

¿Cómo se configura el routing basado en políticas (PBR) en un switch o router multicapa de Cisco para reenviar el tráfico al WSA?

Contenido

[Pregunta:](#)

Pregunta:

¿Cómo se configura el routing basado en políticas (PBR) en un switch o router multicapa de Cisco para reenviar el tráfico al WSA?

Entorno: dispositivo de seguridad Cisco Web Security Appliance (WSA), modo transparente (switch L4)

Cuando WSA se configura en modo transparente mediante un switch L4, no es necesario realizar ninguna configuración en el WSA. El redireccionamiento es controlado por el switch (o router) L4.

Es posible utilizar el routing basado en políticas (PBR) para redirigir el tráfico web a WSA. Esto se logra haciendo coincidir el tráfico correcto (según los puertos TCP) e indicando al router/switch que redirija este tráfico al WSA.

En el siguiente ejemplo, la interfaz de datos/proxy de WSA (M1 o P1 según la configuración) se encuentra en una interfaz VLAN dedicada del switch/router multicapa (Vlan3) y el router de Internet también se encuentra en una interfaz VLAN dedicada (Vlan4). Los clientes se encuentran en Vlan1 y Vlan2.

Configuración inicial (solo se muestran las piezas relevantes)

```
interfaz Vlan1
desc User VLAN 1
IP address 10.1.1.1 255.255.255.0
!
interface Vlan2
desc User VLAN 2
IP address 10.1.2.1 255.255.255.0
!
interface Vlan3
```

```
desc VLAN dedicada de Cisco WSA
ip address 192.168.1.1 255.255.255.252
!
interface Vlan4
desc Internet Router dedicated VLAN
ip address 192.168.2.1 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

En el ejemplo anterior, y si Cisco WSA tiene una dirección IP 192.168.1.2, debe agregar los siguientes comandos para configurar el routing basado en políticas (PBR):

Paso 1: Definir el tráfico web

```
! Coincidir tráfico HTTP
access-list 100 permit tcp 10.1.1.0 0.0.0.255 any eq 80
access-list 100 permit tcp 10.1.2.0 0.0.0.255 any eq 80
! Coincidir con tráfico HTTPS
access-list 100 permit tcp 10.1.1.0 0.0.0.255 any eq 443
access-list 100 permit tcp 10.1.2.0 0.0.0.255 any eq 443
```

Paso 2: Defina un mapa de ruta para controlar dónde se envían los paquetes.

```
route-map ForwardWeb permit 10
match ip address 100
set ip next-hop 192.168.1.2
```

Paso 3: Aplique el mapa de ruta a la interfaz correcta.

```
!Tenga en cuenta que esto debe aplicarse a la interfaz de origen (lado del cliente)
interfaz Vlan1
ip policy route-map ForwardWeb
!
interface Vlan2
ip policy route-map ForwardWeb
```

Nota: este método de redirección del tráfico (PBR) tiene algunas limitaciones. El principal problema de este método es que el tráfico siempre se redirigirá al WSA aunque el dispositivo no sea accesible (por ejemplo, debido a problemas de red). Por lo tanto, no existe una opción de recuperación.

Para solucionar esta deficiencia, puede configurar uno de los siguientes elementos:

1. PBR con opciones de seguimiento al utilizar routers de Cisco. Esta función se utiliza para verificar la disponibilidad del salto siguiente antes de redirigir el tráfico.

Más detalles en el siguiente artículo:

[Ruteo basado en la política con el ejemplo de configuración de la función de opciones de seguimiento múltiple](#)

2. Las opciones de seguimiento no están disponibles para los switches Catalyst de Cisco. Sin embargo, existe una solución alternativa avanzada disponible para lograr el mismo comportamiento.

Puede encontrar más información en la siguiente wiki de Cisco:

[Routing basado en políticas \(PBR\) con seguimiento para switches Catalyst 3xxx: una solución alternativa mediante EEM](#)

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).