Configuración de PBR con HTTP Path Monitor en FMC

Contenido

Introducción

En este documento se describe cómo configurar el routing basado en políticas (PBR) con la supervisión de rutas HTTP en Cisco Secure Firewall Management Center (FMC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- conocimientos básicos de PBR
- Experiencia básica de Cisco Secure Management Center
- Protección básica frente a amenazas con firewall seguro de Cisco (FTD)

Componentes Utilizados

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

- Cisco Secure Firewall Management Center Virtual (FMCv) VMware con versión 7.4

- Appliance virtual Cisco Secure Firewall Threat Defence (FTDv) VMware con versión 7.4

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.

Antecedentes

En el ruteo tradicional, los paquetes se rutean según la dirección IP de destino; sin embargo, es difícil cambiar el ruteo de la especificación del tráfico en un sistema de ruteo basado en el destino. PBR le brinda más control sobre el ruteo al extender y complementar los mecanismos existentes provistos por los protocolos de ruteo.

PBR permite establecer la precedencia IP. También permite especificar una trayectoria para cierto tráfico, como el tráfico prioritario sobre un link de alto costo. Con PBR, el enrutamiento se basa en criterios distintos de la red de destino, como el puerto de origen, la dirección de destino, el puerto de destino, las aplicaciones de protocolo o una combinación de estos objetos. PBR se puede utilizar para clasificar el tráfico de red en función de la aplicación, el nombre de usuario, la pertenencia al grupo y la asociación al grupo de seguridad. Este método de routing es aplicable en situaciones en las que numerosos dispositivos acceden a aplicaciones y datos en una implementación de red de gran tamaño. Tradicionalmente, las grandes implementaciones tienen topologías que reenvían todo el tráfico de red a un hub como tráfico cifrado en una VPN basada en routing. Estas topologías suelen dar lugar a problemas como la latencia de paquetes, la reducción del ancho de banda y la pérdida de paquetes.

PBR se soporta solamente en el modo de firewall ruteado y no se aplica para las conexiones Embryonic. La aplicación basada en HTTP es compatible con interfaces físicas, de canal de puerto, subinterfaces y de túnel de estado. No es compatible con dispositivos de clúster.

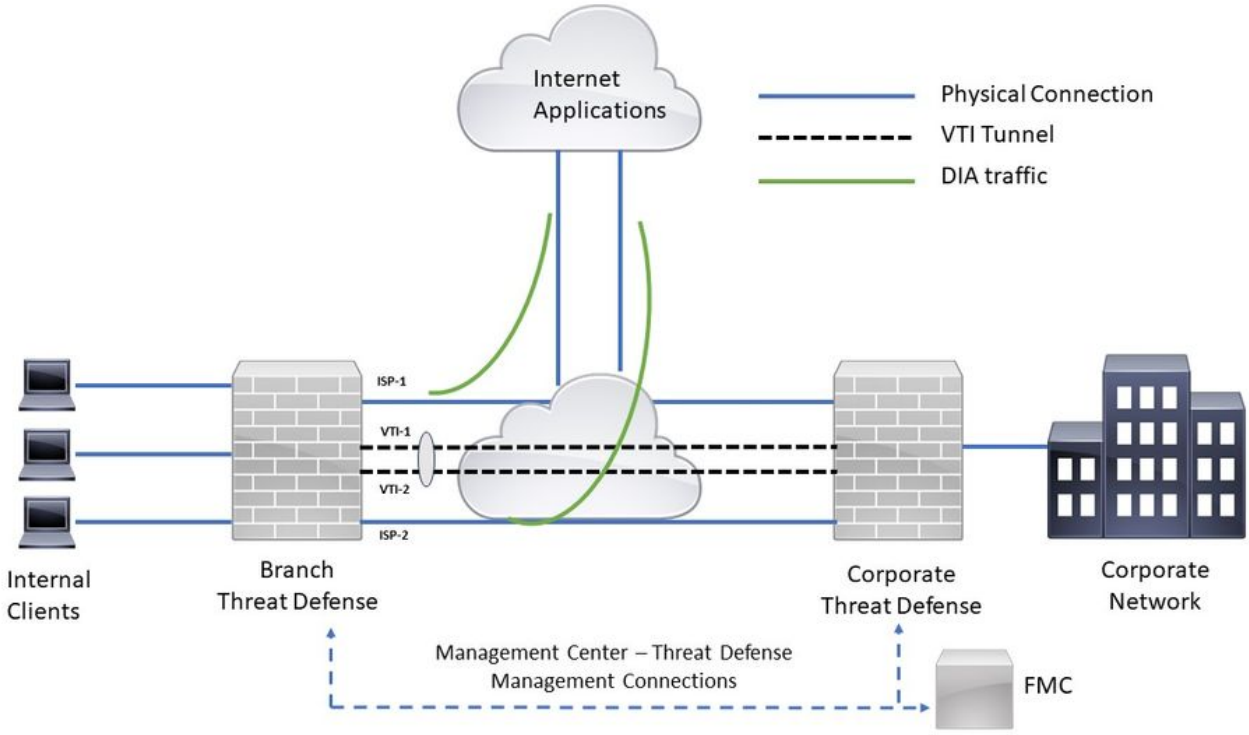
Cuando las interfaces configuradas derivan métricas como el tiempo de ida y vuelta (RTT), la fluctuación, la puntuación de opinión media (MOS) y la pérdida de paquetes por interfaz, se utilizan para determinar la mejor trayectoria para el ruteo del tráfico PBR. La supervisión de rutas calcula métricas flexibles para varios peers remotos por interfaz. Para monitorear y determinar la mejor trayectoria para varias aplicaciones a través de una política en un firewall de sucursal, HTTP es preferido sobre ICMP por estas razones:

- El ping HTTP puede derivar las métricas de rendimiento de la ruta hasta la capa de aplicación del servidor, donde se aloja la aplicación.
- Se elimina la necesidad de cambiar la configuración del firewall cada vez que se cambia la dirección IP del servidor de aplicaciones, ya que se realiza un seguimiento del dominio de aplicación en lugar de la dirección IP.

Configurar

Diagrama de la red

Considere un escenario típico de la red corporativa en el que todo el tráfico de la red de la sucursal se envía a través de una VPN basada en ruta de la red corporativa y se desvía a la extranet cuando es necesario. La siguiente topología muestra una red de sucursal conectada a la red corporativa a través de una VPN basada en ruta. Tradicionalmente, la defensa frente a amenazas corporativas se configuraba para gestionar el tráfico interno y externo de la sucursal. Con la política PBR, la defensa contra amenazas de la sucursal se configura con una política que enruta el tráfico específico a la red WAN en lugar de los túneles virtuales. El resto del tráfico fluye a través de la VPN basada en rutas, como de costumbre.



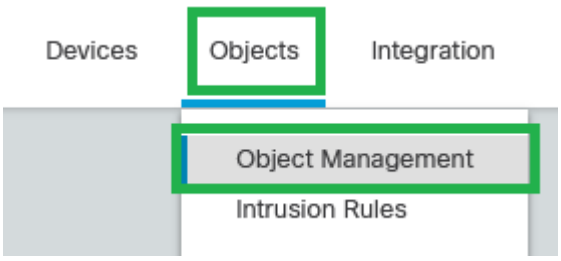
Topología de red

La sección configure asume que las interfaces ISP y VTI ya están configuradas para la defensa contra amenazas de sucursal en el FMC seguro.

Configuración de PBR para el Monitoreo de Trayectoria HTTP

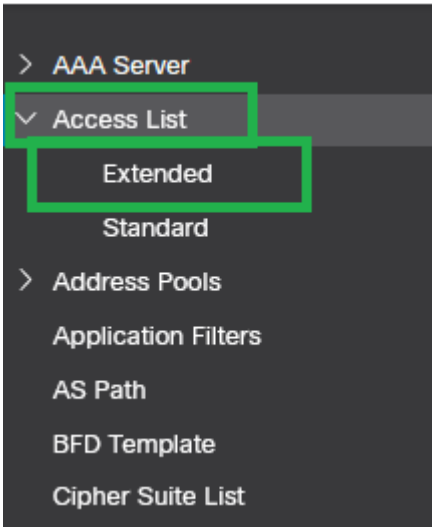
Esta sección de configuración muestra la configuración de Path Monitoring en las interfaces ISP-1 e ISP-2.

Paso 1. Crear una lista de acceso ampliada para aplicaciones supervisadas. Vaya a .Objects > Object Management



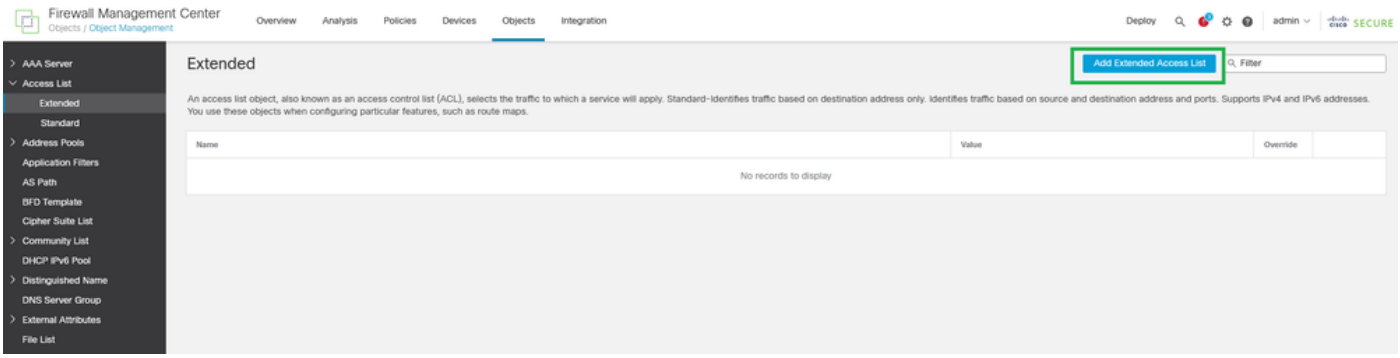
Objetos - Gestión de objetos

Paso 2. Desplácese hasta Access-list > Extended en el menú de la izquierda.



