

Proceso de elección de Director de Balanceo de Carga VPN de ASA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Algoritmo de Balanceo de Carga](#)

[Proceso de elección del director](#)

[Advertencia sobre los escenarios de reinicio](#)

[Proceso de reelección del director](#)

[Dispositivo Director eliminado del clúster](#)

[El dispositivo Director no responde a los mensajes Hello de miembro del clúster](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe el proceso de elección de Director en un escenario de balanceo de carga VPN con Cisco 5500-X Series Adaptive Security Appliance (ASA).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en el Cisco ASA 5500-X que ejecuta la versión de software 9.2.

Nota: Este documento también se aplica a todas las versiones de software, ya que la función se introdujo por primera vez en la versión 7.0(1).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

El balanceo de carga VPN es un mecanismo que se utiliza para distribuir el tráfico de red equitativamente entre los dispositivos en un agrupamiento virtual. El equilibrio de carga se basa en una distribución simple; no tiene en cuenta la utilización del rendimiento ni otros factores. Un clúster de equilibrio de carga consta de dos o más dispositivos, un director y uno o más dispositivos secundarios, y estos dispositivos no tienen que configurarse de forma idéntica.

Algoritmo de Balanceo de Carga

A continuación se presenta una descripción general del algoritmo de balanceo de carga:

- El dispositivo director mantiene una lista ordenada de miembros secundarios del clúster en orden ascendente de direcciones IP internas.
- La carga se calcula como un porcentaje entero (número de sesiones activas/máximas) que proporciona cada miembro del clúster secundario.
- El dispositivo director redirige el túnel VPN IPSec/Secure Sockets Layer (SSL) a un dispositivo con la carga más baja primero, hasta que sea un 1% superior que los demás dispositivos.
- El dispositivo director se redirige a sí mismo sólo cuando todos los miembros del clúster secundario son un 1% más altos que el dispositivo director.

Este es un ejemplo con un director y dos miembros secundarios del clúster:

- Todos los nodos comienzan con una carga del 0% y todos los porcentajes se redondean al 0,5% más cercano.
- El dispositivo director toma la conexión si todos los miembros tienen una carga un 1% mayor que el dispositivo director.
- Si el dispositivo director no toma la conexión, la sesión la toma el dispositivo de respaldo que actualmente tiene el menor porcentaje de carga.
- Si todos los miembros tienen el mismo porcentaje de carga, entonces el dispositivo de respaldo con la menor cantidad de sesiones toma la sesión.
- Si todos los miembros tienen el mismo porcentaje de carga y el mismo número de sesiones, entonces el dispositivo de respaldo con la menor cantidad de direcciones IP toma la sesión.

Proceso de elección del director

El proceso de balanceo de carga VPN Director Election se realiza en el clúster fuera de la red. Hay dos tipos de datos intercambiados en la red externa:

- Se intercambian los paquetes del protocolo de resolución de direcciones (ARP) para la dirección IP del clúster que se utilizan para la detección del director. El número máximo de paquetes ARP que se envían para la dirección IP del clúster para detectar al director es:

(10 - prioridad) + 1

Aquí, la *prioridad* se configura como en el subcomando **priority** del comando CLI **vpn load-balance**.

- Los paquetes UDP en el exterior para los mensajes de solicitud/respuesta Hello se intercambian. El número de puerto se especifica en el subcomando **cluster port load-balance** y es predeterminado en **9023**.

Por ejemplo, si la *prioridad* es cinco para un dispositivo de balanceo de carga, intenta enviar hasta seis paquetes ARP para ver si algún dispositivo director posee la dirección IP del clúster. Si se detecta un dispositivo director, el ASA no envía más mensajes ARP y espera 15 segundos antes de enviar la solicitud de saludo UDP. Luego, el dispositivo director responde con una respuesta UDP Hello.

Advertencia sobre los escenarios de reinicio

En una situación de reinicio con dos ASA en un clúster de balanceo de carga:

- ASA-1 o ASA-2 fueron los directores antes del reinicio.
- ASA-1 se reinicia.
- ASA-2 se convierte en el director si no lo era anteriormente.
- ASA-1 simplemente se une al clúster como miembro después del reinicio.

El algoritmo de balanceo de carga podría verse afectado por una configuración del switch donde también se conecta la interfaz exterior de los dispositivos de clúster. Por ejemplo, un algoritmo de árbol de expansión podría causar un retraso en la conectividad cuando se reinicie el dispositivo que está conectado al switch.

Consejo: El comando [spanning-tree port fast](#) ayuda a acelerar el proceso.

En algunos casos, un ASA recién reiniciado que tiene el balanceo de carga habilitado podría intentar convertirse en el dispositivo director (incluso si ya existe un dispositivo director) porque no puede alcanzar el dispositivo director actual debido a un retraso en la conectividad en el switch. Cuando se detecta un conflicto de dirección como resultado de una colisión ARP, el ASA con una dirección de control de acceso a medios (MAC) baja gana, mientras que el ASA con una dirección MAC más alta renuncia a la función de dispositivo director.

Proceso de reelección del director

Hay dos situaciones que provocan la reelección del dispositivo director.

Dispositivo Director eliminado del clúster

Cuando inhabilita la función en el ASA, se envía un mensaje de difusión a todos los miembros del clúster para informar del cambio y se realiza el [proceso electoral](#) descrito anteriormente.

El dispositivo Director no responde a los mensajes Hello de miembro del clúster

Si el dispositivo director no responde a un mensaje Hello del miembro del clúster, un miembro del clúster ASA tarda aproximadamente 20 segundos en detectar que el director ya no está presente. Los mensajes Hello se envían cada cinco segundos (no configurables). Si los miembros del clúster no reciben una respuesta del dispositivo director después de cuatro mensajes Hello, se activa el proceso electoral.

Troubleshoot

Nota: Consulte el artículo de Cisco [Información Importante sobre Comandos Debug](#) antes de utilizar los **comandos debug**.

Estos comandos de depuración pueden ser útiles en los intentos de resolver problemas con el sistema:

- **debug fsm 255** - Utilice este comando para activar el debug general de la Máquina de estado finito. Ingrese el comando **no debug all** para desactivarlo.
- **debug menu vpnlb 3** - Utilice este comando para activar el seguimiento de depuración del balanceo de carga VPN. Ingrese el comando **debug menu vpnlb 3** una vez más para desactivarlo.
- **debug menu vpnlb 4** - Utilice este comando para activar el seguimiento de la función de balanceo de carga VPN. Ingrese el comando **debug menu vpnlb 4** una vez más para desactivarlo.

Información Relacionada

- [Introducción al equilibrio de carga](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)