Configurar la defensa de la amenaza de la potencia de fuego interconecta en el modo ruteado

Contenido

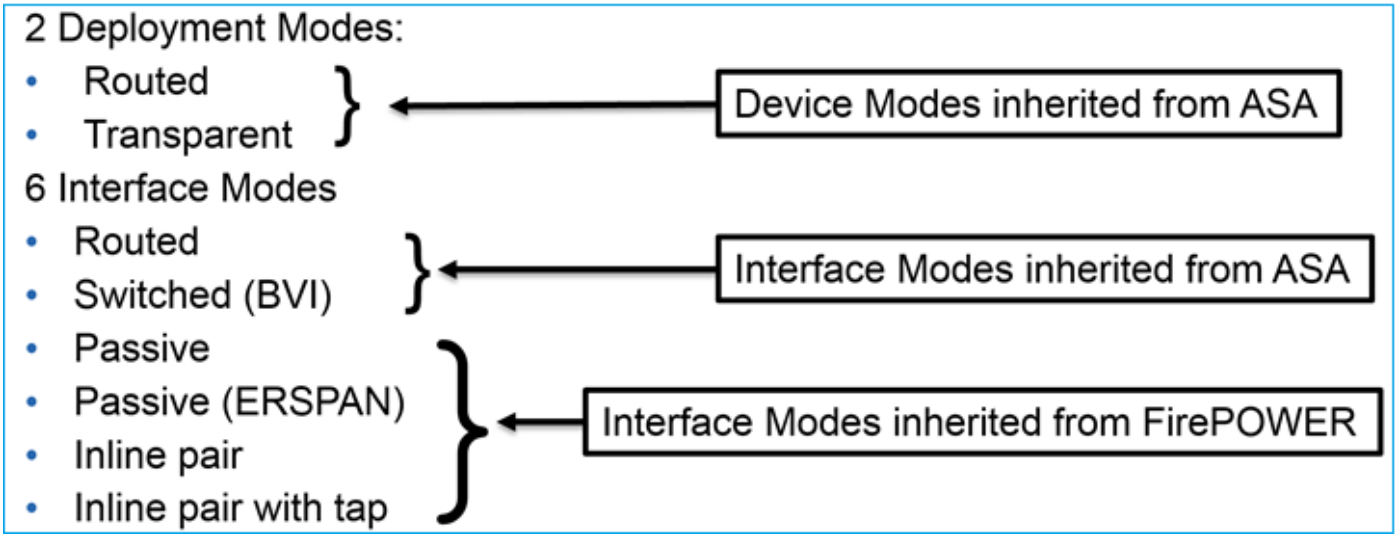
[Introducción](#)
[El objetivo](#)
[Componentes usados](#)
[Agregar una interfaz ruteada y una interfaz sub](#)
[Topología](#)
[Paso 1 - Configurando la interfaz lógica (interfaz sub)](#)
[Paso 2 - Configurar la interfaz física](#)
[Operación de la interfaz ruteada FTD](#)
[Descripción general de la arquitectura FTD](#)
[Descripción de la interfaz ruteada FTD](#)
[Localizar un paquete en la interfaz ruteada FTD](#)
[Documentos Relacionados](#)

Introducción

La defensa de la amenaza de la potencia de fuego (FTD) es una imagen del software unificada que se puede instalar en las Plataformas siguientes:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR4100, FPR9300
- VMware (ESXi)
- Servicios web del Amazonas (AWS)
- KVM
- Módulo del router ISR

FTD proporciona 2 modos del despliegue y 6 modos de la interfaz



Nota: Usted puede mezclar los modos de la interfaz en un dispositivo del sigle FTD

Aquí está una 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	ASA-motor y controles completos del Snort-motor	Sí
Conmutado	Transparente	ASA-motor y controles completos del Snort-motor	Sí
Pares en línea	Ruteado o transparente	ASA-motor parcial y controles completos del Snort-motor	Sí
Pares en línea con el golpecito	Ruteado o transparente	ASA-motor parcial y controles completos del Snort-motor	No
Pasivo	Ruteado o transparente	ASA-motor parcial y controles completos del Snort-motor	No
Voz pasiva (ERSPAN)	Ruteado	ASA-motor parcial y controles completos del Snort-motor	No

El objetivo

La meta de este documento está a:

