

Configurar la defensa de la amenaza de FirePOWER interconecta en el modo ruteado

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configure una interfaz ruteada y una subinterfaz](#)

[Paso 1. Configure la interfaz lógica](#)

[Paso 2. Configure la interfaz física](#)

[Operación de la interfaz ruteada FTD](#)

[Descripción de la interfaz ruteada FTD](#)

[Verificación](#)

[Localice un paquete en la interfaz ruteada FTD](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración, verificación y la operación de fondo de un par en línea interconecta en un dispositivo de la defensa de la amenaza de FirePOWER (FTD).

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

- ASA5512-X que funciona con el código 6.1.0.x FTD
- Centro de administración de FirePOWER (FMC) 6.1.0.x que se ejecuta

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

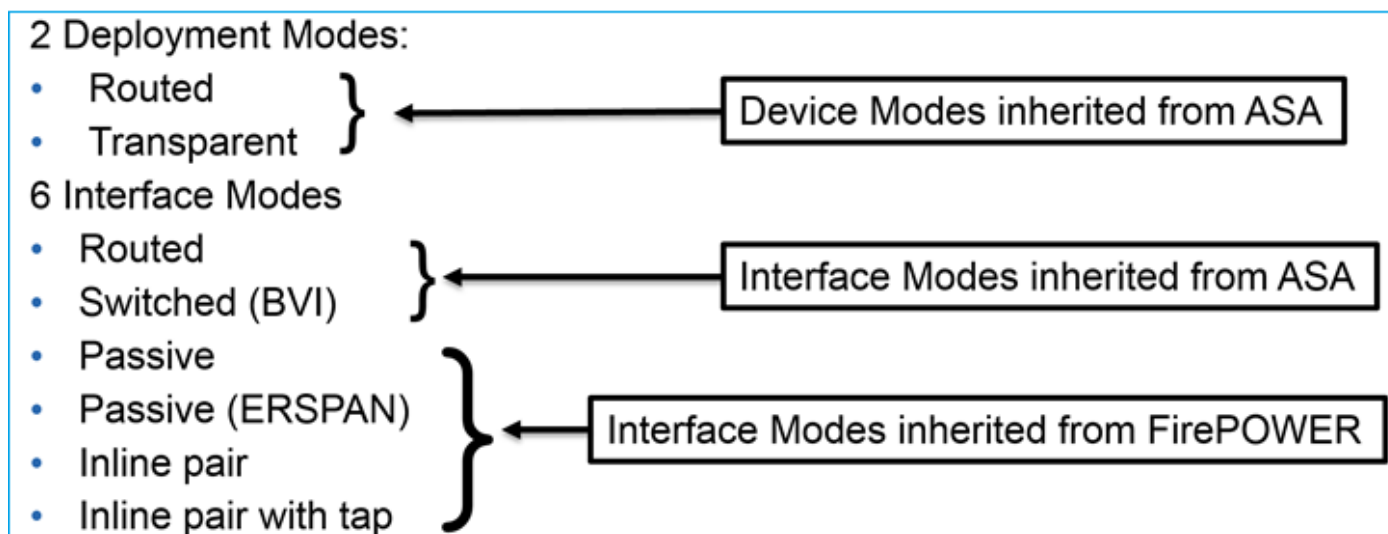
Productos Relacionados

Este documento se puede también utilizar con estas versiones de software y hardware:

- 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), servicios web del Amazonas (AWS), máquina virtual Corazón-basada (KVM)
- Código del software 6.2.x FTD y posterior.

Antecedentes

FTD proporciona dos modos del despliegue y seis modos de la interfaz tal y como se muestra en de la imagen siguiente:



Note: Usted puede mezclar los modos de la interfaz en un solo dispositivo FTD.

Descripción general de alto nivel de los diversos modos del despliegue y de la interfaz FTD:

Modo de la interfaz FTD	Modo del despliegue FTD	Descripción	El tráfico puede ser caído
Ruteado	Ruteado	Controles completos del motor y del Snort-motor de LINA	Yes
Conmutado	Transparente	Controles completos del motor y del Snort-motor de LINA	Yes
Pares en línea	Ruteado o transparente	Motor parcial de LINA y controles completos del Snort-motor	Yes

Pares en línea con el golpecito Pasivo	Ruteado o transparente	Motor parcial de LINA y controles completos del Snort-motor	No
Voz pasiva (ERSPAN)	Ruteado	Motor parcial de LINA y controles completos del Snort-motor	No

Configurar

Diagrama de la red



Configure una interfaz ruteada y una subinterfaz

Configure la subinterfaz G0/0.201 e interconecte G0/1 según los requisitos siguientes:

Interfaz	G0/0.201	G0/1
Nombre	DENTRO	FUERA
Zona de Seguridad	INSIDE_ZONE	OUTSIDE_ZONE
Descripción	INTERNO	EXTERNO
Interfaz sub ID	201	-
ID DE VLAN	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
Duplex/velocidad	Auto	Auto