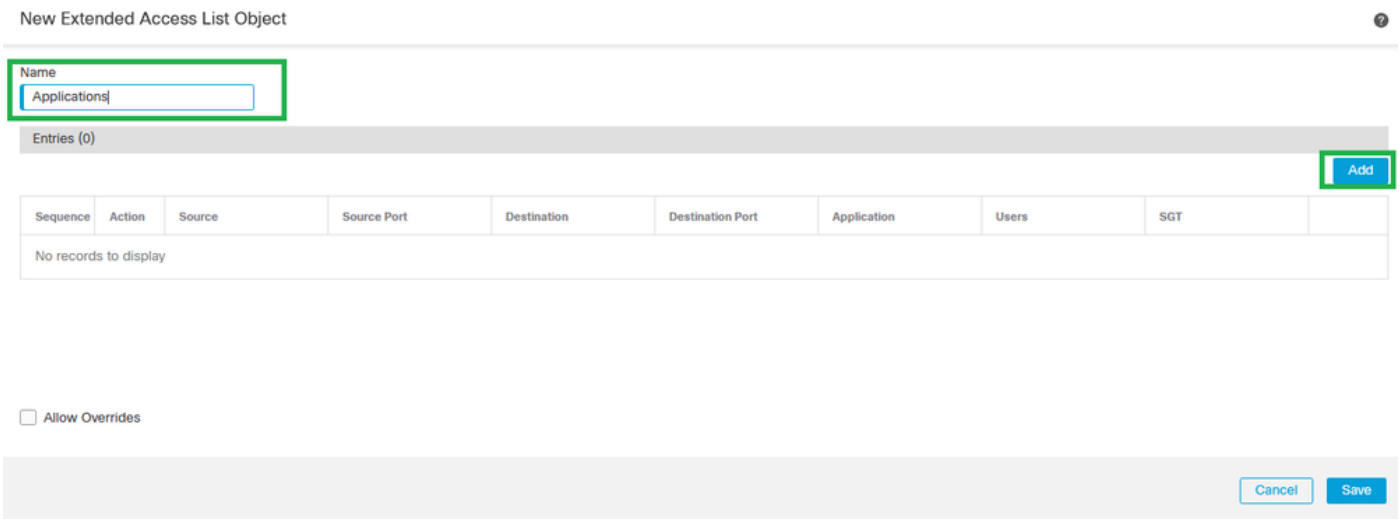
Lista de acceso - Ampliada

Paso 3. Haga clic en Add Extended Access List



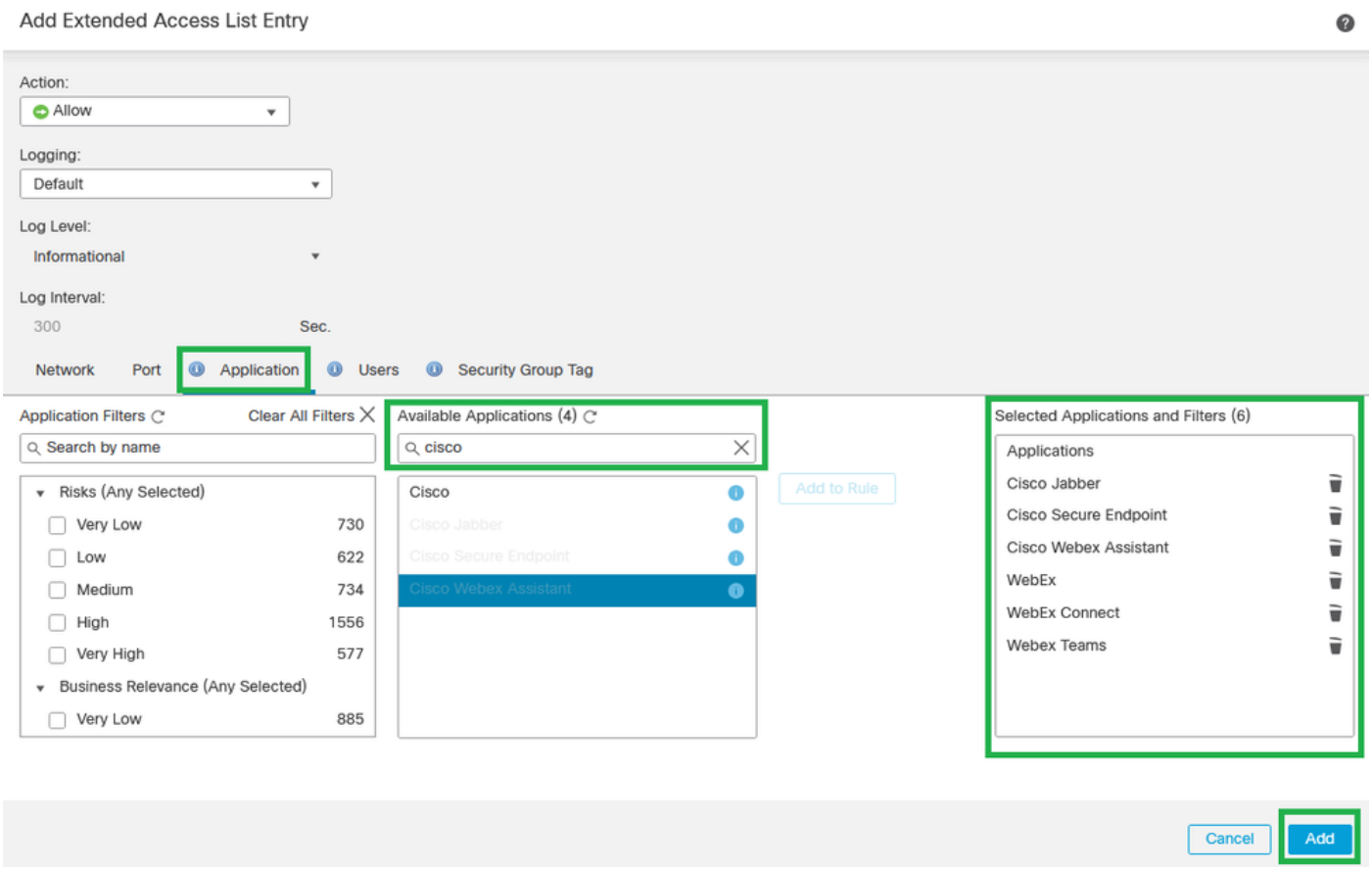
Agregar lista de acceso ampliada

Paso 4. Configure un nombre en la lista de acceso extendido y haga clic en Add.



Nuevo objeto de lista de acceso extendido

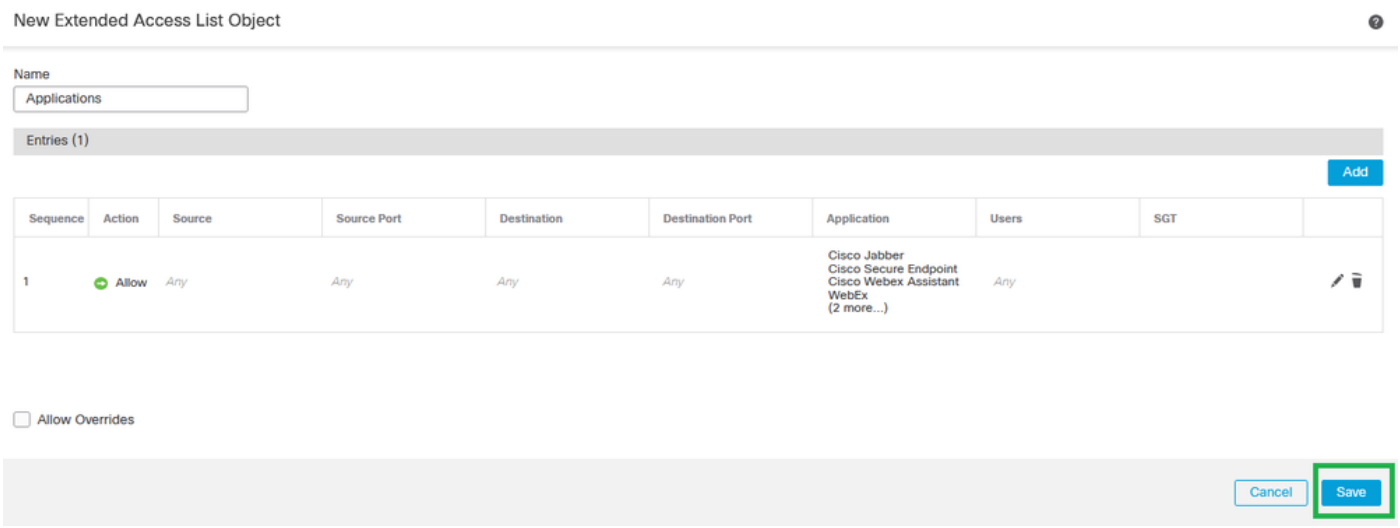
Paso 5. Haga clic Application y seleccione las aplicaciones deseadas (se han seleccionado algunas aplicaciones de Cisco para este ejemplo). A continuación, haga clic en Add.



Agregar entrada de lista de acceso extendido

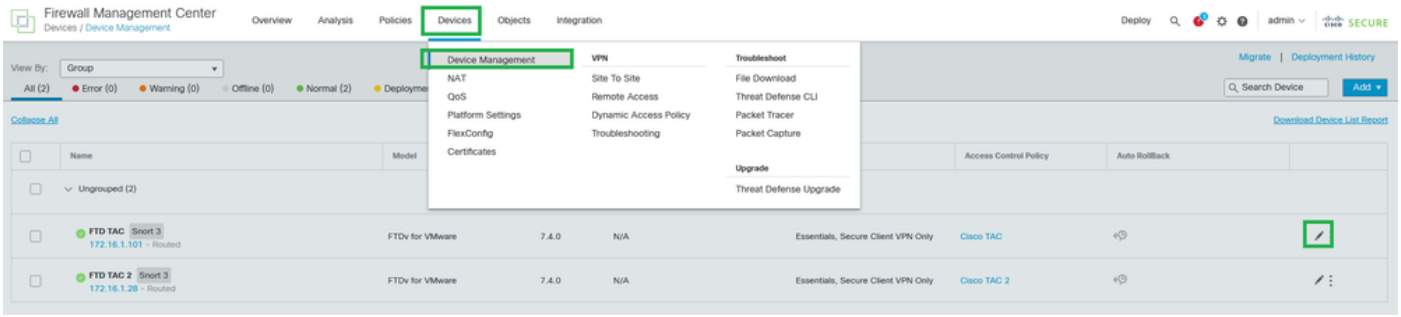
Nota: La lista de acceso ampliada se puede configurar con las IP y los puertos de origen/destino para hacer coincidir el tráfico específico con las aplicaciones deseadas. Puede crear varias listas de control de acceso extendido para aplicarlas a la configuración PBR.

Paso 6. Valide la configuración de la lista de acceso ampliada y haga clic en Save.



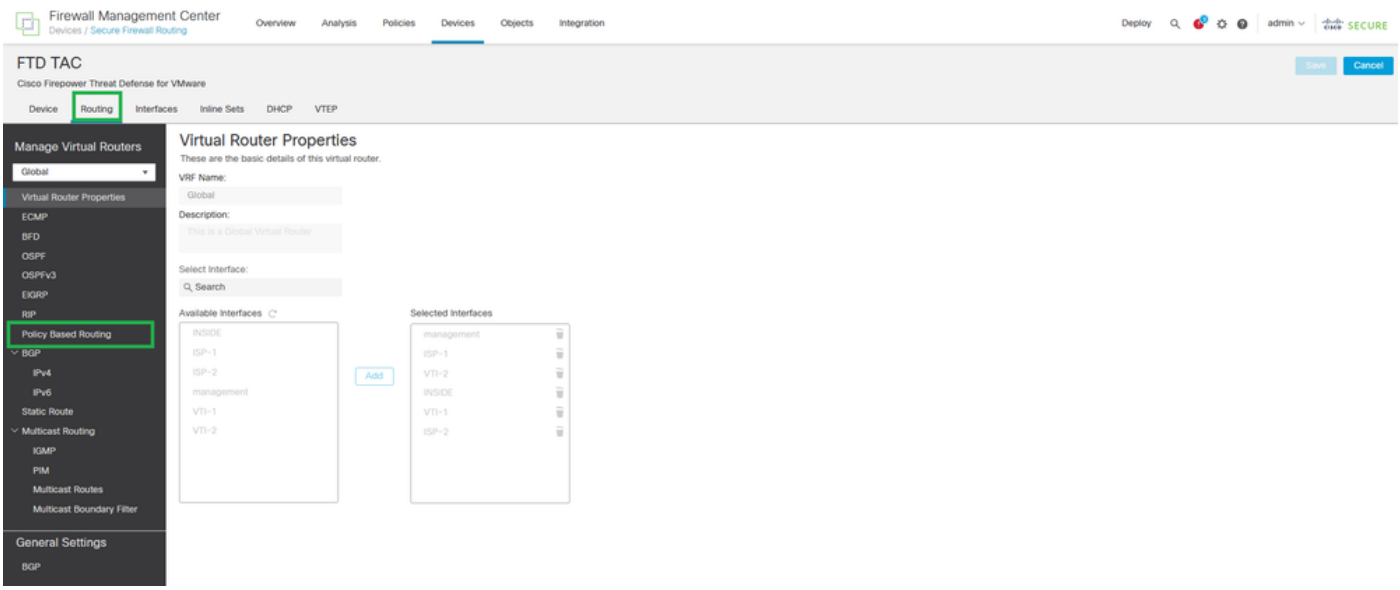
Guardar objeto de lista de acceso extendido

Paso 7. Desplácese hasta Devices > Device Managementla defensa contra amenazas y edítela.



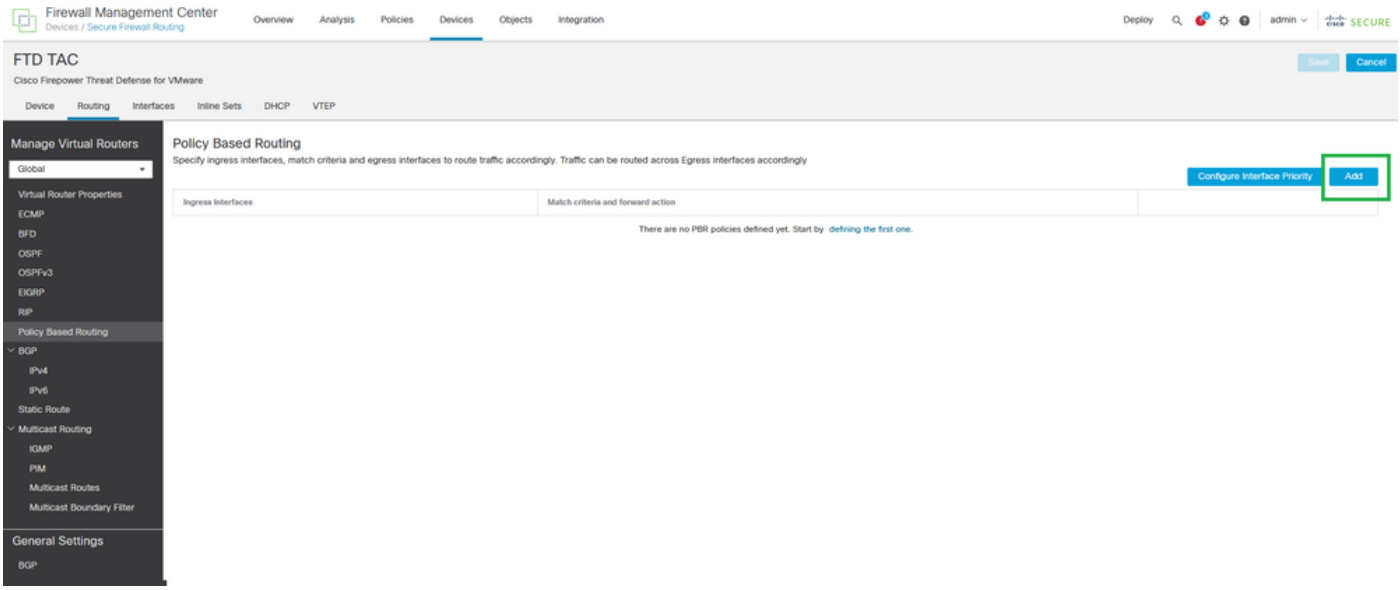
Dispositivo - Gestión de dispositivos

Paso 8. Acceda a Routing > Policy-Based Routing.