- Demuestre cómo configurar una interfaz ruteada FTD y una interfaz sub
- Describa la operación del modo de la interfaz ruteada

Componentes usados

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

Agregar una interfaz ruteada y una interfaz sub

Configure la interfaz sub G0/0.201 e interconecte G0/1 por los requisitos siguientes:

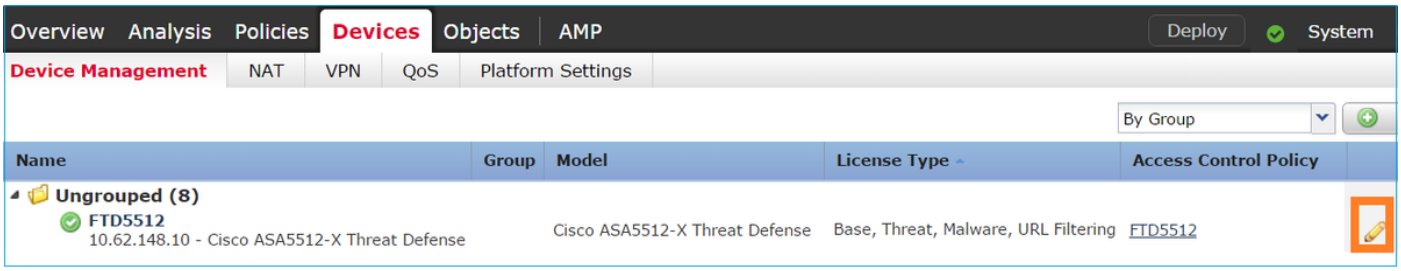
Interfaz	G0/0.201	G0/1
Nombre	DENTRO	FUERA
Zona de Seguridad	INSIDE_ZONE	OUTSIDE_ZONE
Descripción	INTERNO	EXTERNO
Interfaz sub ID	201	-
ID DE VLAN	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
Duplex/velocidad	Auto	Auto

Topología

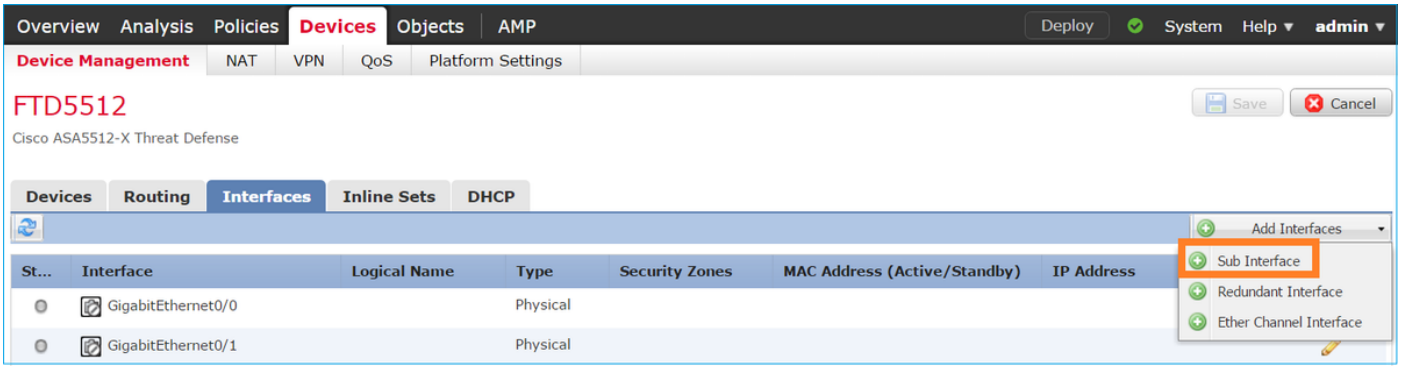
Solución

Paso 1 - Configurando la interfaz lógica (interfaz sub)

