Configuración de interfaces de Firepower Threat Defence en modo enrutado

Contenido

Introducción

Este documento describe la configuración, verificación y operación de una interfaz de par en línea en un dispositivo Firepower Threat Defence (FTD).

Prerequisites

Requirements

No existen requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

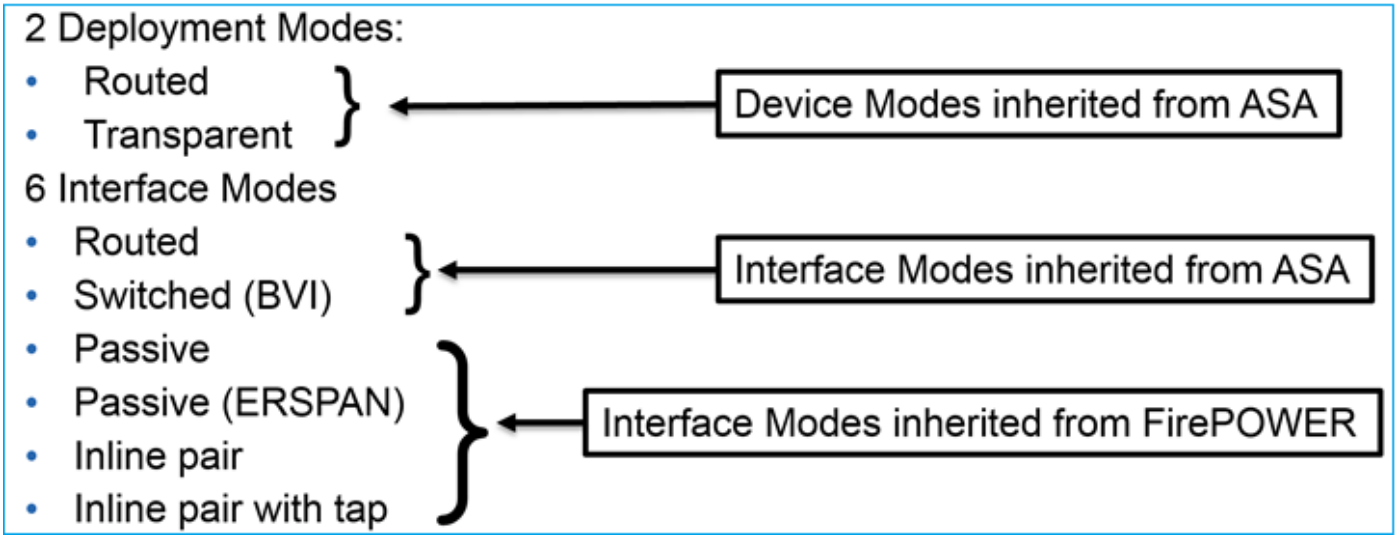
Productos Relacionados

Este documento también puede utilizarse 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 y FPR9300
- VMware (ESXi), Amazon Web Services (AWS), máquina virtual basada en kernel (KVM)
- Código de software FTD 6.2.x y posterior

Antecedentes

Firepower Threat Defence (FTD) proporciona dos modos de implementación y seis modos de interfaz, tal y como se muestra en esta imagen:



Nota: Puede mezclar modos de interfaz en un único dispositivo FTD.

Descripción general de alto nivel de los diversos modos de implementación e interfaz de FTD:

interfaz FTD	Modo de	Descripción	El tráfico se

modo	implementación de FTD		puede descartar
Enrutado	Enrutado	Comprobaciones completas del motor LINA y del motor Snort	Yes
Conmutado	Transparente	Comprobaciones completas del motor LINA y del motor Snort	Yes
Par lineal	Enrutado o transparente	Motor LINA parcial y comprobaciones completas del motor Snort	Yes
Par en línea con toque	Enrutado o transparente	Motor LINA parcial y comprobaciones completas del motor Snort	No
Pasivo	Enrutado o transparente	Motor LINA parcial y comprobaciones completas del motor Snort	No
Pasivo (ERSPAN)	Enrutado	Motor LINA parcial y comprobaciones completas del motor Snort	No