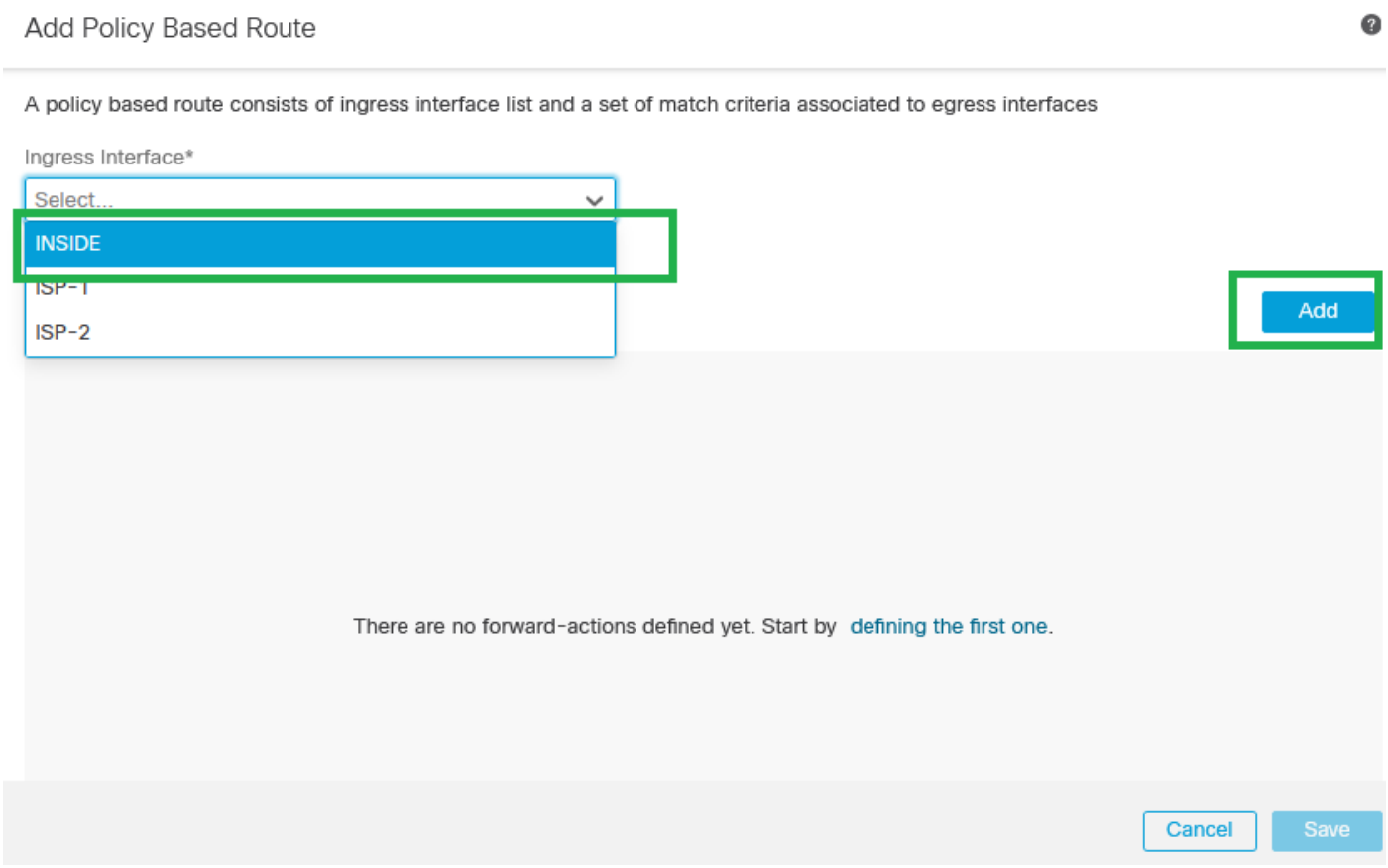
Routing: Routing basado en políticas

Paso 9. Haga clic en Add



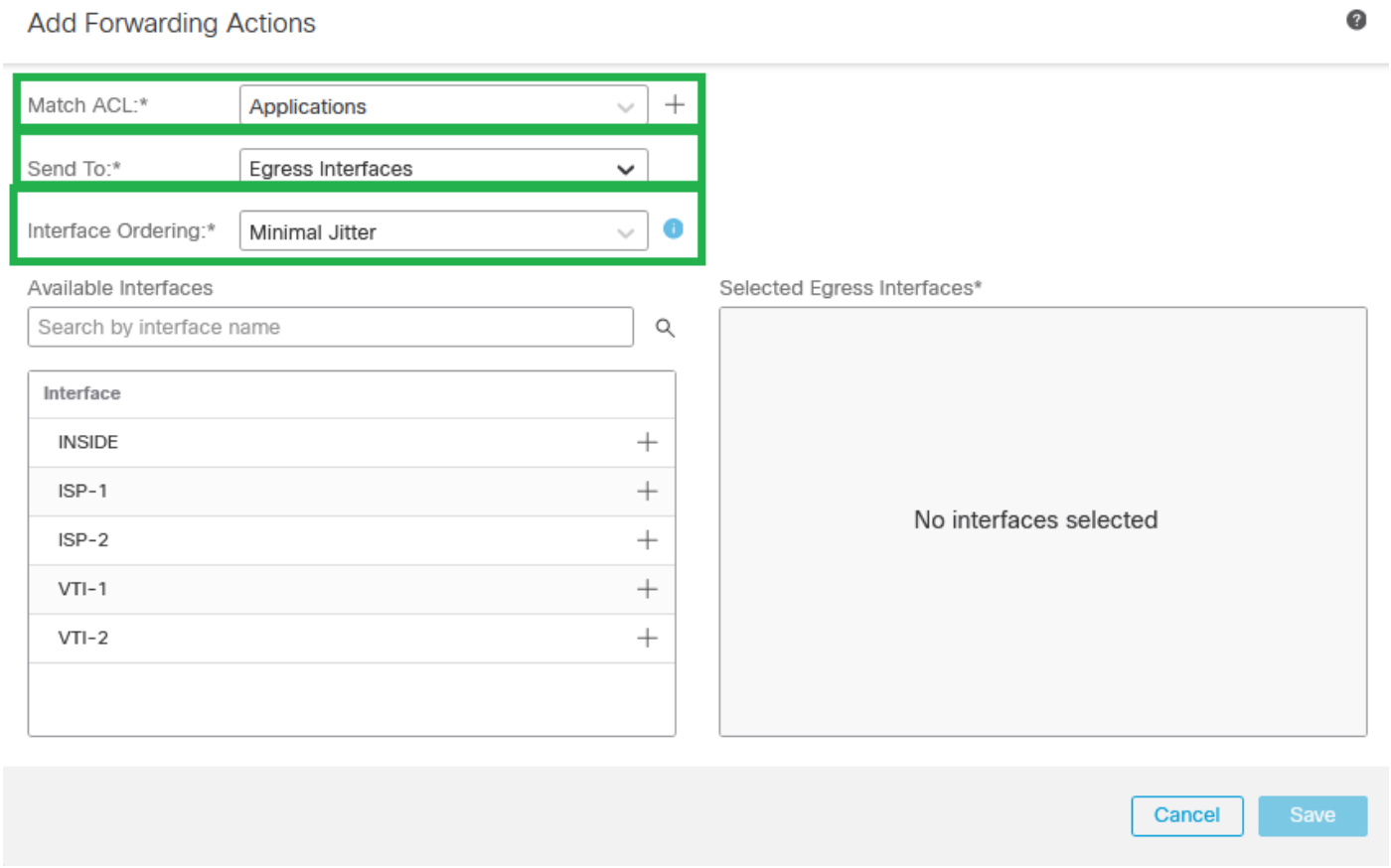
Agregar routing basado en políticas

Paso 10. Agregue la interfaz de ingreso para la configuración PBR (INSIDE en este ejemplo), luego haga clic en Add.



Agregar ruta basada en políticas

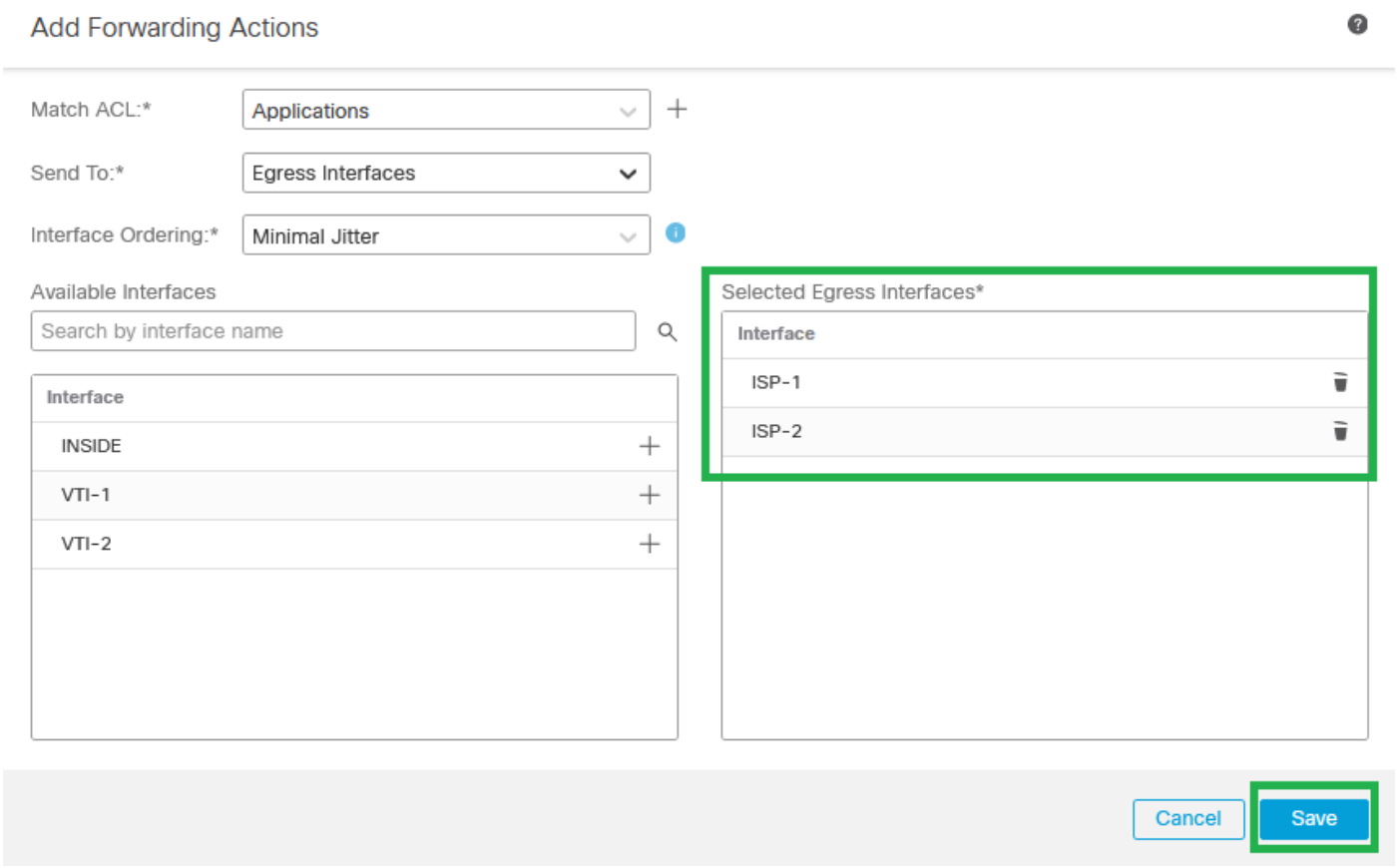
Paso 11. Defina los criterios de coincidencia (con la lista de acceso ampliada creada en los pasos anteriores), las interfaces de salida y la ordenación de interfaces.