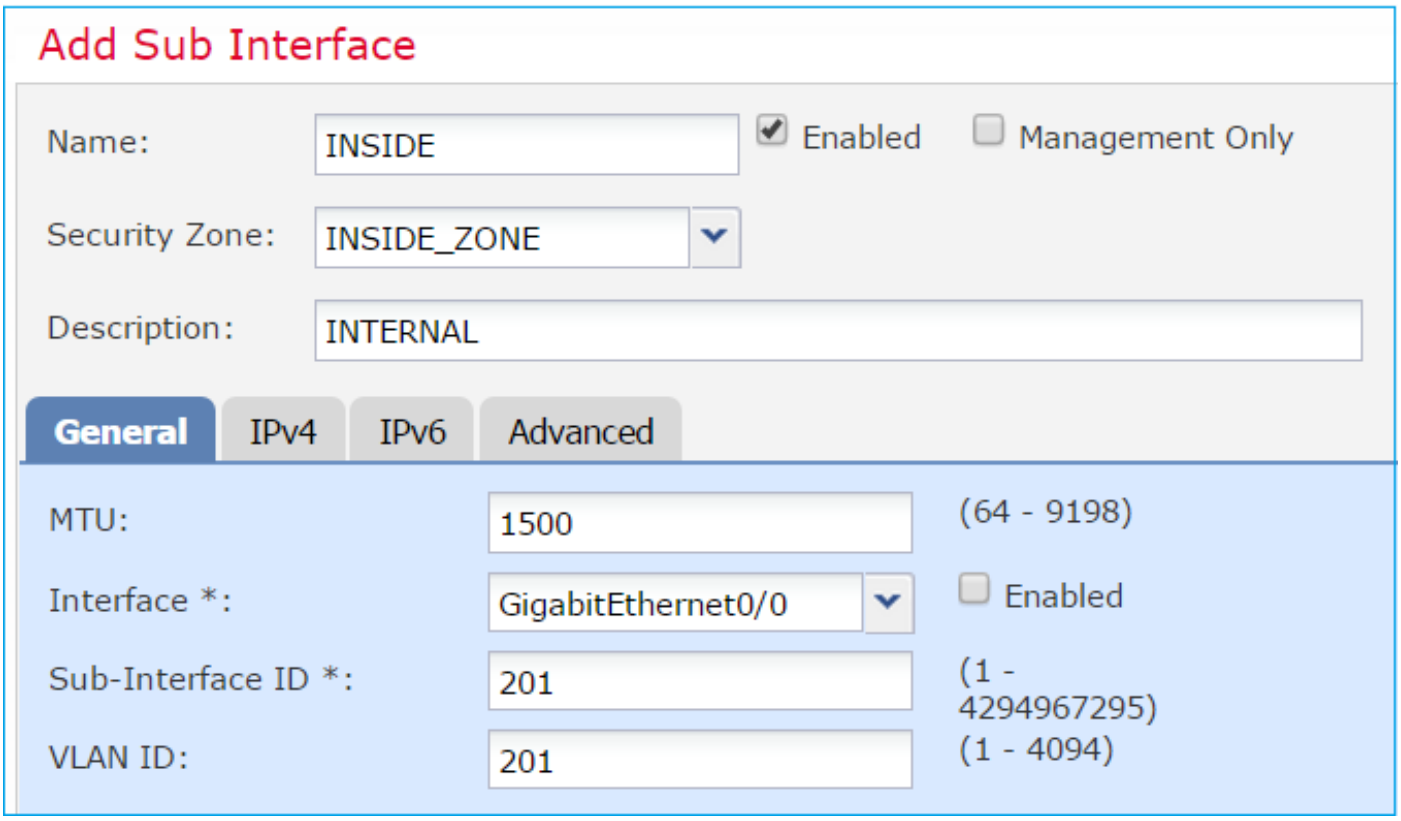
Navegue a los **dispositivos > a la Administración de dispositivos,** seleccione el dispositivo apropiado y haga clic en **editan el** icono:



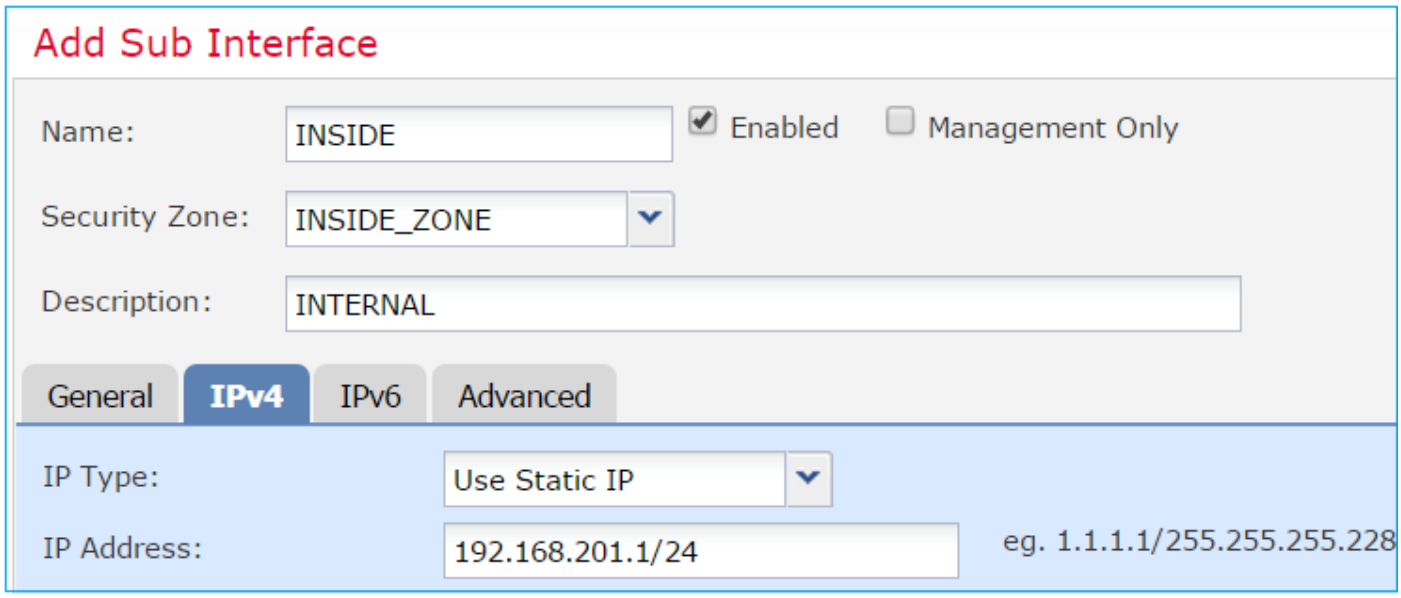
Haga clic en **agregan las interfaces > la interfaz del submarino**



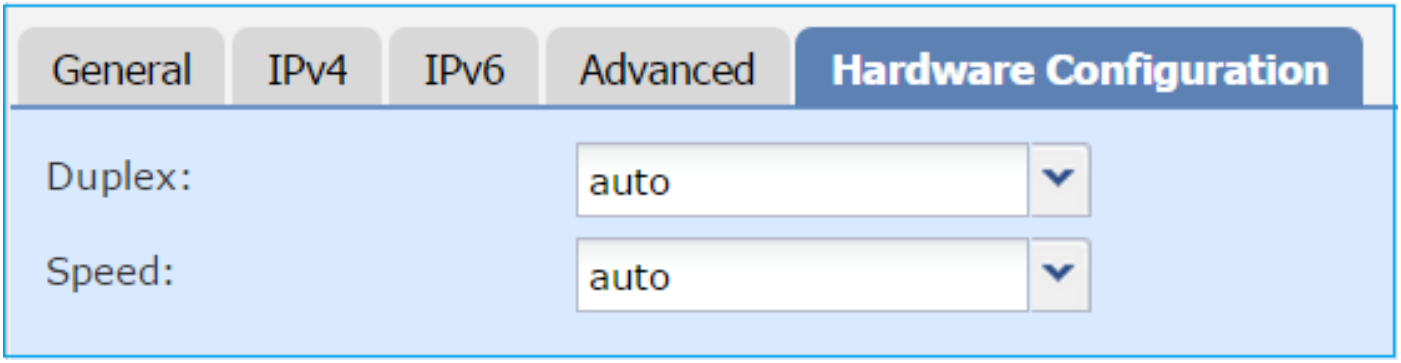
Configure las configuraciones sub de la interfaz por los requisitos:



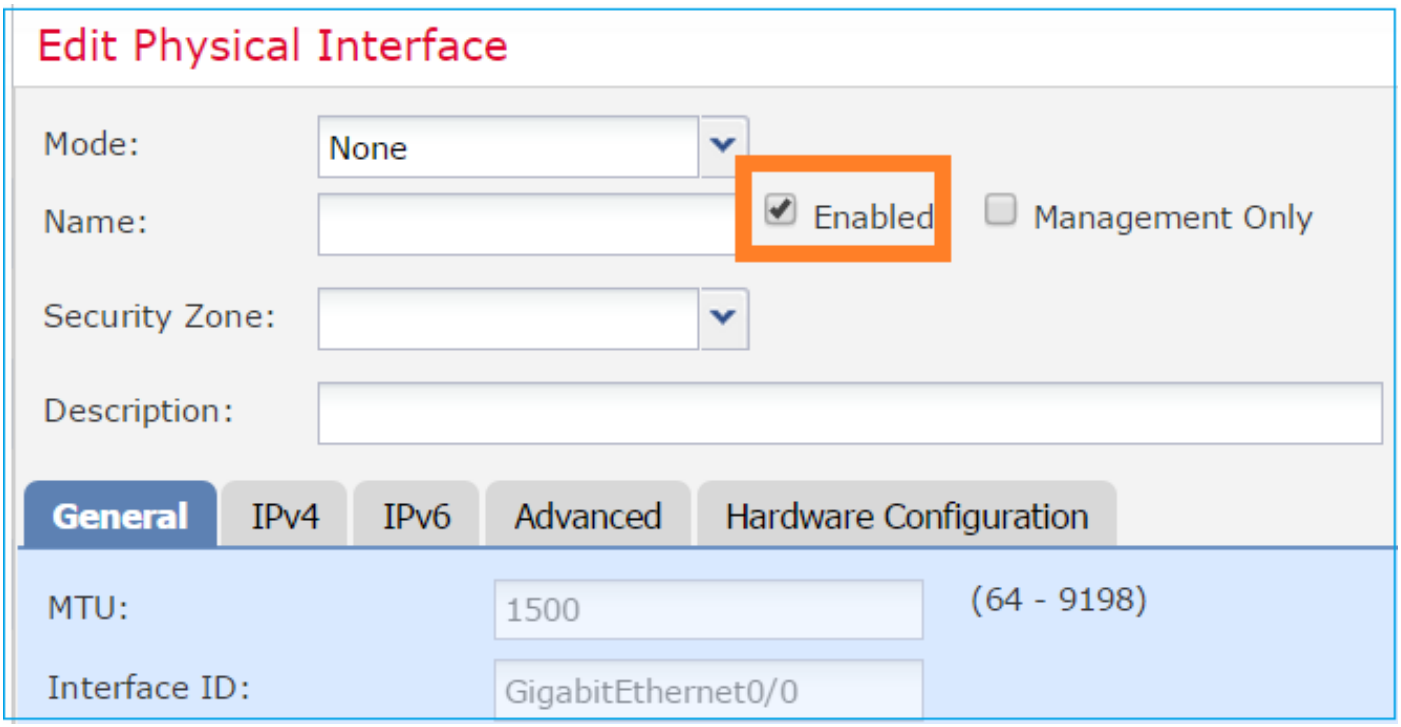
Interconecte las configuraciones IP:



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

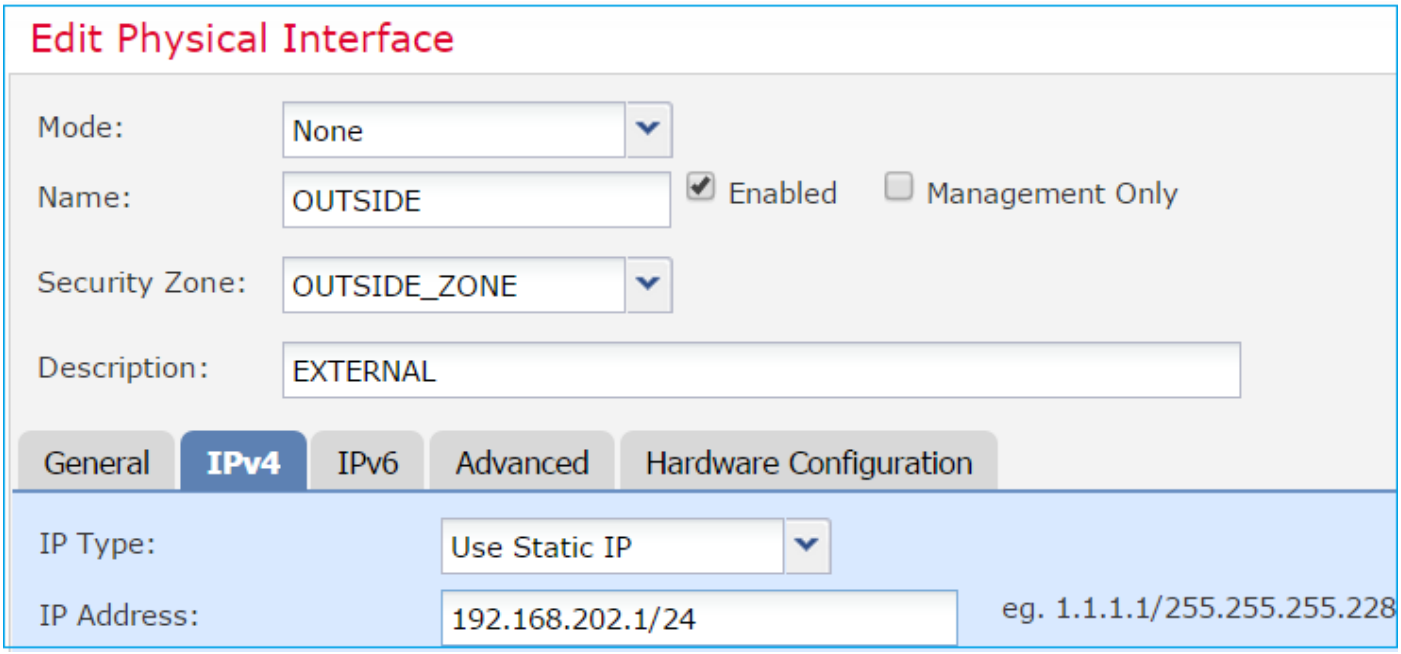


Habilite la interfaz física (G0/0 en este caso):



Paso 2 - Configurar la interfaz física

Edite la interfaz física GigabitEthernet0/1 según los requisitos:

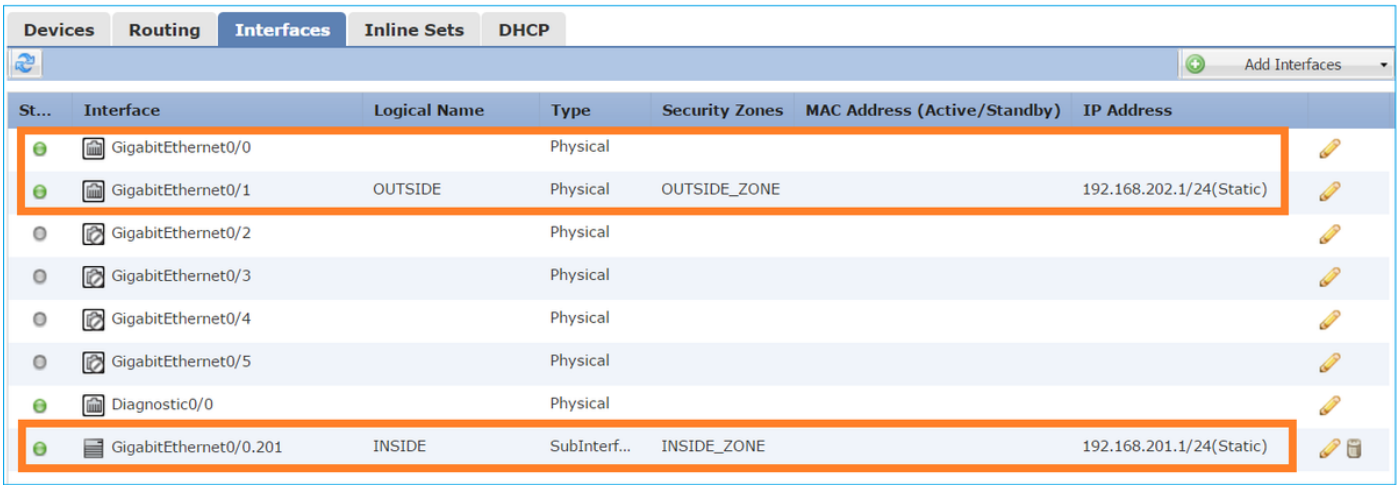


- Para la interfaz ruteada el modo es: **Ninguno**
- El nombre es equivalente al **nameif de la** interfaz ASA
- En FTD todas las interfaces tienen nivel de seguridad = 0
- el "trafico de seguridad igual" es no corresponde en FTD. El tráfico entre las interfaces FTD (interes) y el hairpinning (intra) se permite por abandono.