Configurar

Diagrama de la red

Configurar una interfaz enrutada y una subinterfaz

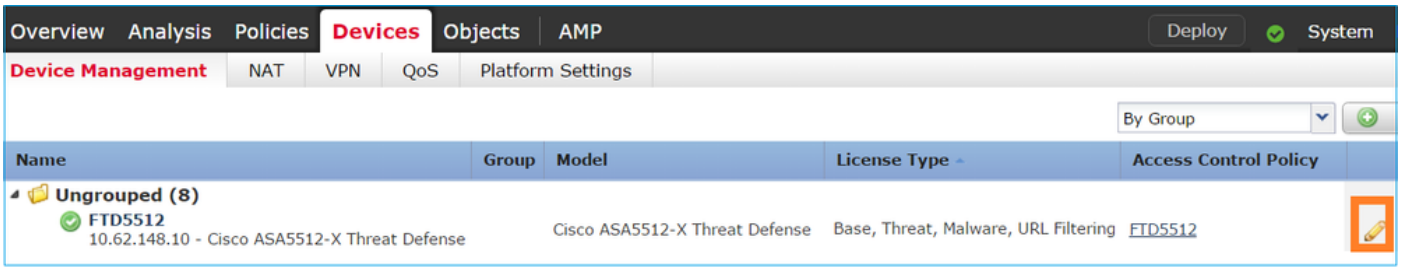
Configure la subinterfaz G0/0.201 y la interfaz G0/1 según estos requisitos:

Interfaz	G0/0,201	G0/1
Nombre	DENTRO	FUERA
Zona de seguridad	INSIDE_ZONE	OUTSIDE_ZONE
Descripción	INTERNO	EXTERNO
ID de subinterfaz	201	-
ID DE VLAN	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
Dúplex/Velocidad	Auto	Auto