Solución

Paso 1. Configure la interfaz lógica

Navegue a los **dispositivos** > a la **Administración de dispositivos**, seleccione el dispositivo apropiado y seleccione el icono del **editar**:

Overview Analysis Policies Devices Objects AMP				
Device Management NAT VPN QoS Platform Settings				
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

Seleccione agregue las interfaces > la interfaz del submarino:

Overview Analysis Policies Devices Objects AMP						
Device Management NAT VPN QoS Platform Settings						
FTD5512						
Cisco ASA5512-X Threat Defense						
Devices Routing Interfaces Inline Sets DHCP						
Add Interfaces						
<ul style="list-style-type: none"> Sub Interface Redundant Interface Ether Channel Interface 						
St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
	GigabitEthernet0/0		Physical			
	GigabitEthernet0/1		Physical			

Configure las configuraciones de la subinterfaz según los 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)

Interconecte las configuraciones IP:

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"/>	<input type="button" value="v"/>	
Description:	<input type="text" value="INTERNAL"/>		
General IPv4 IPv6 Advanced			
IP Type:	<input type="text" value="Use Static IP"/>	<input type="button" value="v"/>	
IP Address:	<input type="text" value="192.168.201.1/24"/>	eg. 1.1.1.1/255.255.255.228	

Bajo interfaz física (GigabitEthernet0/0) especifique el duplex y las configuraciones de la velocidad:

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

Habilite la interfaz física (G0/0 en este caso):

Edit Physical Interface			
Mode:	<input type="text" value="None"/>	<input type="button" value="v"/>	
Name:	<input type="text"/>	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Management Only
Security Zone:	<input type="text"/>	<input type="button" value="v"/>	
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"/>		

Paso 2. Configure la interfaz física

Edite la interfaz física GigabitEthernet0/1 según los 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 la interfaz ruteada el modo es: **Ninguno**
- El nombre es equivalente al **nameif de la** interfaz ASA
- En FTD todas las interfaces tienen nivel de seguridad = 0
- **el tráfico de seguridad igual** es no corresponde en FTD. El tráfico entre las interfaces FTD (interfaz) y el hairpinning (intra) se permite por abandono

Seleccione la **salvaguardia** y **despliegúela**.

Verificación

Del 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)

Del 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

Correlación FMC GUI y 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

>

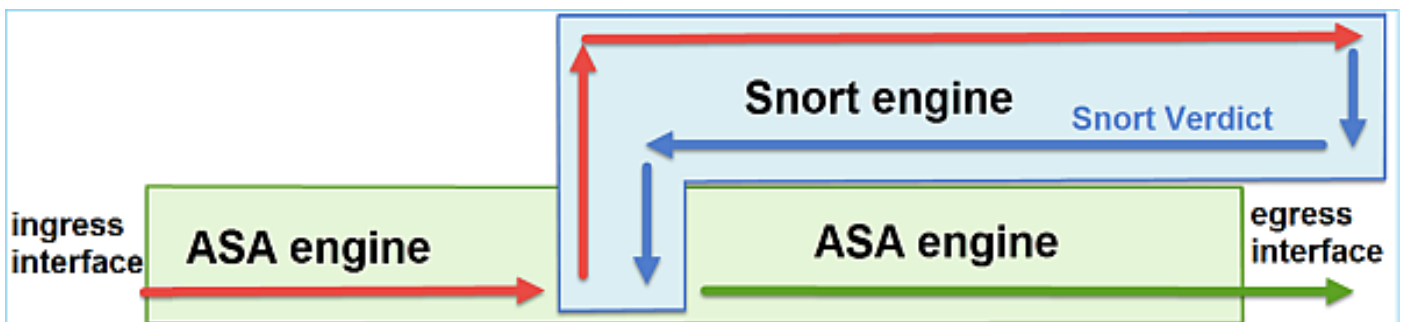
Operación de la interfaz ruteada FTD

Verifique el paquete FTD que procesa cuando las interfaces ruteadas son funcionando.