Finalmente **salve** y **despliegue**

Verificación

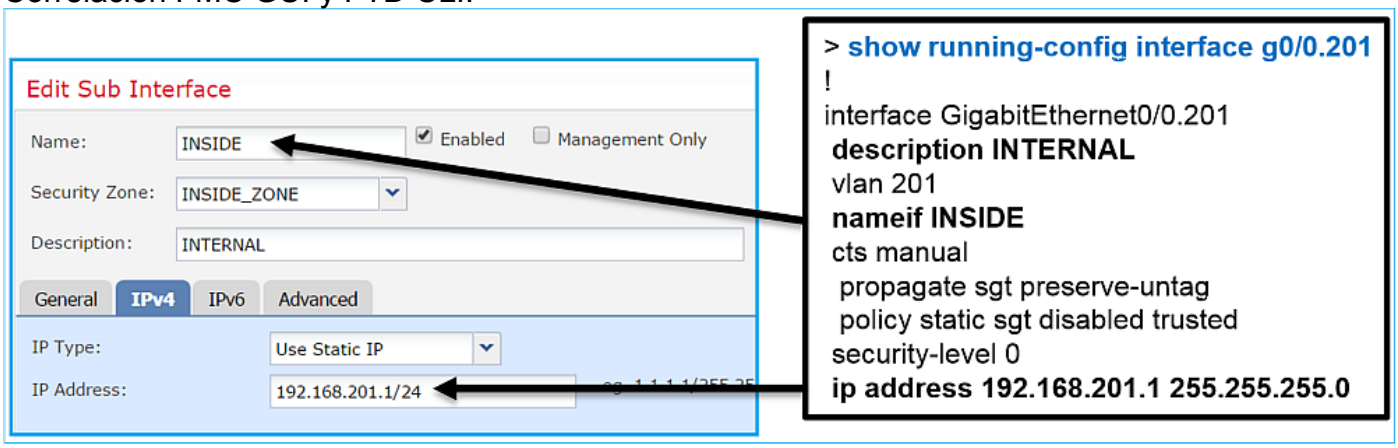
Del FMC GUI:



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-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
```

Correlación FMC GUI y FTD CLI:




```
> 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 >
```

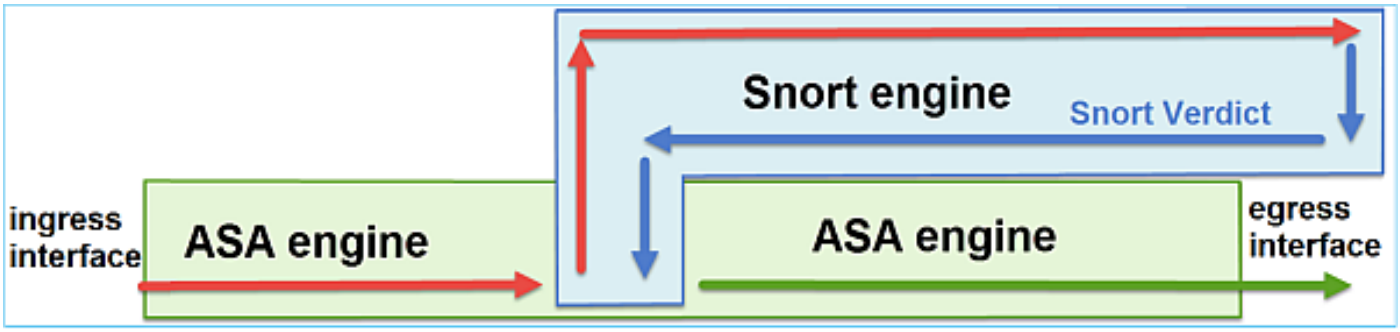
Operación de la interfaz ruteada FTD

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

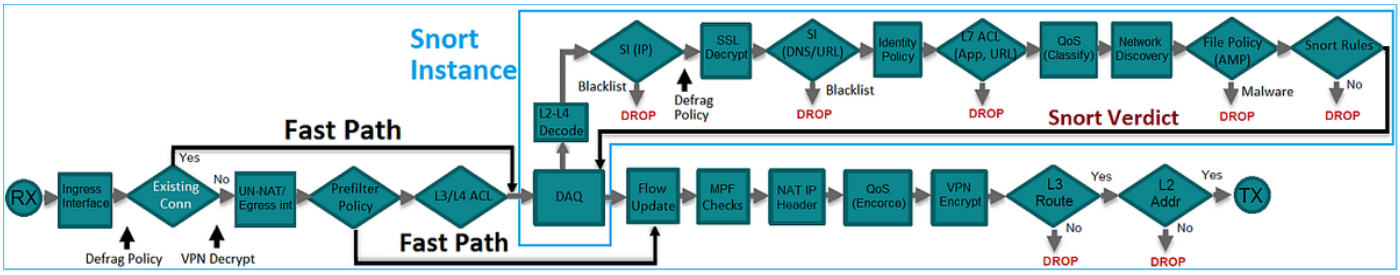
Solución

Descripción general de la arquitectura FTD

Aquí está 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:



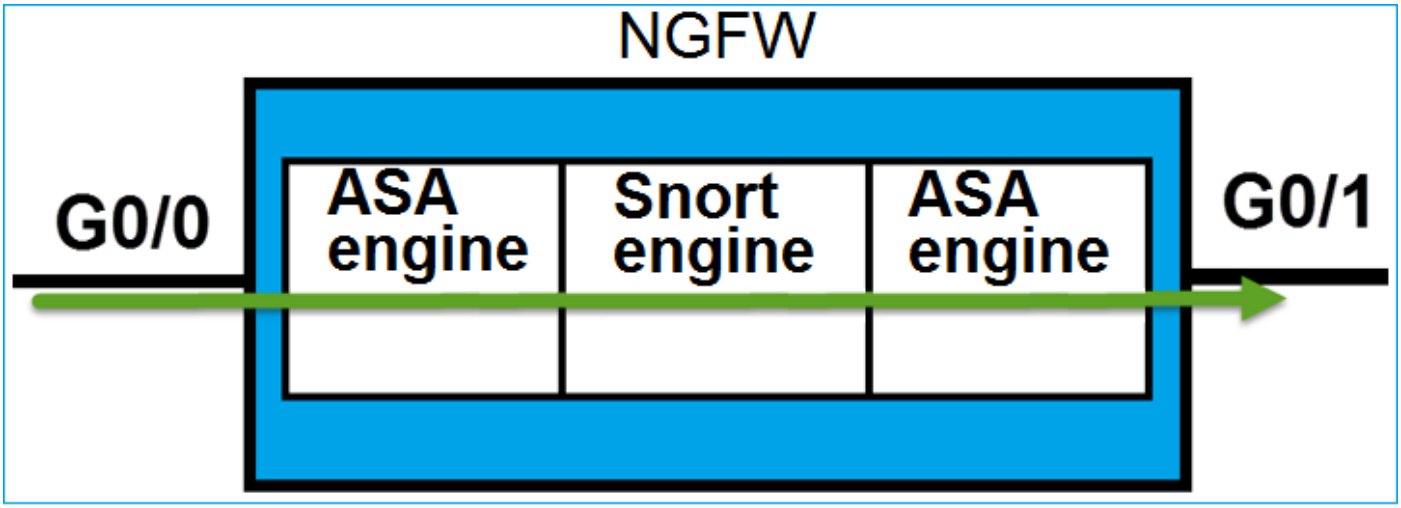
Puntos claves

- Los controles inferiores corresponden al trayecto de datos del motor FTD ASA
- 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 ASA** son aplicados junto con los controles **completos del motor del Snort**

La punta más reciente puede ser visualizada como sigue:



Localizar un paquete en la interfaz ruteada FTD

Topología

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

Interfaz de Entrada	DENTRO
Protocolo/servicio	Puerto TCP 80
IP de la fuente	192.168.201.100
IP de destino	192.168.202.100

Solución

Mientras que puede ser visto abajo, 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 ASA. Además, si la directiva del control de acceso dicta así pues, el paquete será examinado por el motor del Snort (uno de los casos del Snort)

donde un veredicto (lista negra, lista blanca) será alcanzado:

```
> 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 – 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
!
>
```

Documentos Relacionados

Guía de configuración de la defensa de la amenaza de la potencia de fuego de Cisco para el administrador de dispositivo de la potencia de fuego, versión 6.1

Instalando y actualizando la defensa de la amenaza de la potencia de fuego en los dispositivos ASA 55xx-X

Trabajo con las capturas y el Paquete-trazalíneas de la defensa de la amenaza de la potencia de fuego (FTD)