Contenido

Pregunta:

¿Cómo configuro el Routing basado en políticas (PBR) en un switch multicapa o un router de Cisco para remitir el tráfico al WSA?

Entorno: Dispositivo de seguridad de la red de Cisco (WSA), modo transparente - Switch L4

Cuando WSA se configura en el modo transparente que usa un Switch L4, no se necesita ninguna configuración en el WSA. El cambio de dirección es controlado por el Switch L4 (o el router).

Es posible utilizar el Routing basado en políticas (PBR) para reorientar el tráfico de la Web al WSA. Esto es alcanzada correspondiendo con el tráfico correcto (basado en los puertos tcp) y dando instrucciones el router/el Switch para reorientar este tráfico al WSA.

En el siguiente ejemplo, los datos WSA/la interfaz del proxy (M1 o P1 dependiendo de la configuración) está en una interfaz del vlan dedicada del switch multicapa/del router (Vlan 3) y el router de Internet está en una interfaz del vlan dedicada también (Vlan4). Los clientes están en el vlan1 y Vlan2.

Configuración inicial (solamente partes pertinentes visualizadas)
interfaz Vlan1 VLAN de usuario 1 del desc dirección IP 10.1.1.1 255.255.255.0 ¡! interfaz Vlan2 VLAN de usuario 2 del desc dirección IP 10.1.2.1 255.255.255.0 ¡! interfaz Vlan3 vlan dedicada de Cisco WSA del desc dirección IP 192.168.1.1 255.255.255.252 ¡! interfaz Vlan4 vlan dedicada del router de Internet del desc dirección IP 192.168.2.1 255.255.255.252 ¡! ruta de IP 0.0.0.0 0.0.0.0 192.168.2.2

Dado el ejemplo antedicho, y Cisco WSA que tiene una dirección IP de 192.168.1.2, usted agregaría los siguientes comandos de configurar el Routing basado en políticas (PBR):

Paso 1: Defina el tráfico de la Web

¡! Haga juego el tráfico HTTP la lista de acceso 100 permite tcp 10.1.1.0 0.0.0.255 cualquier eq 80 la lista de acceso 100 permite tcp 10.1.2.0 0.0.0.255 cualquier eq 80 *¡! Tráfico de la coincidencia HTTPS* la lista de acceso 100 permite tcp 10.1.1.0 0.0.0.255 cualquier eq 443 la lista de acceso 100 permite tcp 10.1.2.0 0.0.0.255 cualquier eq 443
Paso 2: Defina un Route Map para controlar donde se hacen salir los paquetes.
permiso 10 de ForwardWeb del route-map IP Address 100 de la coincidencia fije el Next-Hop 192.168.1.2 del IP
Paso 3: Aplique el Route Map a la interfaz correcta.
¡! Observe que esto se debe aplicar a la interfaz de origen (lado del cliente) interfaz Vlan1 route-map ForwardWeb de la directiva del IP ¡! interfaz Vlan2 route-map ForwardWeb de la directiva del IP

Nota: Este método de (PBR) del cambio de dirección del tráfico tiene algunas limitaciones. El problema principal con este método es que el tráfico será reorientado siempre al WSA incluso si el dispositivo no es accesible (debido a los problemas de red por ejemplo). Así pues, no hay fall sobre la opción.

A la solución alternativa esta deficiencia, usted puede configurar cualquiera del siguiente:

1. **PBR con las opciones de seguimiento** al usar a los routeres Cisco. Esta característica se utiliza para verificar la Disponibilidad del salto siguiente antes de reorientar el tráfico.

   Más detalles en el artículo siguiente:
   Ruteo basado en la política con el ejemplo de configuración de la función de opciones de seguimiento múltiple
2. Siguiendo las opciones no esté disponible para el Switches del Cisco Catalyst. Sin embargo, hay una solución alternativa avanzada disponible alcanzar el mismo comportamiento.

   Los detalles se pueden encontrar en Cisco siguiente Wiki:
   Routing basado en políticas (PBR) con el seguimiento para los Catalyst 3xxx Switch - Una solución alternativa usando EEM