Agregar acciones de reenvío

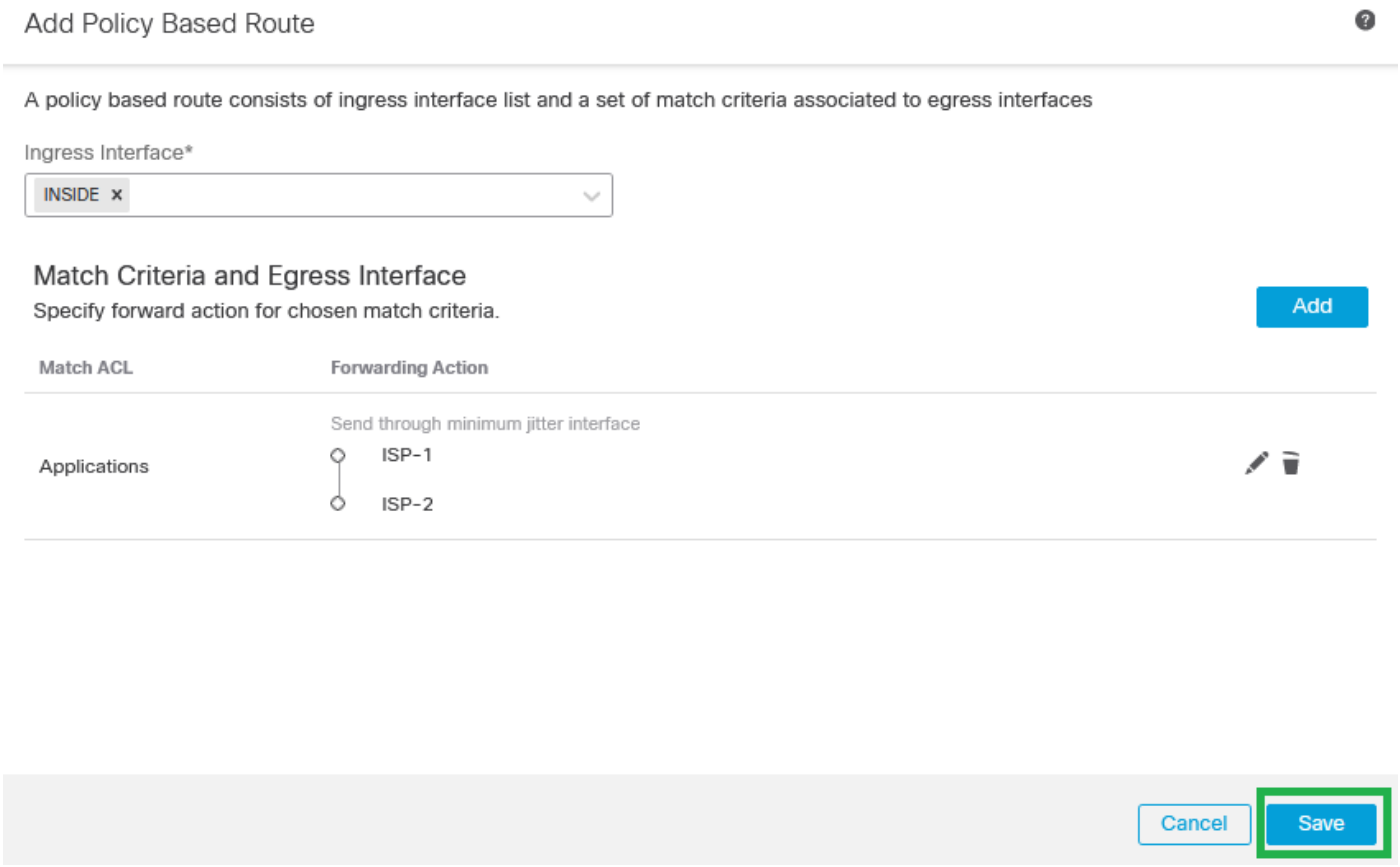
Nota: Egress Interfaces y Minimal Jitter se eligieron para esta guía de configuración. Consulte la documentación oficial de PBR para obtener más información sobre las otras opciones.

Paso 12. Elija las interfaces de salida (ISP-1 e ISP-2 para este ejemplo) y, a continuación, haga clic en Save.



Interfaces de salida seleccionadas

Paso 13. Valide la configuración PBR y haga clic en Save.



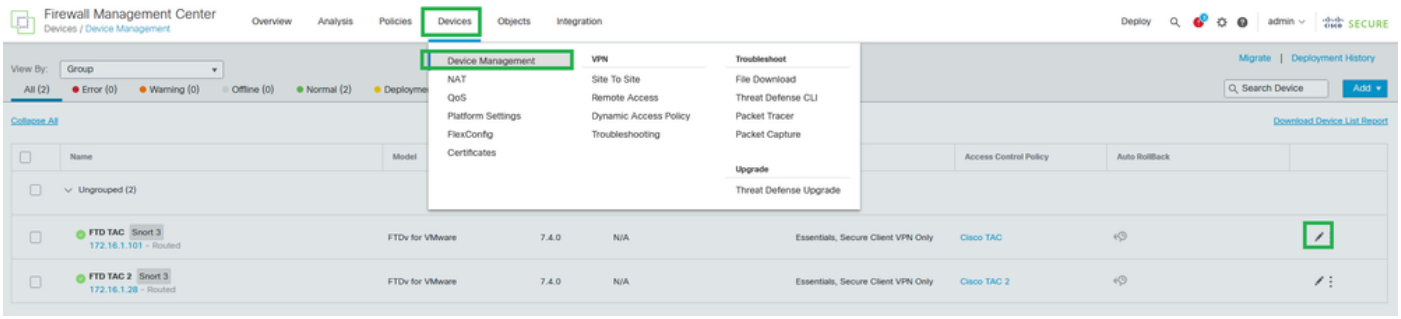
Validación de Ruteo Basada en Políticas

Paso 14. (Opcional) Repita los pasos 9, 10, 11, 12 y 13 si se crearon más listas de control de acceso extendido o si hay más interfaces de origen en las que se debe aplicar la configuración PBR.

Paso 15. Guarde e implemente los cambios de FMC.

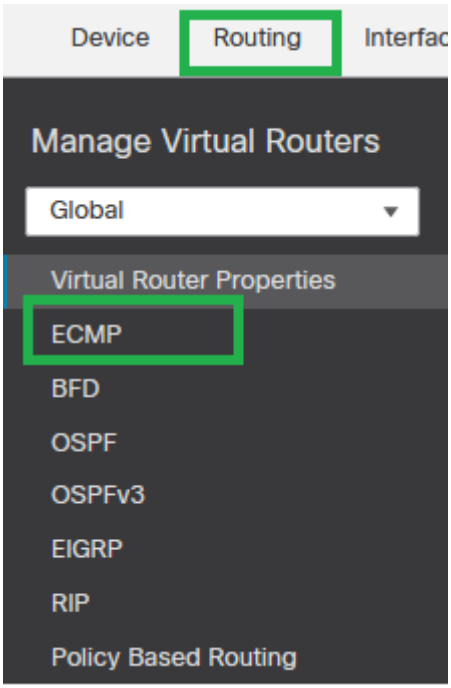
Configuración de ECMP (Equal-cost-multi-path)

Paso 1. Desplácese hasta Devices > Device Managementy edite la defensa contra amenazas.



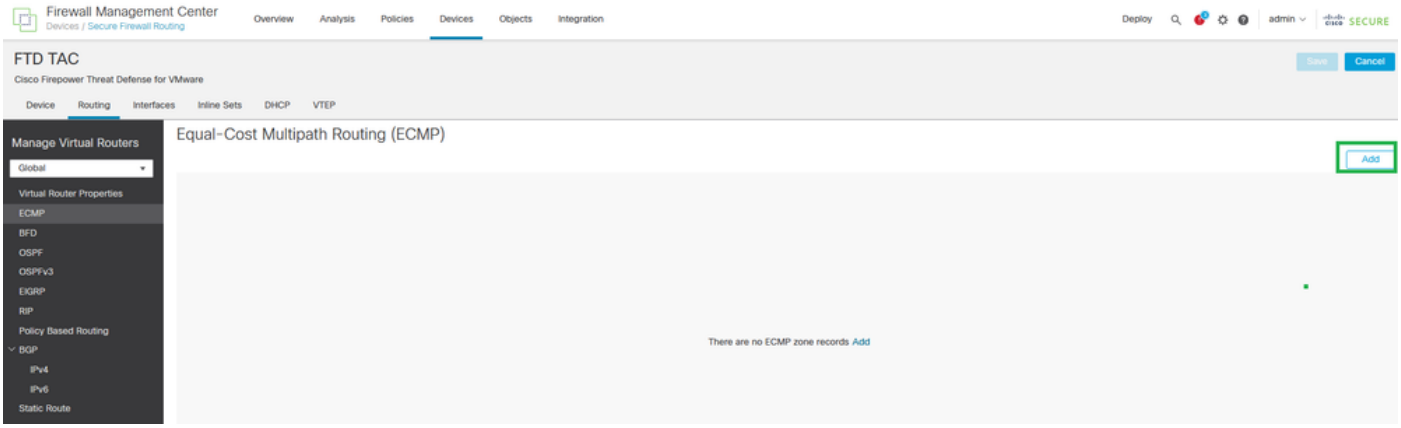
Dispositivo - Gestión de dispositivos

Paso 2. Desplácese hasta Routing > ECMP.



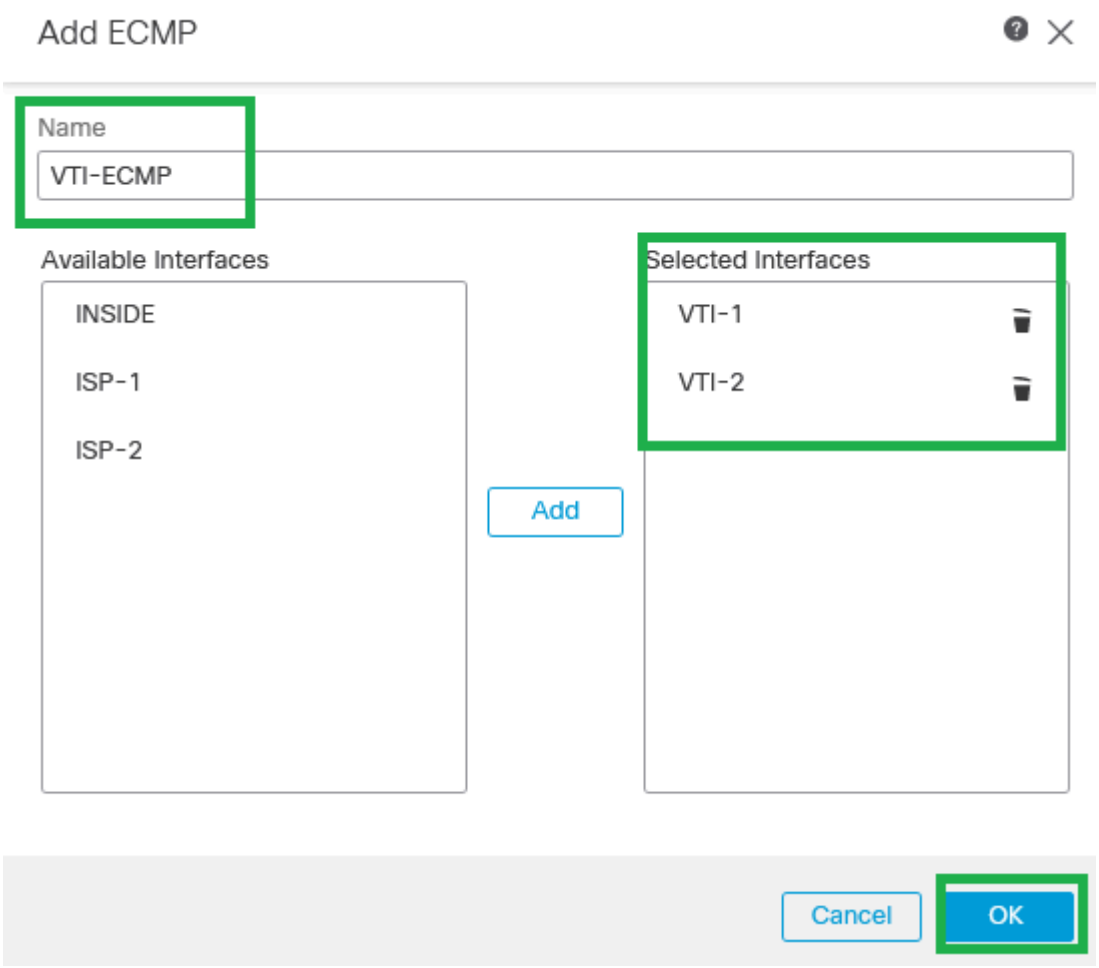
Routing - ECMP

Paso 3. Haga clic Add para crear ECMP entre las interfaces VTI y WAN (ISP-1 e ISP-2 para esta guía de configuración).



