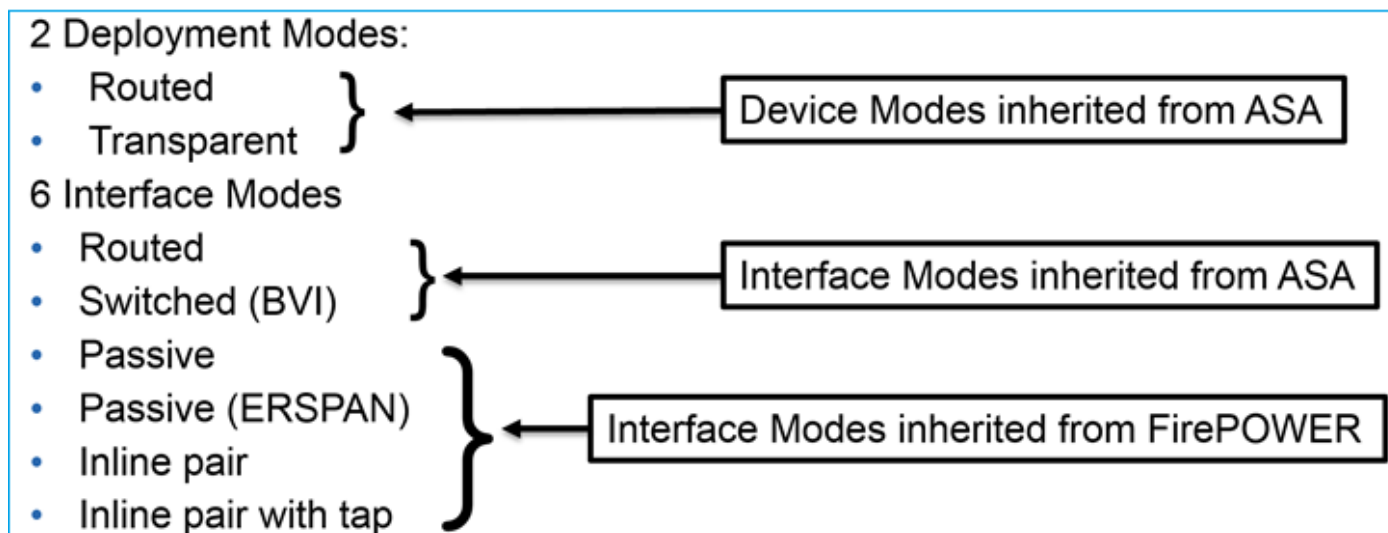
Produtos Relacionados

Este documento pode igualmente ser usado com estas versão 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), os serviços de Web das Amazonas (AW), Núcleo-baseou a máquina virtual (o KVM)
- Código de software 6.2.x FTD e mais tarde.

Informações de Apoio

FTD fornece dois modos do desenvolvimento e seis modos da relação segundo as indicações da seguinte imagem:



Note: Você pode misturar modos da relação em um único dispositivo FTD.

Visão geral de alto nível dos vários modos do desenvolvimento e da relação FTD:

Modo da relação FTD	Modo do desenvolvimento o FTD	Descrição	O tráfego pode ser deixado cair
Roteado	Roteado	Verificações completas do motor e do Snort-motor de LINA	Yes
Comutado	Transparente	Verificações completas do motor e do Snort-motor de LINA	Yes

Pares Inline	Roteado ou transparente	Motor parcial de LINA e verificações completas do Snort-motor	Yes
Pares Inline com torneira	Roteado ou transparente	Motor parcial de LINA e verificações completas do Snort-motor	No
Passivo	Roteado ou transparente	Motor parcial de LINA e verificações completas do Snort-motor	No
Voz passiva (ERSPAN)	Roteado	Motor parcial de LINA e verificações completas do Snort-motor	No

Configurar

Diagrama de Rede



Configurar uma interface roteada e uma subinterface

Configurar a subinterface G0/0.201 e a relação G0/1 conforme seguintes exigências:

Interface	G0/0.201	G0/1
Nome	INTERNA	EXTERNA
Zona de Segurança	INSIDE_ZONE	OUTSIDE_ZONE
Descrição	INTERNO	EXTERNO
Relação secundária ID	201	-
ID da VLAN	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
Duplex/velocidade	Automático	Automático