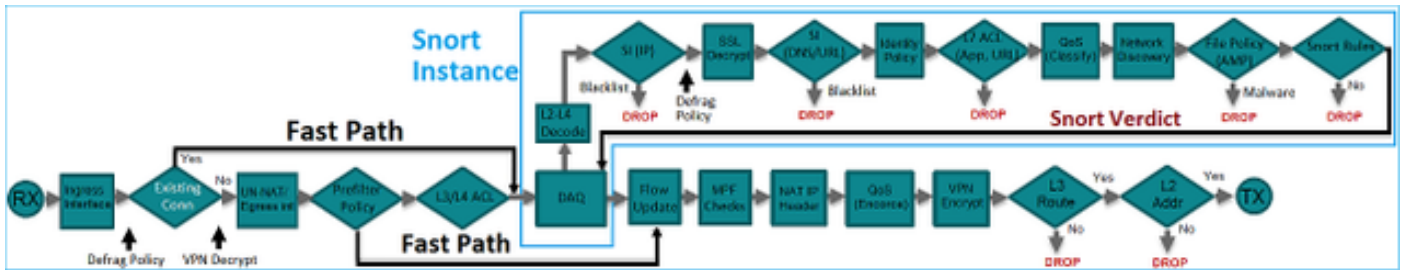
Solución

Descripción general de la arquitectura FTD

Una descripción general de alto nivel del avión de los datos FTD:



La imagen siguiente muestra algunos de los controles que ocurren dentro de cada motor:



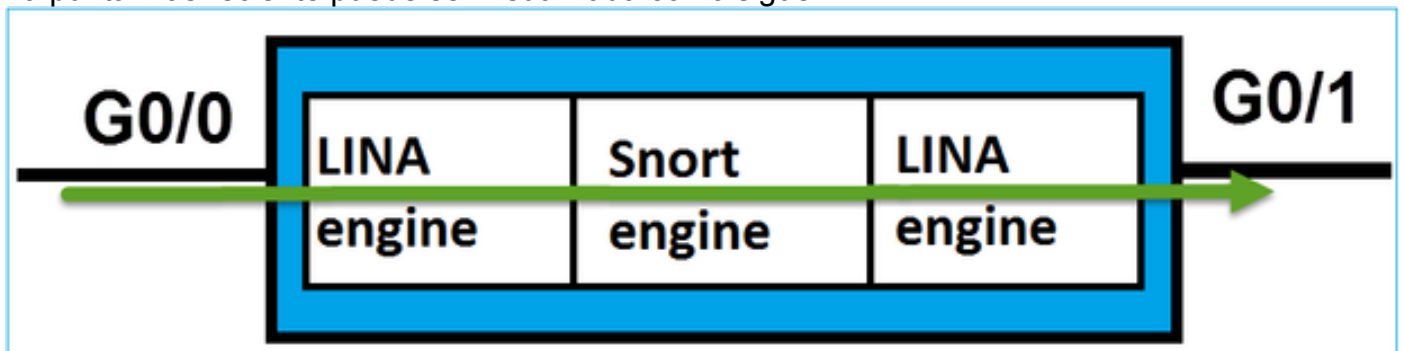
Puntos claves

- Los controles inferiores corresponden al trayecto de datos del motor FTD LINA
- Los controles dentro del recuadro azul corresponden al caso del motor del Snort FTD

Descripción de la interfaz ruteada FTD

- Disponible solamente en el despliegue **ruteado**
- **Despliegue** tradicional del **Firewall L3**
- Una o más interfaces enrutables físicas o lógicas (del VLA N)
- Permite las características como el NAT o los Dynamic Routing Protocol que se configurarán
- Los paquetes se remiten sobre la base de las **operaciones de búsqueda de la ruta** y se resuelve el salto siguiente basó en la **búsqueda ARP**
- El tráfico real **puede ser caído**
- Los controles **completos del motor de LINA** son aplicados junto con los controles **completos del motor del Snort**

La punta más reciente puede ser visualizada como sigue:



Verificación

Localice un paquete en la interfaz ruteada FTD

Diagrama de la red



Utilice el paquete-trazalíneas con los parámetros siguientes para ver las directivas aplicadas:

Interfaz de	DENTRO
Entrada	
Protocolo/ser	Puerto TCP
vicio	80
IP de la	192.168.201.1
fuelle	00
IP de destino	192.168.202.1
	00

Solución

Cuando se utiliza una interfaz ruteada el paquete se procesa de una manera similar a una interfaz ruteada clásica ASA. Los controles como las operaciones de búsqueda de la ruta, el Marco de políticas modular (MPF), NAT, la búsqueda ARP etc están ocurriendo en el trayecto de datos del motor de LINA. Además, si la directiva del control de acceso requiere así pues, el paquete es examinado por el motor del Snort (uno de los casos del Snort) donde un veredicto (lista negra, lista blanca) se genera y se vuelve de nuevo al 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

1t/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: En la fase 4 el paquete se marca contra una correspondencia TCP llamada UM_STATIC_TCP_MAP. Éste es el mapa del valor por defecto TCP en 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  
!  
>
```

Información Relacionada

- [Guía de configuración de la defensa de la amenaza de Cisco FirePOWER para el administrador de dispositivo de FirePOWER, versión 6.1](#)
- [Instalando y actualizando la defensa de la amenaza de FirePOWER en los dispositivos ASA 55xx-X](#)
- [Trabajo con las capturas y el Paquete-trazalíneas de la defensa de la amenaza de FirePOWER \(FTD\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)