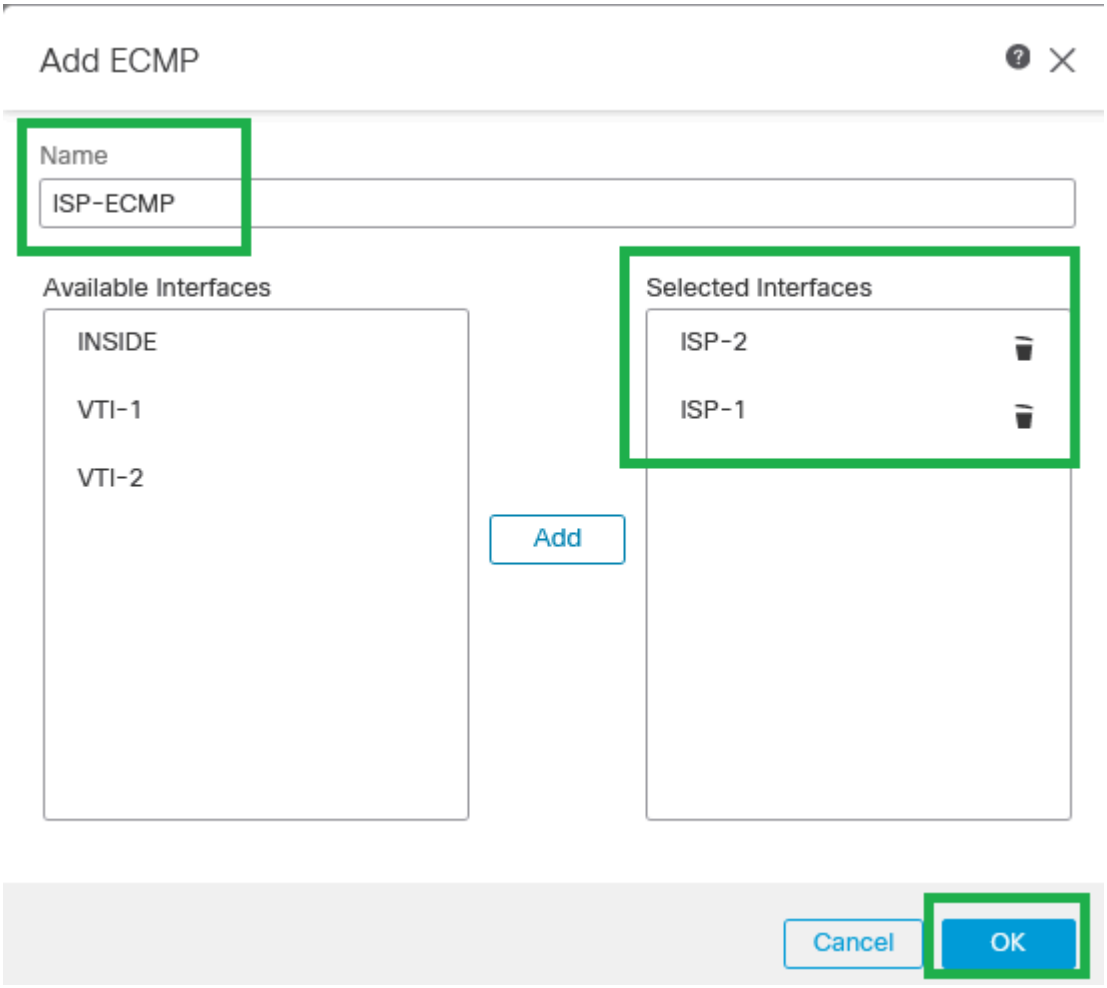
Routing de múltiples rutas de igual coste (ECMP)

Paso 4. Configure el nombre ECMP y elija todas las interfaces VTIs, luego haga clic en Add.



ECMP para VTI

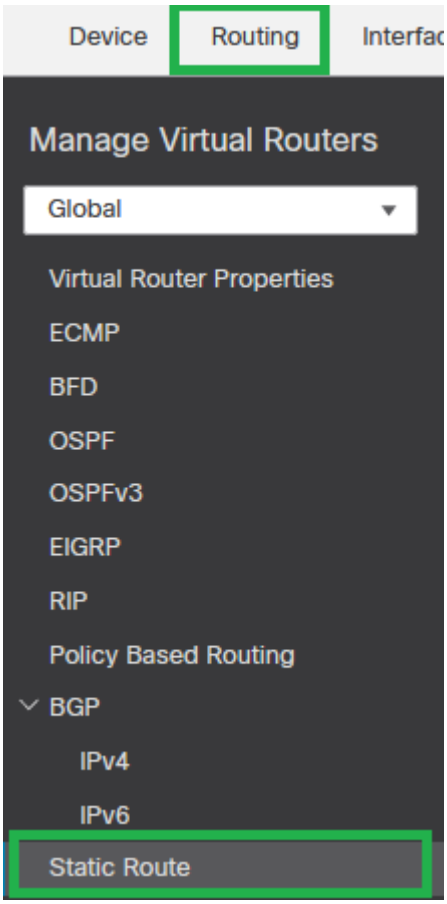
Paso 5. Repita los pasos 3 y 4 para crear ECMP entre interfaces WAN (ISP-1 e ISP-2 para esta guía de configuración).



ECMP para interfaces ISP

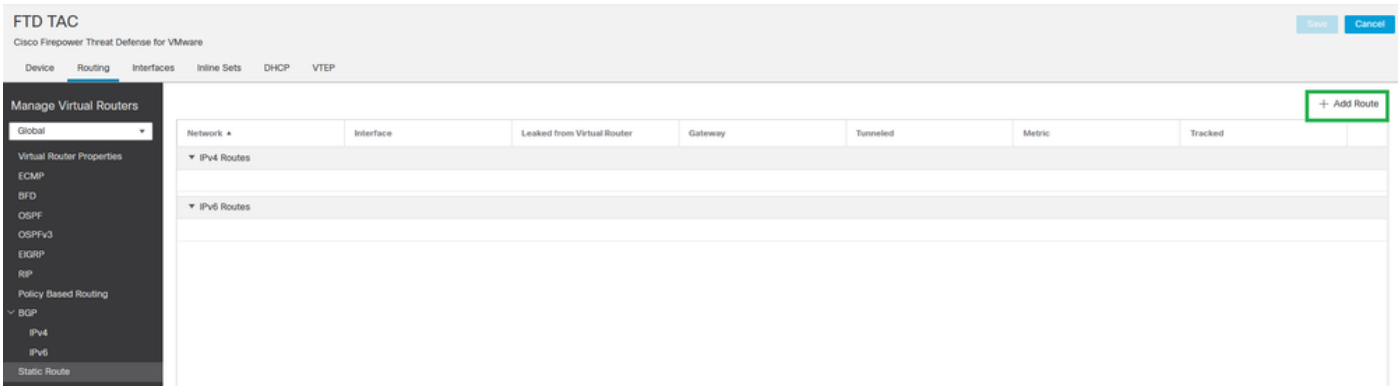
Paso 6. Guarde la configuración de ECMP.

Paso 7. Configure las Rutas Estáticas para las interfaces de zona para equilibrar la carga. Vaya a Routing > Static Route.



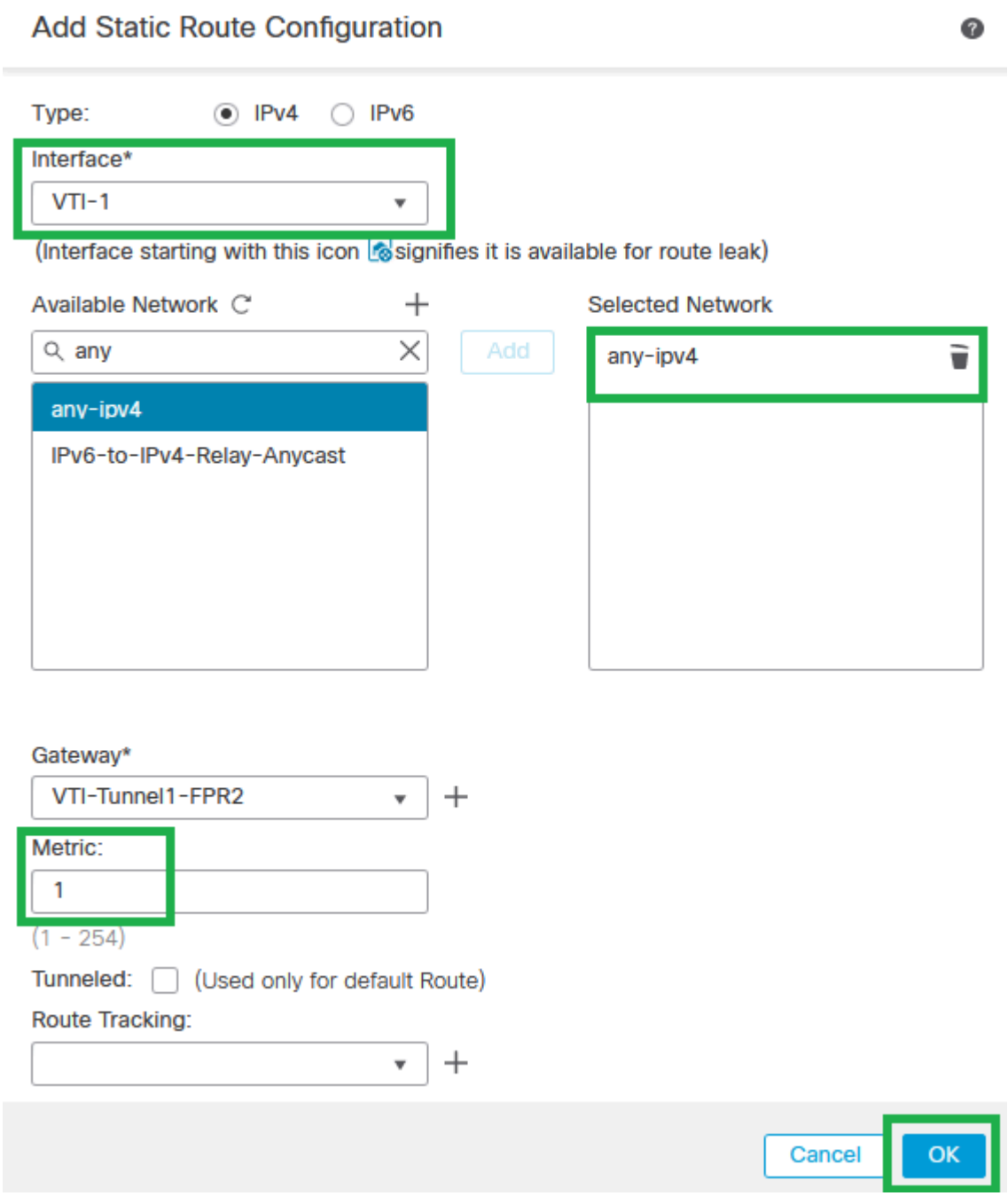
Routing - Ruta estática

Paso 8. Haga clic en + Add Route



+ Agregar ruta

Paso 9. Cree una ruta estática por defecto para las interfaces VTI (VTI-1 para esta guía de configuración) con 1 como valor de métrica y, a continuación, haga clic en OK.

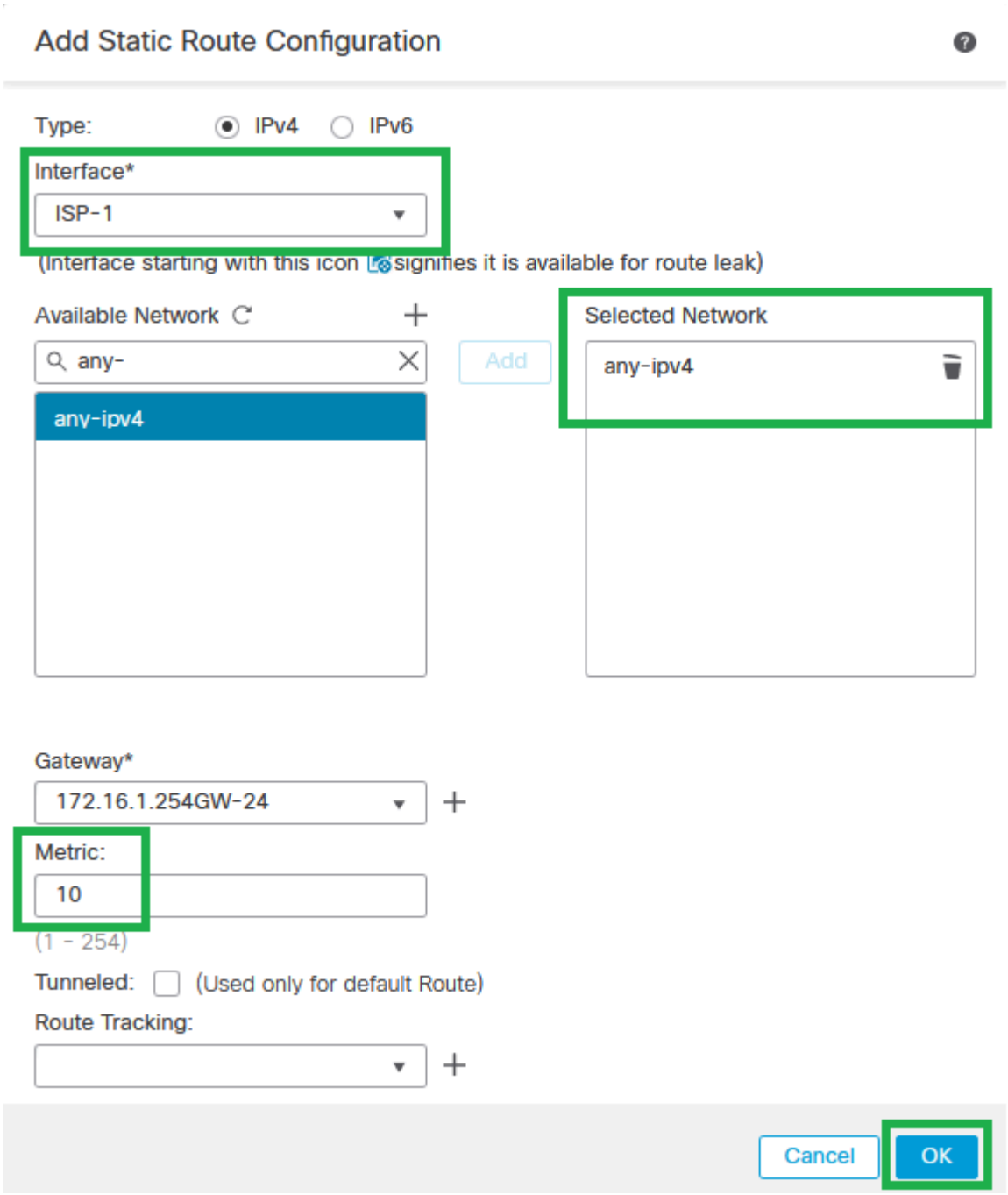


Ruta estática predeterminada para VTI-1

Paso 10. Repita el Paso 8 si hay más interfaces VTI configuradas.