Solução

Etapa 1. Configurar a interface lógica

Navegue aos **dispositivos** > ao **Gerenciamento de dispositivos**, selecione o dispositivo apropriado e selecione o ícone da **edição**:

Overview Analysis Policies **Devices** Objects AMP Deploy System

Device Management NAT VPN QoS Platform Settings By Group +

Name	Group	Model	License Type	Access Control Policy
Ungrouped (8) FTD5512 10.62.148.10 - Cisco ASA5512-X Threat Defense		Cisco ASA5512-X Threat Defense	Base, Threat, Malware, URL Filtering	FTD5512

Selecione **adicionar relações** > **relação do sub**:

Overview Analysis Policies **Devices** Objects AMP Deploy System Help admin

Device Management NAT VPN QoS Platform Settings Save Cancel

FTD5512

Cisco ASA5512-X Threat Defense

Devices Routing **Interfaces** Inline Sets DHCP

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

- Add Interfaces
- Sub Interface**
- Redundant Interface
- Ether Channel Interface

Configurar os ajustes da subinterface conforme exigências:

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)

Conecte ajustes IP:

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

Sob a interface física (GigabitEthernet0/0) especifique os ajustes do duplex e da velocidade:

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

Duplex: ▼

Speed: ▼

Permita a interface física (G0/0 neste 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 conforme exigências:

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 **nameif da** relação ASA
- Em FTD todas as relações têm o nível de segurança = 0
- o **same-security-traffic** não é aplicável em FTD. O tráfego entre as relações FTD (inter) e o hairpinning (intra) é permitido à revelia

Selecione a **salvaguarda e distribua-a**.

Verificação

Do 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)

Do 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

Correlação FMC GUI e FTD CLI:

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
>

```

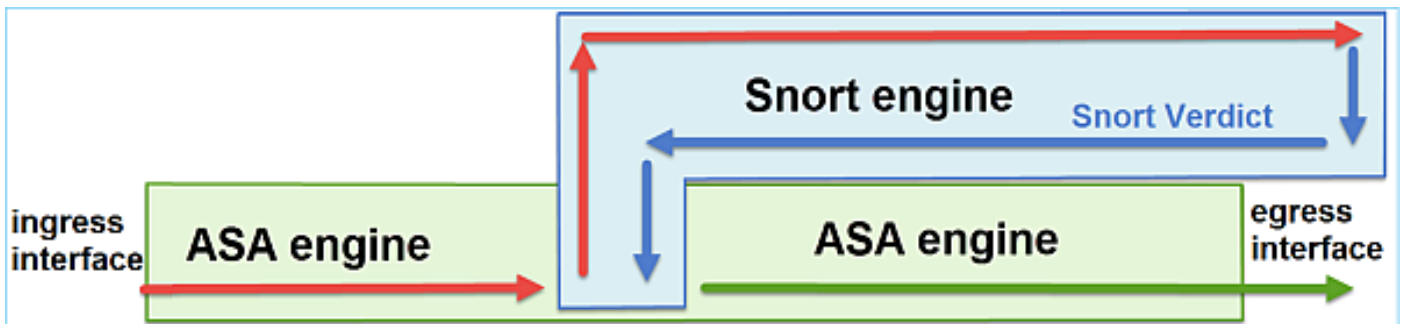
Operação da interface roteada FTD

Verifique o pacote FTD que processa quando as interfaces roteada estão no uso.

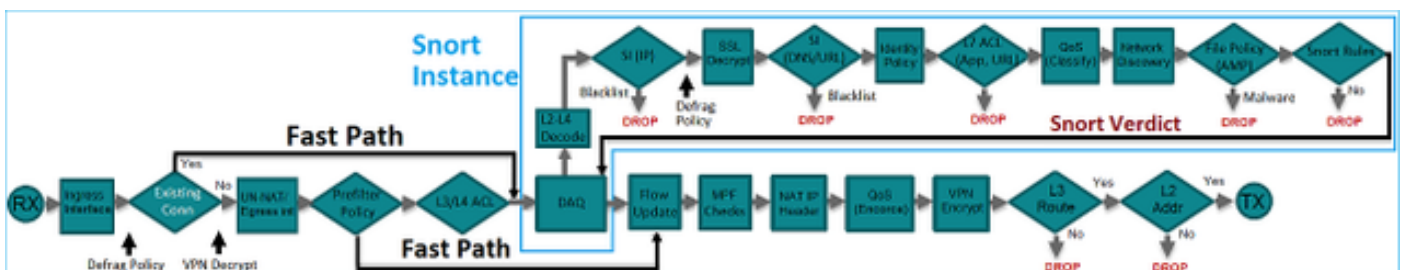
Solução

Visão geral arquitetural FTD

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



A seguinte imagem mostra algumas das verificações que ocorrem dentro de cada motor:



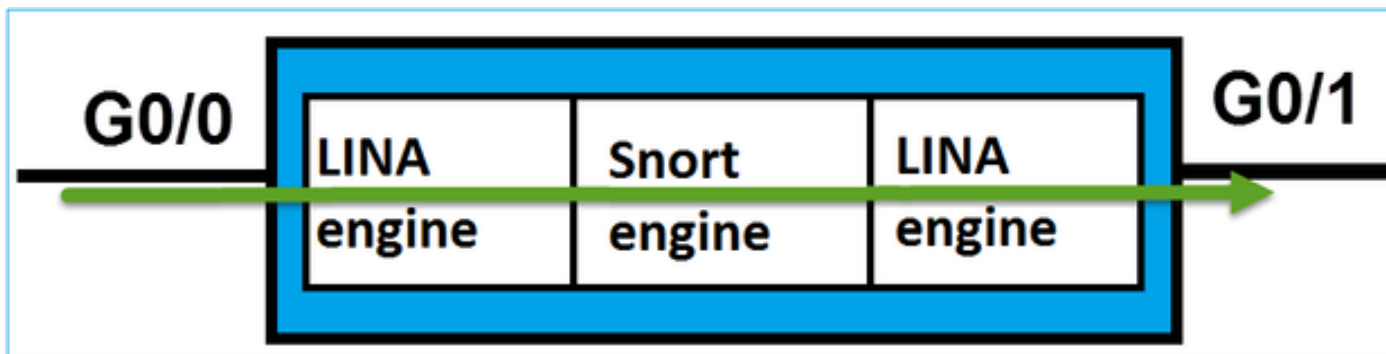
Pontos chaves

- As verificações inferiores correspondem ao trajeto de dados do motor FTD LINA
- As verificações dentro da caixa azul correspondem ao exemplo do motor do Snort FTD

Vista geral da interface roteada FTD

- Disponível somente no desenvolvimento roteado
- Desenvolvimento tradicional do Firewall L3
- Uma ou várias interfaces roteável (VLAN) físicas ou lógicas
- Permite características como o NAT ou os protocolos de roteamento dinâmico a ser configurados
- Os pacotes são enviados com base na **consulta da rota** e o salto seguinte é resolved baseado na **consulta ARP**
- O tráfego real **pode ser deixado cair**
- As verificações **completas do motor de LINA** são aplicadas junto com verificações **completas do motor do Snort**

O último ponto pode ser visualizado como segue:



Verificar

Siga um pacote na interface roteada FTD

Diagrama de Rede



Use o pacote-projétil luminoso com os seguintes parâmetros para ver as políticas aplicadas:

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

Solução

Quando uma interface roteada é usada o pacote está processado em uma maneira similar a uma interface roteada clássica ASA. As verificações como a consulta da rota, a estrutura de política modular (MPF), o NAT, a consulta ARP etc. estão ocorrendo no trajeto de dados do motor de LINA. Adicionalmente, se a política do controle de acesso exige assim, o pacote é inspecionado pelo motor do Snort (um dos exemplos do Snort) onde uma sentença (lista negra, Whitelist) é gerada e retornada de volta ao motor de 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 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
```

>

Note: Na fase 4 o pacote é verificado contra um mapa TCP chamado UM_STATIC_TCP_MAP. Este é o mapa do padrão TCP em 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

- [Manual de configuração da defesa da ameaça de Cisco FirePOWER para o gerenciador de dispositivo de FirePOWER, versão 6.1](#)
- [Instalando e promovendo a defesa da ameaça de FirePOWER em dispositivos ASA 55xx-X](#)
- [Trabalho com captações e Pacote-projétil luminoso da defesa da ameaça de FirePOWER](#)

(FTD)

- Suporte Técnico e Documentação - Cisco Systems