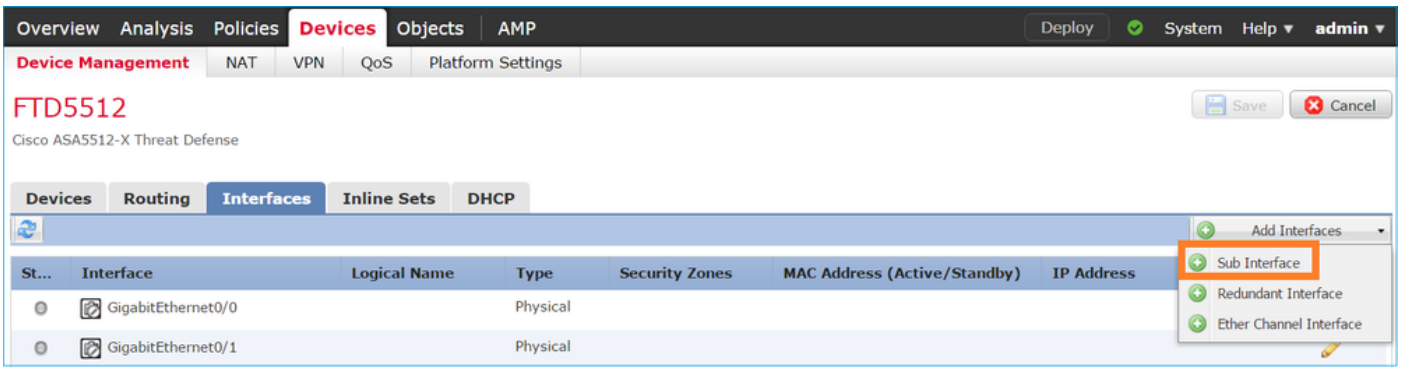
Solución

Paso 1. Configuración de la interfaz lógica

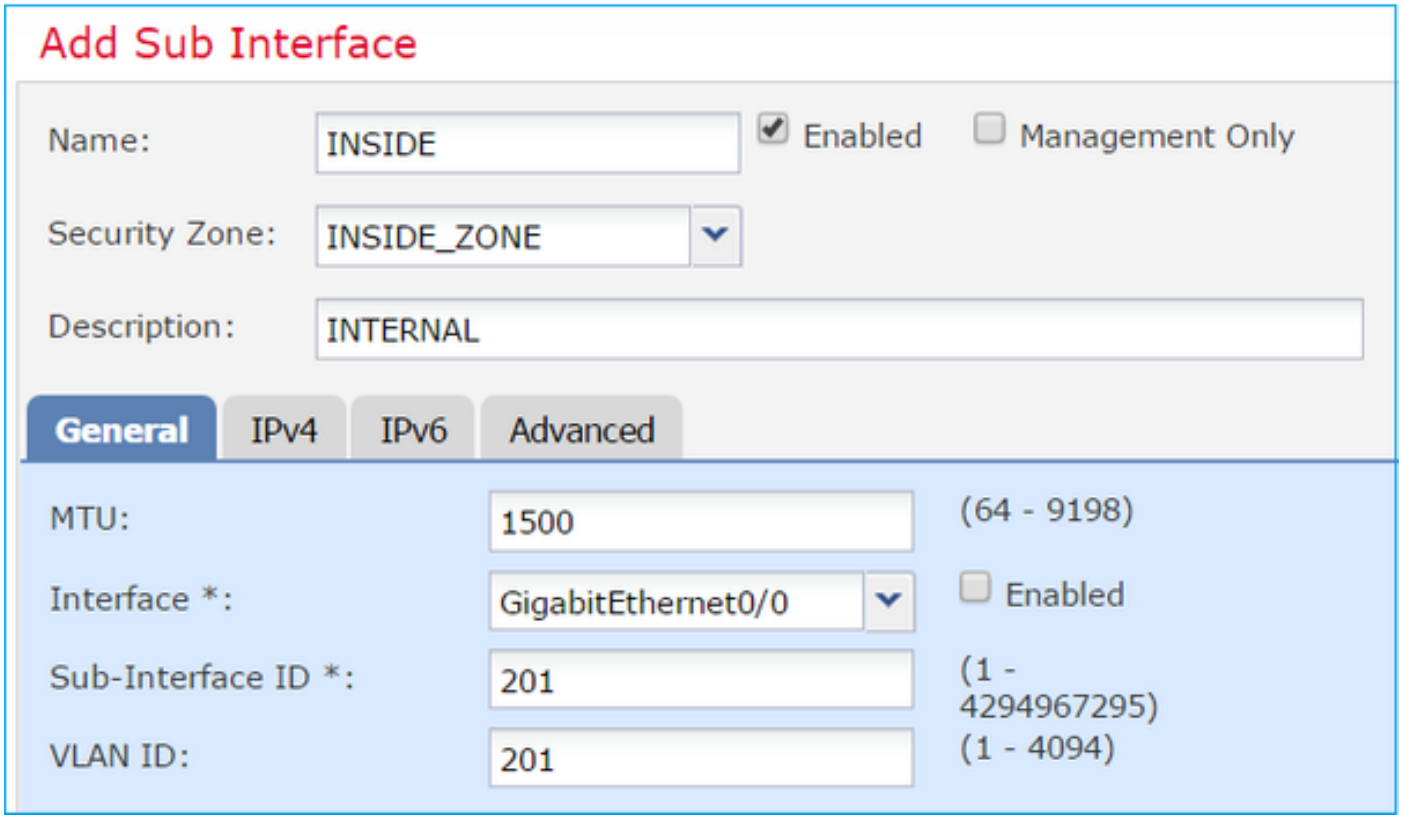
Vaya a Devices > Device Management, seleccione el dispositivo apropiado y seleccione el icono Edit:



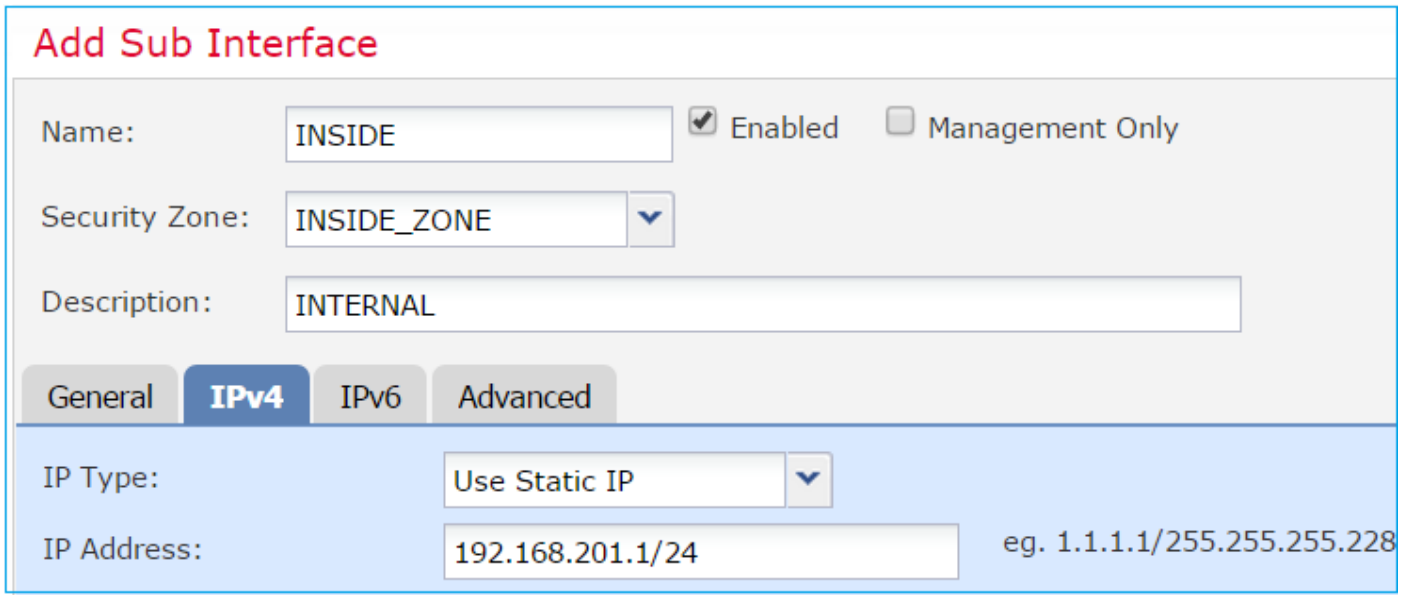
Seleccione Add Interfaces > Sub Interface:



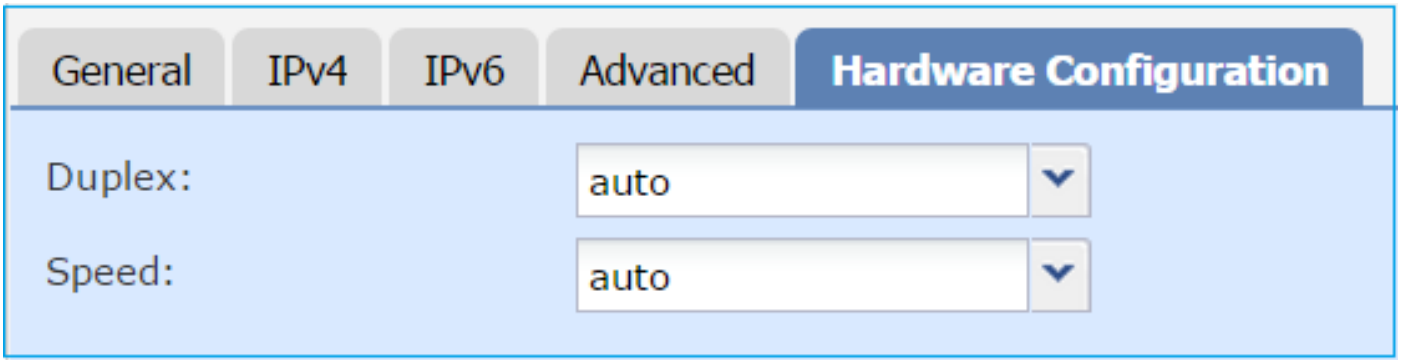
Configure las opciones de la subinterfaz según los requisitos:



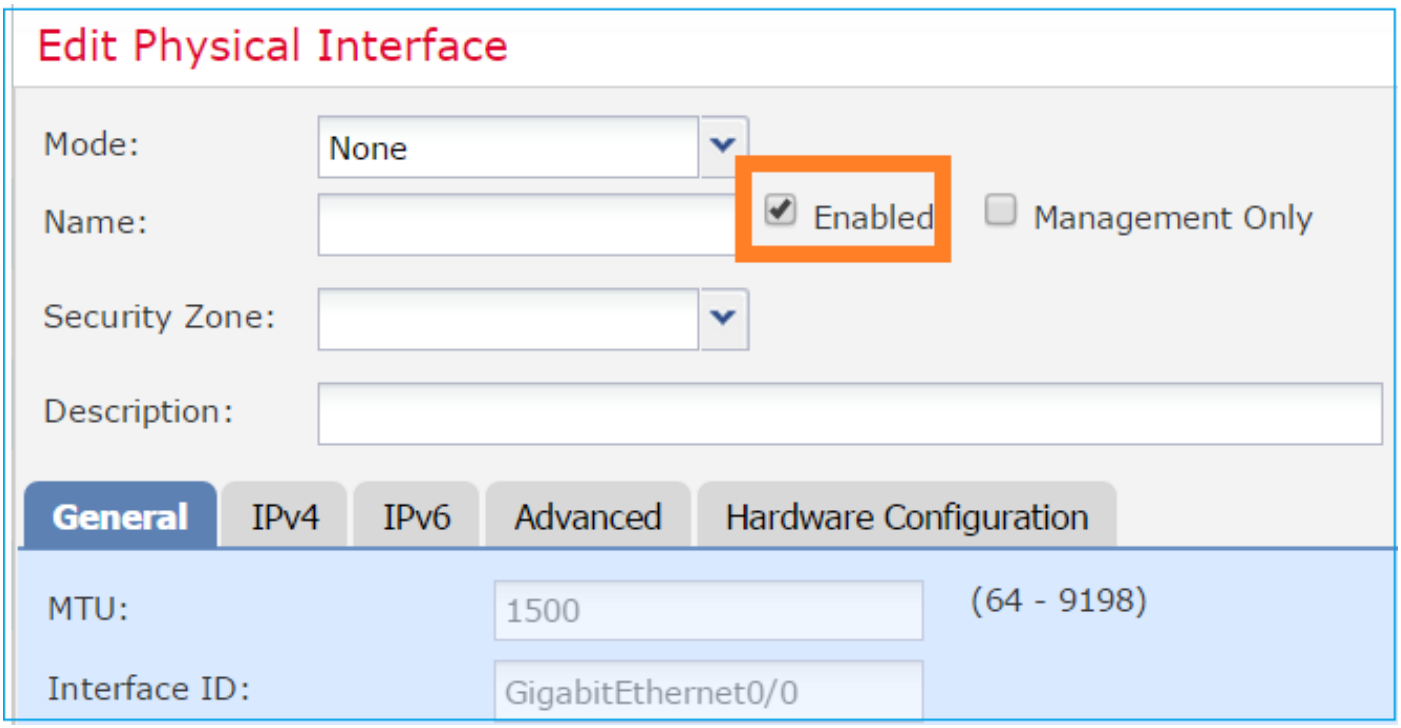
Configuración de IP de interfaz:



En la interfaz física (GigabitEthernet0/0), especifique la configuración de dúplex y velocidad:

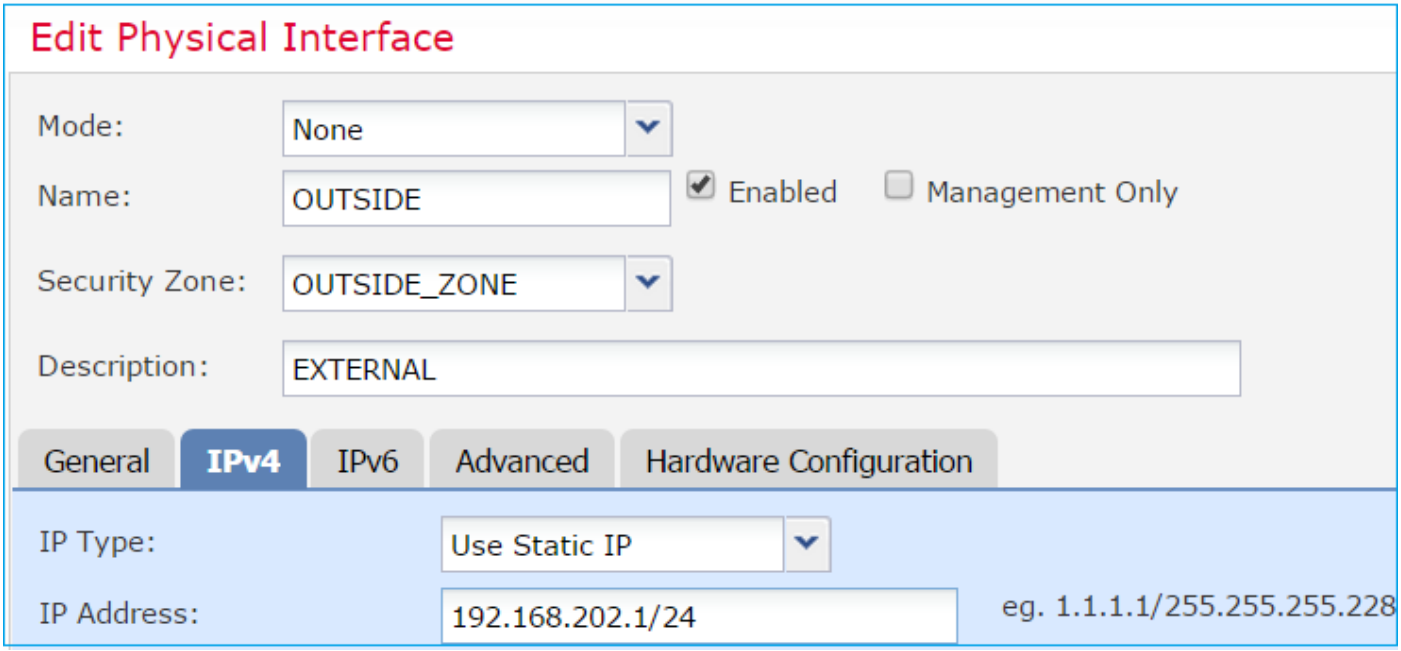


Habilite la interfaz física (G0/0 en este caso):



Paso 2. Configuración de la interfaz física

Edite la interfaz física GigabitEthernet0/1 según los requisitos:

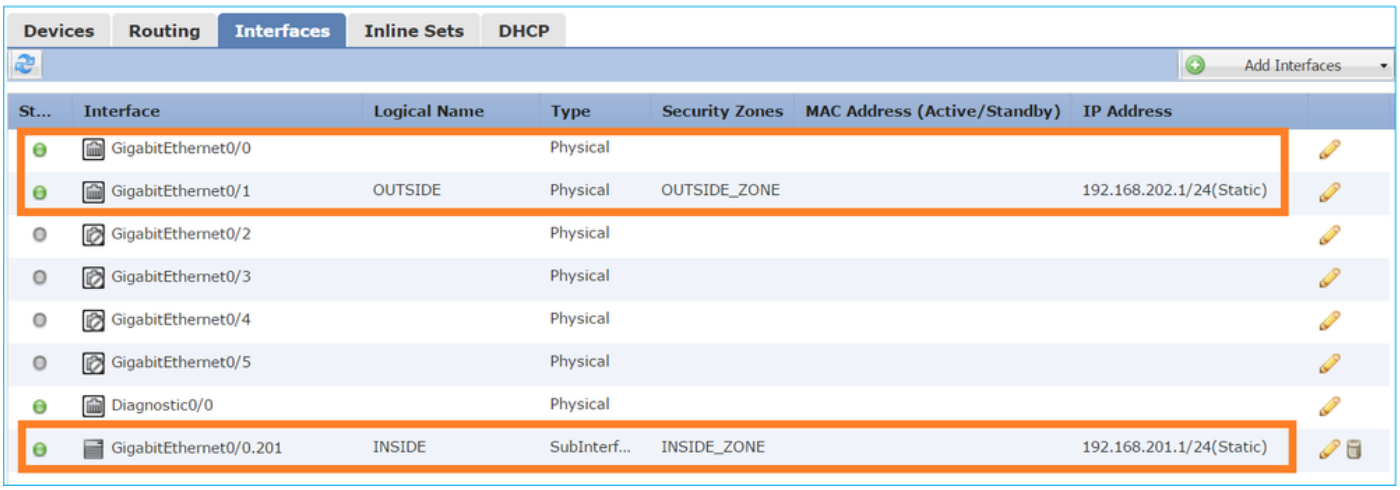


- Para la interfaz ruteada, el modo es: Ninguno
- El nombre es equivalente al nombre de la interfaz ASA si
- En FTD, todas las interfaces tienen un nivel de seguridad = 0
- same-security-traffic no es aplicable en FTD. El tráfico entre interfaces FTD (inter) e (intra) está permitido de forma predeterminada

Seleccione Guardar e implementar.