Nota: Cree una ruta predeterminada para cada interfaz VTI configurada.

Paso 11. Cree una ruta estática predeterminada para las interfaces WAN/ISP (ISP-1 para esta guía de configuración) con un valor de métrica mayor que VTI y, a continuación, haga clic en OK.

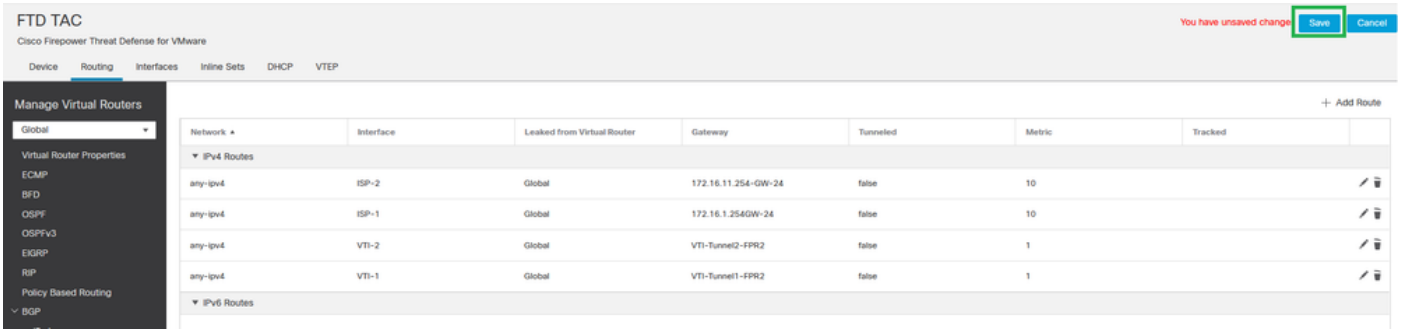


Ruta estática predeterminada para ISP-1

Paso 12. Repita el paso 10 si hay más interfaces WAN/ISP configuradas.

Nota: Cree una ruta predeterminada para cada interfaz WAN/ISP configurada.

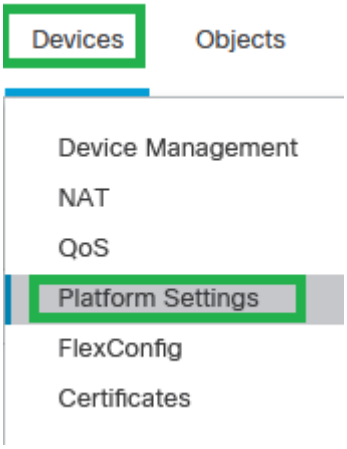
Paso 13. Valide la configuración de rutas predeterminadas y haga clic en OK.



Configuración de ruta estática

Configuración de DNS de confianza para FTD seguro

Paso 1. Desplácese hastaDevices > Platform Settings.

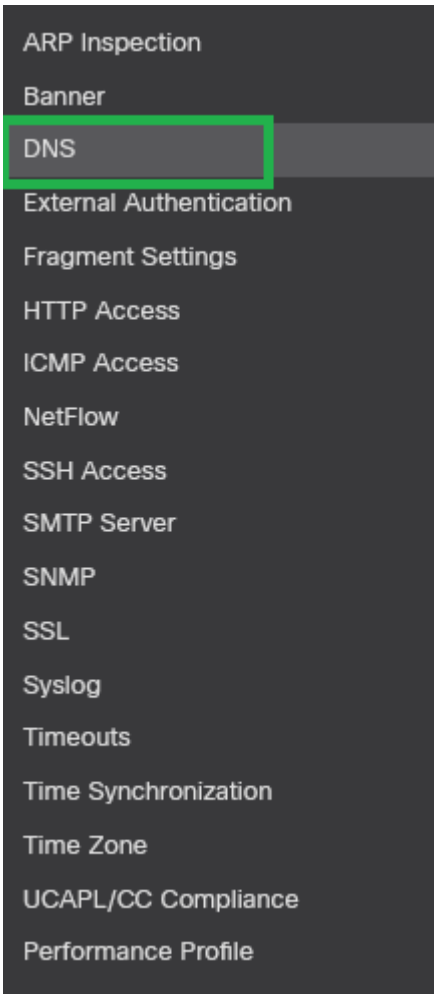


Dispositivos - Configuración de la plataforma

Paso 2. Cree o edite una política de configuración de plataforma existente.

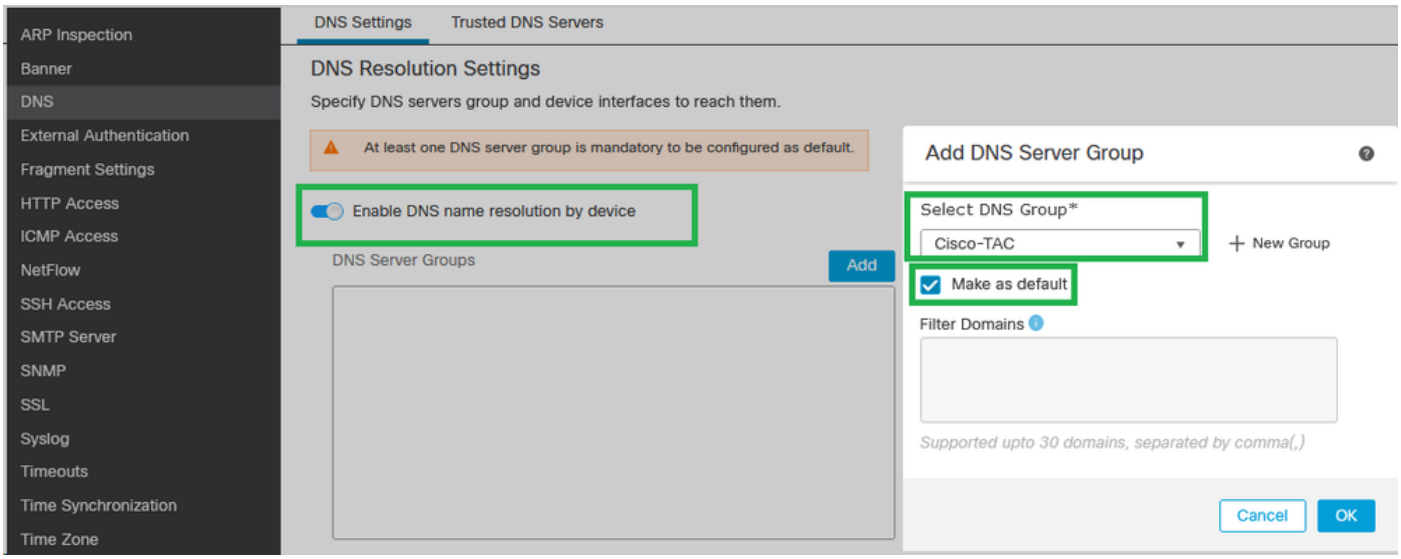
Nota: Asegúrese de que se aplica la política de configuración de la plataforma a los dispositivos de defensa frente a amenazas seguras.

Paso 3. Haga clic en DNS



Configuración de plataforma DNS

Paso 4. Habilite DNS name resolution by devicey haga clic en Add o elija un grupo DNS existente. Elija Make as defaulty, a continuación, haga clic en OK.

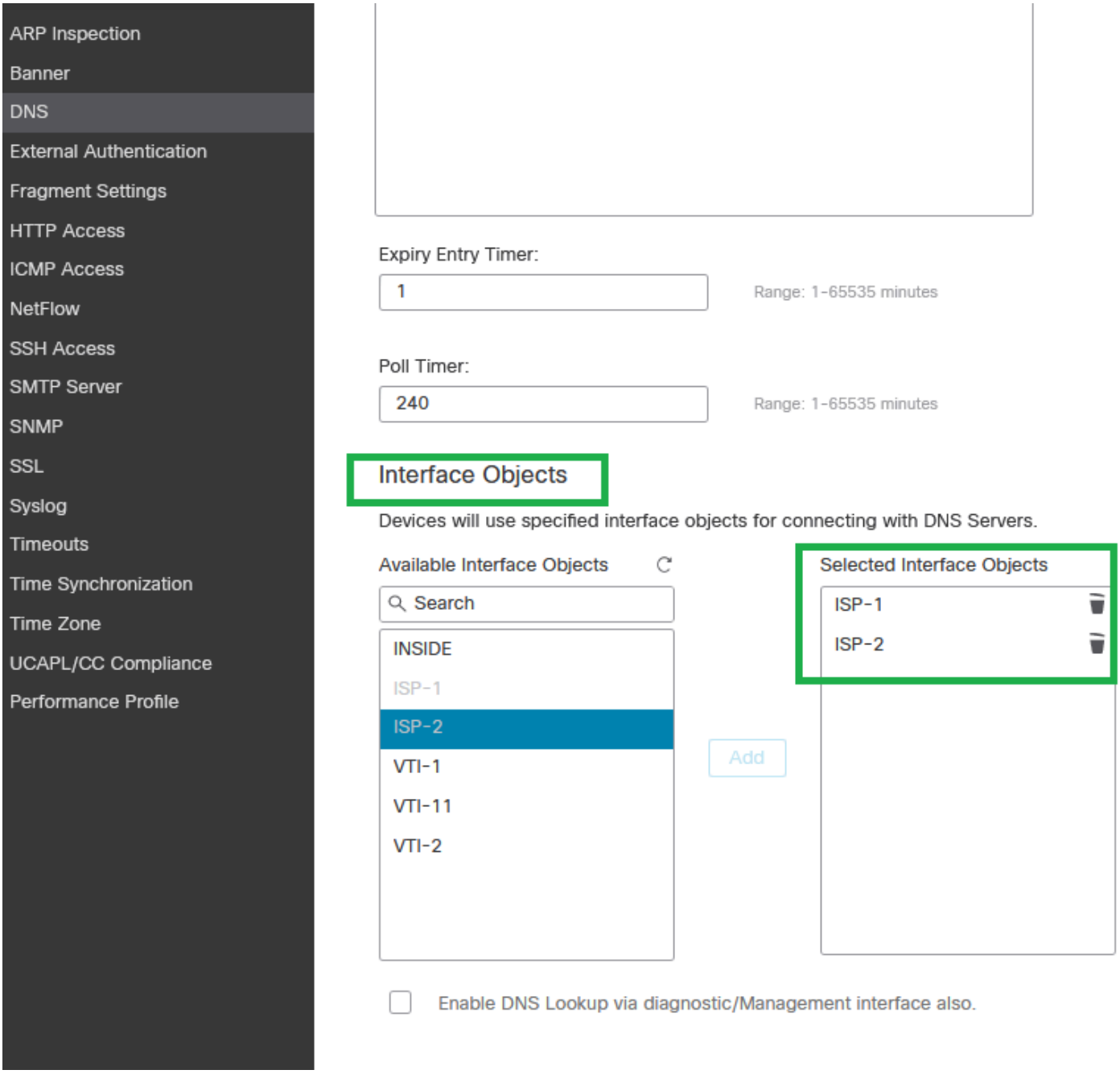


Agregar grupo de servidores DNS

Nota: Si desea obtener más información sobre la configuración de DNS en la política de

configuración de la plataforma, consulte la documentación [oficial de configuración de la plataforma](#).

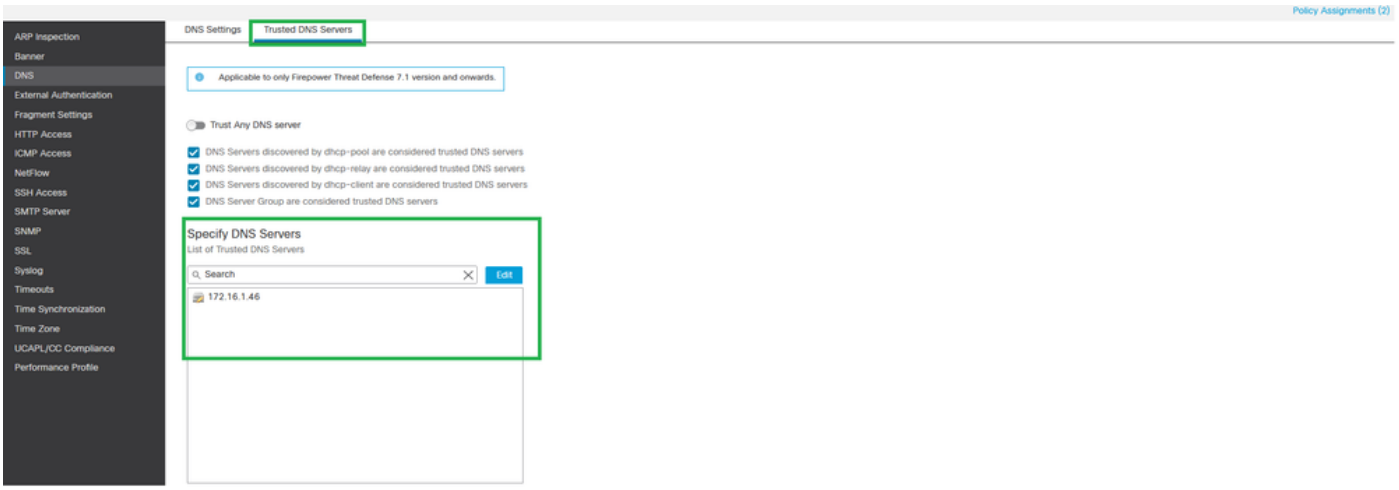
Paso 5. Elija las interfaces WAN/ISP en la Interface Objects sección.



Configuración de la interfaz DNS

Paso 6. Guarde los cambios.

Paso 7. Desplácese hasta el Trusted DNS Servers y especifique los servidores DNS de confianza.

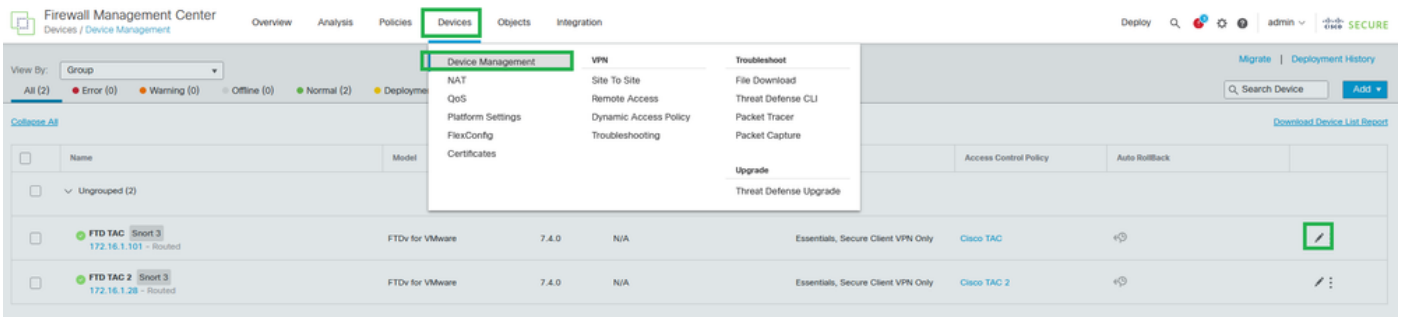


Servidores DNS de confianza

Paso 8. Haga clic Save y despliegue los cambios.

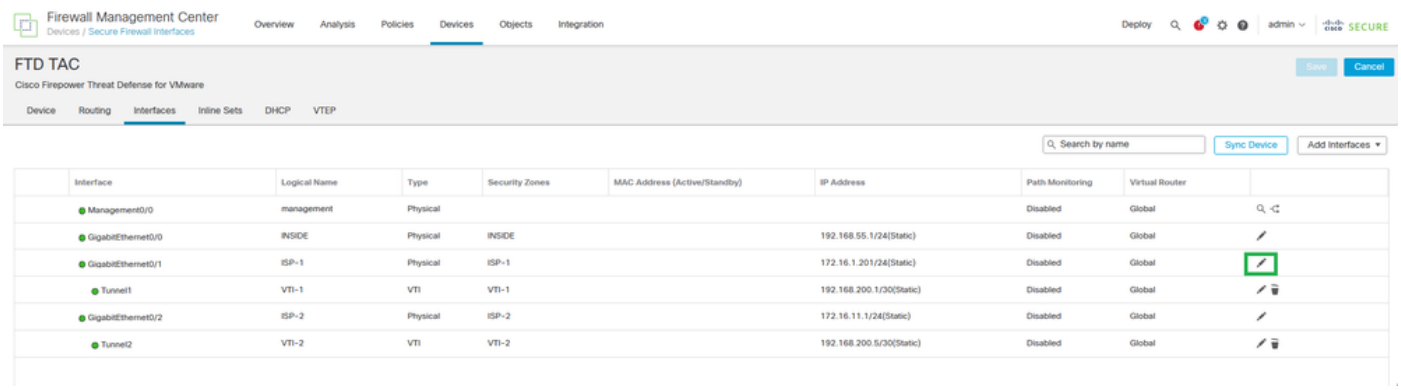
Habilitar supervisión de rutas

Paso 1. Desplácese hasta Devices > Device Managementy edite la defensa contra amenazas.



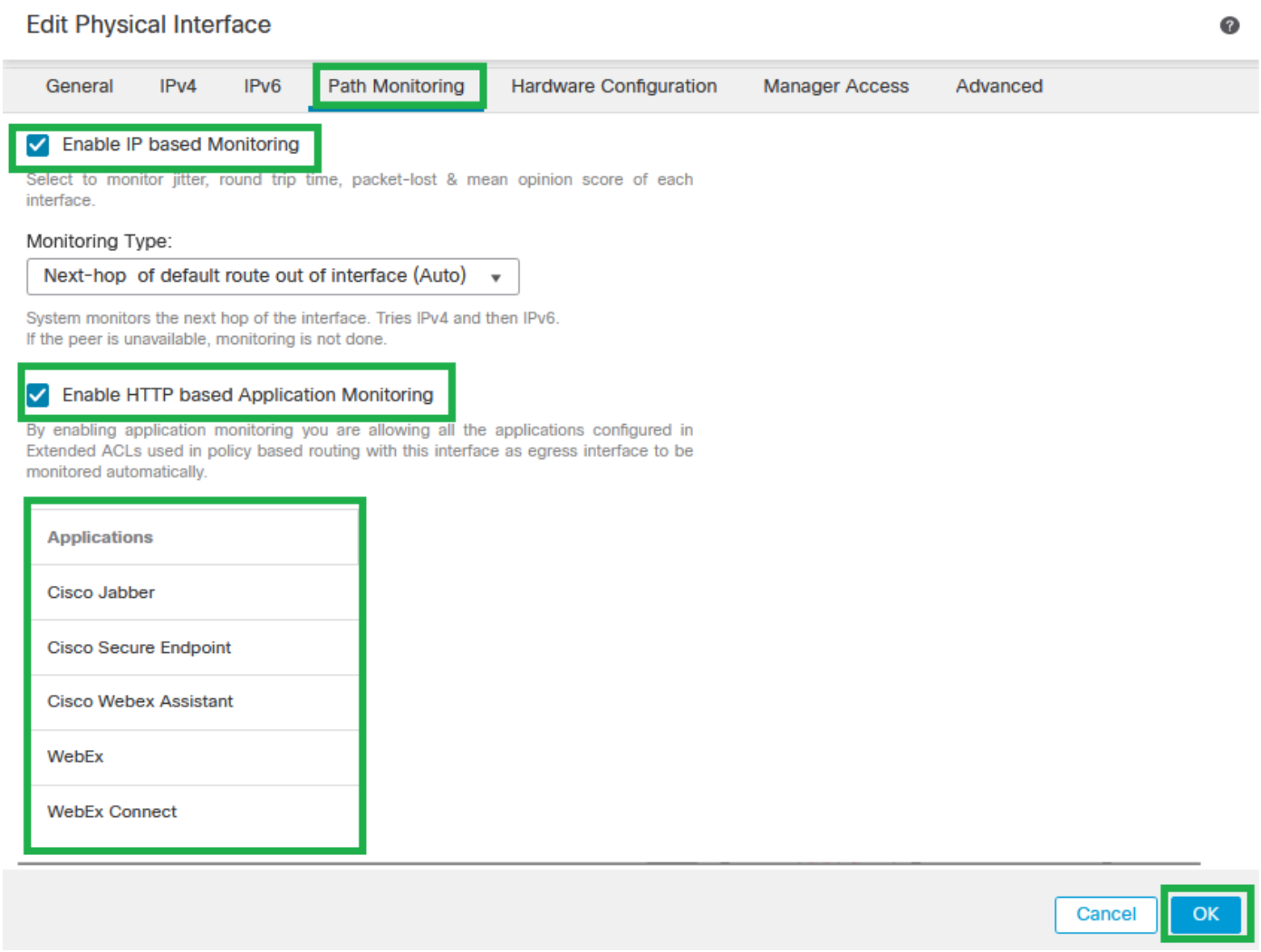
Dispositivo - Gestión de dispositivos

Paso 2. En la Interfaces ficha, edite la interfaz WAN/ISP interfaces (ISP-1 e ISP-2 para esta guía de configuración).



Configuración de la Interfaz

Paso 3. Haga clic en la Path Monitoring pestaña, seleccione el Enable IP Monitoring y active la HTTP-based Application Monitoring casilla de verificación. A continuación, haga clic en Save.



Configuración de Monitoreo de Trayectoria de Interfaz

Precaución: Se deben enumerar las aplicaciones configuradas en la sección de configuración anterior.

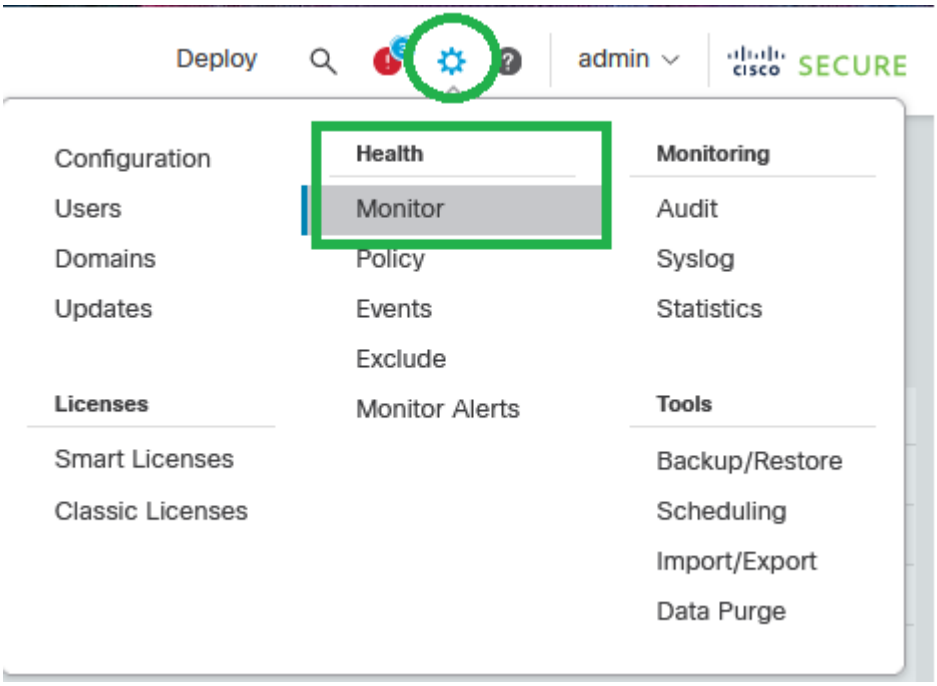
Nota: 'Tipo de supervisión' se ha elegido para esta guía de configuración. Verifique las configuraciones de monitoreo de trayectoria en la guía de configuración oficial para obtener más información sobre otras opciones.

Paso 4. Repita los pasos 2 y 3 para todas las interfaces WAN/ISP configuradas.

Paso 5. Haga clic Save y despliegue los cambios.