Verificación

Desde la GUI de FMC:



Desde la CLI de 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>

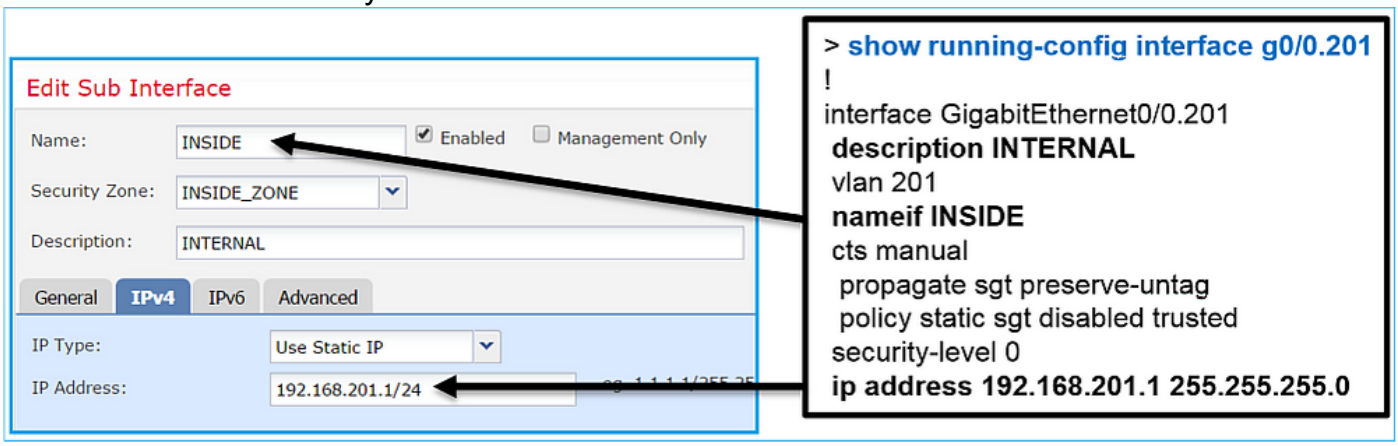
>

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
```

Correlación de FMC GUI y FTD CLI:



<#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
>
```

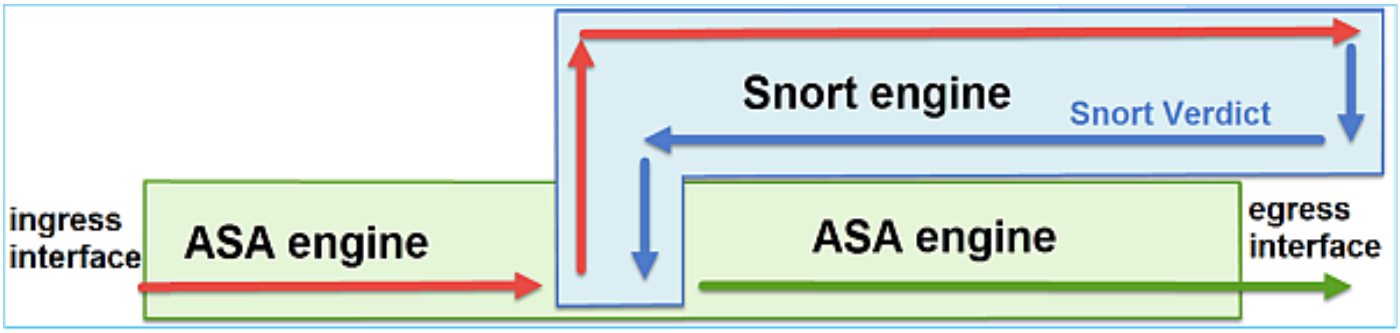
Operación de Interfaz Ruteada FTD

Verifique el flujo de paquetes FTD cuando las interfaces enrutadas están en uso.

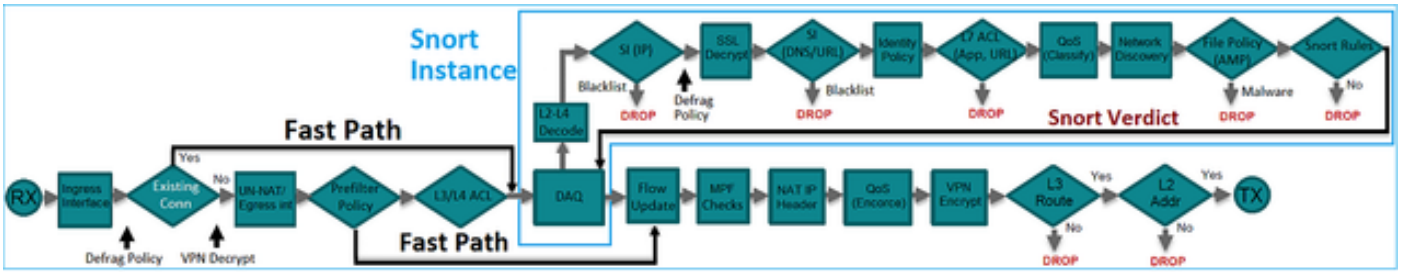
Solución

Descripción general de arquitectura de FTD

Una descripción general de alto nivel del plano de datos del FTD:



Esta imagen muestra algunas de las comprobaciones que se producen dentro de cada motor:



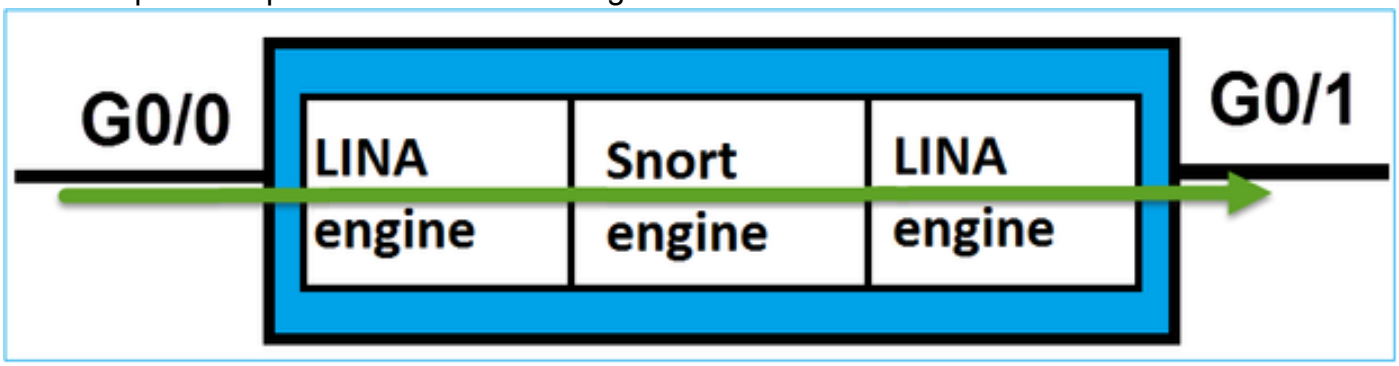
Puntos clave

- Las comprobaciones inferiores corresponden a la ruta de datos del motor FTD LINA
- Las comprobaciones del cuadro azul corresponden a la instancia del motor Snort de FTD

Descripción General de la Interfaz Ruteada FTD

- Disponible sólo en implementación enrutada
- Implementación tradicional de firewall de capa 3
- Una o más interfaces enrutables físicas o lógicas (VLAN)
- Permite configurar funciones como los protocolos NAT o de enrutamiento dinámico
- Los paquetes se reenvían en función de la búsqueda de ruta y el salto siguiente se resuelve en función de la búsqueda ARP
- Tráfico real se puede descartar
- Se realizan comprobaciones completas del motor LINA junto con comprobaciones completas del motor Snort

El último punto se puede visualizar de la siguiente manera:



Verificación

Seguimiento de un Paquete en la Interfaz Ruteada FTD

Diagrama de la red

Utilice packet-tracer con estos parámetros para ver las políticas aplicadas:

Interfaz de	DENTRO

Entrada	
Protocolo/Servicio	Puerto TCP 80
IP de origen	192.168.201.100
IP de destino	192.168.202.100

Solución

Cuando se utiliza una interfaz ruteada, el paquete se procesa de manera similar a una interfaz ruteada clásica de ASA. Las comprobaciones como la búsqueda de rutas, el marco de políticas modulares (MPF), NAT, la búsqueda ARP, etc., se realizan en la ruta de datos del motor LINA. Además, si la política de control de acceso así lo requiere, el paquete es inspeccionado por el motor Snort (una de las instancias de Snort), donde se genera un veredicto y se devuelve al motor 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

>
```

Nota: En la fase 4, el paquete se compara con un mapa TCP llamado UM_STATIC_TCP_MAP. Éste es el mapa TCP predeterminado en 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
!
>
```

Información Relacionada

- Guía de configuración de Cisco Firepower Threat Defense para Firepower Device Manager, versión 6.1
- Instalación y actualización de Firepower Threat Defense en dispositivos ASA 55xx-X
- Cisco Secure Firewall Threat Defence
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).