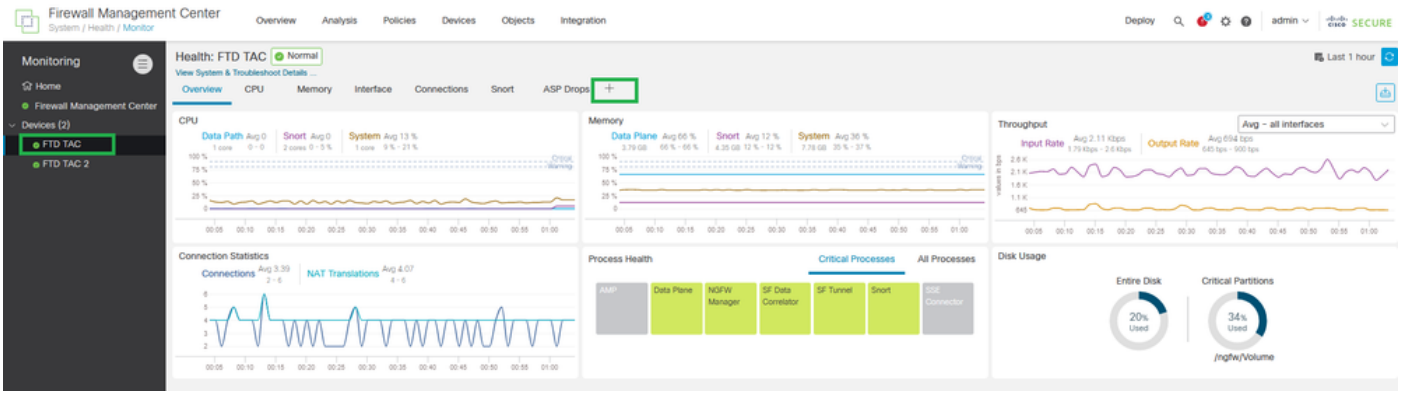
Agregar panel de supervisión

Paso 1. Desplácese hasta System > Health > Monitor.



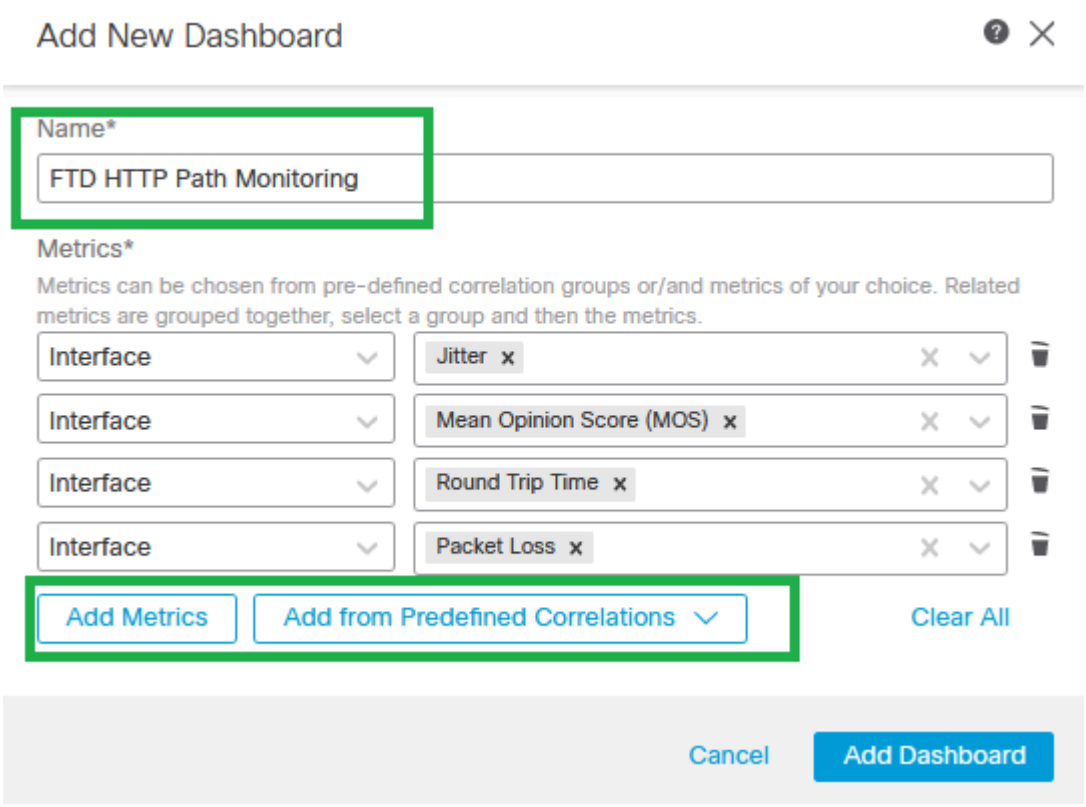
Sistema - Estado - Monitor

Paso 2. Elija el dispositivo FTD seguro y haga clic en Add New Dashboard.



Agregar nuevo panel

Paso 3. Configure el nombre del panel y, en el Correlate Metrics cuadro de diálogo, en la lista desplegable, seleccione Interface - Path Metrics. A continuación, haga clic en Add Dashboard.



Agregar nuevo panel con indicadores de ruta

Verificación

En esta sección se describe cómo verificar las rutas estáticas flotantes, ECMP, el grupo de objetos con aplicaciones y las configuraciones PBR.

Verifique la configuración de rutas predeterminadas y rutas estáticas flotantes:

```
firepower# show run route
route VTI-1 0.0.0.0 0.0.0.0 192.168.200.1 1
route VTI-2 0.0.0.0 0.0.0.0 192.168.200.5 1
route ISP-1 0.0.0.0 0.0.0.0 172.16.1.254 10
route ISP-2 0.0.0.0 0.0.0.0 172.16.11.254 10
```

Verifique la configuración de ECMP:

```
firepower# sh run | i ecmp
zone ECMP-VTI ecmp
zone ECMP-ISP ecmp
```

Verifique si el ECMP está equilibrando el tráfico en la tabla de ruteo. La tabla de ruteo debe instalar ambas rutas en la tabla de ruteo FTD seguro.

```
firepower# show route static

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 172.16.11.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.200.5, VTI-2
[1/0] via 192.168.200.1, VTI-1
```

Verificar la configuración del mapa de ruta PBR:

```
firepower# show run route-map
!
route-map FMC_GENERATED_PBR_1694885402369 permit 5
match ip address Applications
set adaptive-interface cost ISP-1 ISP-2
!
```

Verifique la ACL asignada a la configuración PBR (verifique el nombre de la ACL en la configuración del route-map):

```
firepower# show run access-list | i Applications
access-list Applications extended permit ip any object-group-network-service FMC_NSG_639950173988
```

Verifique el grupo de objetos con aplicaciones asignadas a la lista de acceso (verifique el nombre del grupo de objetos en la configuración ACL):

```
firepower# show run object-group
object-group network-service FMC_NSG_639950173988
network-service-member "Cisco Jabber"
network-service-member "Cisco Secure Endpoint"
network-service-member "Cisco Webex Assistant"
network-service-member "WebEx"
network-service-member "WebEx Connect"
network-service-member "Webex Teams"
```

Verifique la ruta de política asignada a las interfaces de datos utilizadas en la configuración PBR:

```
interface GigabitEthernet0/0
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 172.16.35.1 255.255.255.0
policy-route route-map FMC_GENERATED_PBR_1694885402369
!
interface GigabitEthernet0/1
nameif ISP-1
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
zone-member ECMP-ISP
ip address 172.16.1.202 255.255.255.0
policy-route path-monitoring auto
!
interface GigabitEthernet0/2
nameif ISP-2
security-level 0
zone-member ECMP-ISP
ip address 172.16.11.2 255.255.255.0
policy-route path-monitoring auto
!
```

Verifique y verifique las estadísticas de Fluctuación, MOS, Tiempo de Ida y Vuelta y Pérdida de Paquetes desde la información del Panel de Control de Trayectoria HTTP.

Verificar Panel de Monitoreo de Trayectoria HTTP

Troubleshoot

En caso de que falle la supervisión de ruta, con la supervisión basada en IP activada, las interfaces WAN/ISP se configuran para enviar paquetes de sonda ICMP al gateway configurado en rutas estáticas. Configure las capturas de ingreso/egreso en las interfaces WAN/ISP para

verificar si ICMP funciona.

Captura de entrada y salida:

```
firepower# cap in interface ISP-1 trace match icmp any any
firepower# cap in2 interface isP-2 trace match icmp any any
```

Captura de entrada:

```
firepower# show cap in

12 packets captured
1: 00:08:28.073604 172.16.1.202 > 172.16.1.254 icmp: echo request
2: 00:08:28.074672 172.16.1.254 > 172.16.1.202 icmp: echo reply
3: 00:08:29.150871 172.16.1.202 > 172.16.1.254 icmp: echo request
4: 00:08:29.151832 172.16.1.254 > 172.16.1.202 icmp: echo reply
5: 00:08:30.217701 172.16.1.202 > 172.16.1.254 icmp: echo request
6: 00:08:30.218876 172.16.1.254 > 172.16.1.202 icmp: echo reply
7: 00:08:31.247728 172.16.1.202 > 172.16.1.254 icmp: echo request
8: 00:08:31.248980 172.16.1.254 > 172.16.1.202 icmp: echo reply
9: 00:08:32.309005 172.16.1.202 > 172.16.1.254 icmp: echo request
10: 00:08:32.310317 172.16.1.254 > 172.16.1.202 icmp: echo reply
11: 00:08:33.386622 172.16.1.202 > 172.16.1.254 icmp: echo request
12: 00:08:33.387751 172.16.1.254 > 172.16.1.202 icmp: echo reply
12 packets shown
1: 00:08:28.073604 172.16.1.202 > 172.16.1.254 icmp: echo request
2: 00:08:28.074672 172.16.1.254 > 172.16.1.202 icmp: echo reply
3: 00:08:29.150871 172.16.1.202 > 172.16.1.254 icmp: echo request
4: 00:08:29.151832 172.16.1.254 > 172.16.1.202 icmp: echo reply
5: 00:08:30.217701 172.16.1.202 > 172.16.1.254 icmp: echo request
6: 00:08:30.218876 172.16.1.254 > 172.16.1.202 icmp: echo reply
7: 00:08:31.247728 172.16.1.202 > 172.16.1.254 icmp: echo request
8: 00:08:31.248980 172.16.1.254 > 172.16.1.202 icmp: echo reply
9: 00:08:32.309005 172.16.1.202 > 172.16.1.254 icmp: echo request
10: 00:08:32.310317 172.16.1.254 > 172.16.1.202 icmp: echo reply
11: 00:08:33.386622 172.16.1.202 > 172.16.1.254 icmp: echo request
12: 00:08:33.387751 172.16.1.254 > 172.16.1.202 icmp: echo reply
12 packets shown
```

Captura de salida:

```
firepower# show cap in2

12 packets captured

1: 00:08:28.073543 172.16.11.2 > 172.16.11.254 icmp: echo request
2: 00:08:28.074764 172.16.11.254 > 172.16.11.2 icmp: echo reply
3: 00:08:29.150810 172.16.11.2 > 172.16.11.254 icmp: echo request
4: 00:08:29.151954 172.16.11.254 > 172.16.11.2 icmp: echo reply
5: 00:08:30.217640 172.16.11.2 > 172.16.11.254 icmp: echo request
```

```
6: 00:08:30.218799 172.16.11.254 > 172.16.11.2 icmp: echo reply
7: 00:08:31.247667 172.16.11.2 > 172.16.11.254 icmp: echo request
8: 00:08:31.248888 172.16.11.254 > 172.16.11.2 icmp: echo reply
9: 00:08:32.308913 172.16.11.2 > 172.16.11.254 icmp: echo request
10: 00:08:32.310012 172.16.11.254 > 172.16.11.2 icmp: echo reply
11: 00:08:33.386576 172.16.11.2 > 172.16.11.254 icmp: echo request
12: 00:08:33.387888 172.16.11.254 > 172.16.11.2 icmp: echo reply
12 packets captured
```

Precaución: Asegúrese de configurar las capturas con las direcciones IP de origen y destino, ya que las capturas pueden aumentar considerablemente el rendimiento en el dispositivo.

Consejo: Si el ping no funciona, resuelva el problema de la conexión directa con el gateway predeterminado, verifique la tabla ARP o comuníquese con el TAC de Cisco.

Para verificar si PBR funciona, puede utilizar la herramienta packet tracer para asegurarse de que el tráfico de la aplicación se rutee con PBR.

```
firepower# packet-tracer input insIDE tcp 172.16.35.2 54352 'PUBLIC-IP-ADDRESS-FOR-WEBEX' $
---
[Output omitted]
---
Phase: 3
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Config:
route-map FMC_GENERATED_PBR_1694885402369 permit 5
match ip address Applications
set ip next-hop 172.16.1.254
Additional Information:
Matched route-map FMC_GENERATED_PBR_1694885402369, sequence 5, permit
Found next-hop 172.16.1.254 using egress ifc ISP-1
---
[Output omitted]
---
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: ISP-1
output-status: up
output-line-status: up
Action: allow
```

Nota: Para aprender sobre las direcciones IP de la aplicación para el servicio de red configurado en los grupos de objetos, utilice el comando **show object-group network-service detail**.

Información Relacionada

Los documentos adicionales relacionados con PBR con HTTP Path Monitoring se pueden encontrar aquí:

- Guía de configuración de routing basado en políticas en el centro de administración de firewall seguro
- Guía de configuración de la supervisión de rutas en la configuración de routing basado en políticas en el centro de administración de firewalls seguros
- Configurar política de ruteo basada en políticas
- Ejemplo de Configuración para Policy-Based Routing
- Ejemplo de Configuración para Monitoreo de Trayectoria PBR
- Agregar panel de supervisión de rutas
- Guía de configuración de la configuración de la plataforma DNS en el Centro de administración de firewall seguro
- 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).