Ejemplo de Configuración de Balanceo de Carga de Cliente VPN Remoto en ASA 5500

Contenido

Introducción

El balanceo de carga es la capacidad de compartir Cisco VPN Clients en varias unidades Adaptive Security Appliance (ASA) sin la intervención del usuario. El balanceo de carga garantiza que la dirección IP pública tenga una alta disponibilidad para los usuarios. Por ejemplo, si falla el Cisco ASA que da servicio a la dirección IP pública, otro ASA del clúster asumirá la dirección IP pública.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Ha asignado direcciones IP a sus ASA y ha configurado el gateway predeterminado.
- IPSec está configurado en los ASA para los usuarios de VPN Client.
- Los usuarios de VPN pueden conectarse a todos los ASA con el uso de su dirección IP pública asignada individualmente.

Clientes aptos

El balanceo de carga sólo es efectivo en sesiones remotas iniciadas con estos clientes:

- Cisco VPN Client (versión 3.0 o posterior)
- Cisco VPN 3002 Hardware Client (versión 3.5 o posterior)
- Cisco ASA 5505 cuando actúa como cliente Easy VPN

Todos los demás clientes, incluidas las conexiones de LAN a LAN, pueden conectarse a un dispositivo de seguridad en el que se habilita el equilibrio de carga, pero no pueden participar en el equilibrio de carga.

Componentes Utilizados

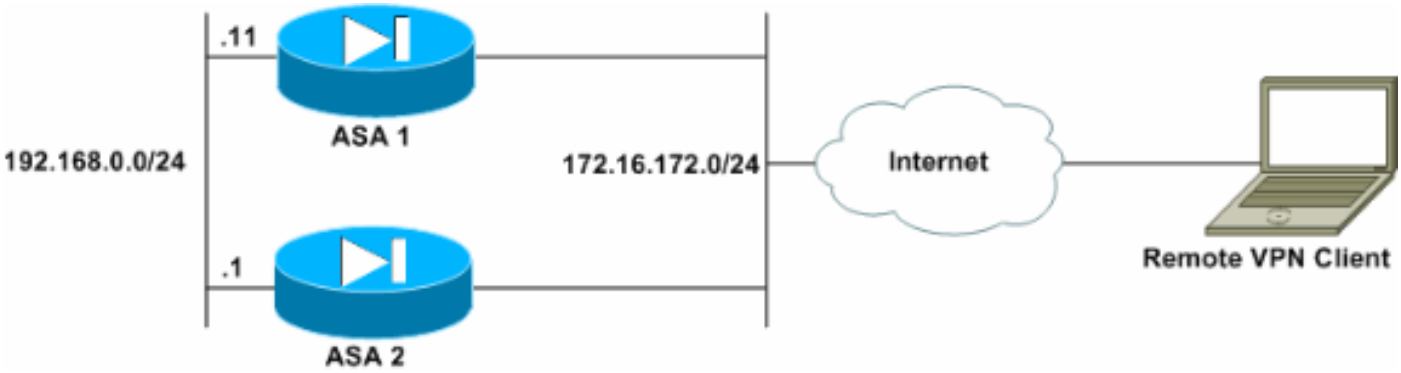
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versiones 4.6 y posteriores del software del cliente VPN
- Versiones 7.0.1 y posteriores del software Cisco ASA**Nota:** Amplía el soporte de balanceo de carga a los modelos ASA 5510 y ASA después de 5520 que tienen una licencia Security Plus con la versión 8.0(2).

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Restricciones

- La dirección IP del agrupamiento virtual VPN, el puerto del protocolo de datagrama de usuario (UDP) y los secretos compartidos deben ser idénticos en cada dispositivo del agrupamiento virtual.

- Todos los dispositivos del clúster virtual deben estar en las mismas subredes IP externas y internas.

Configuración

Asignación de dirección de IP

Asegúrese de que las direcciones IP estén configuradas en las interfaces externa e interna y de que pueda acceder a Internet desde su ASA.

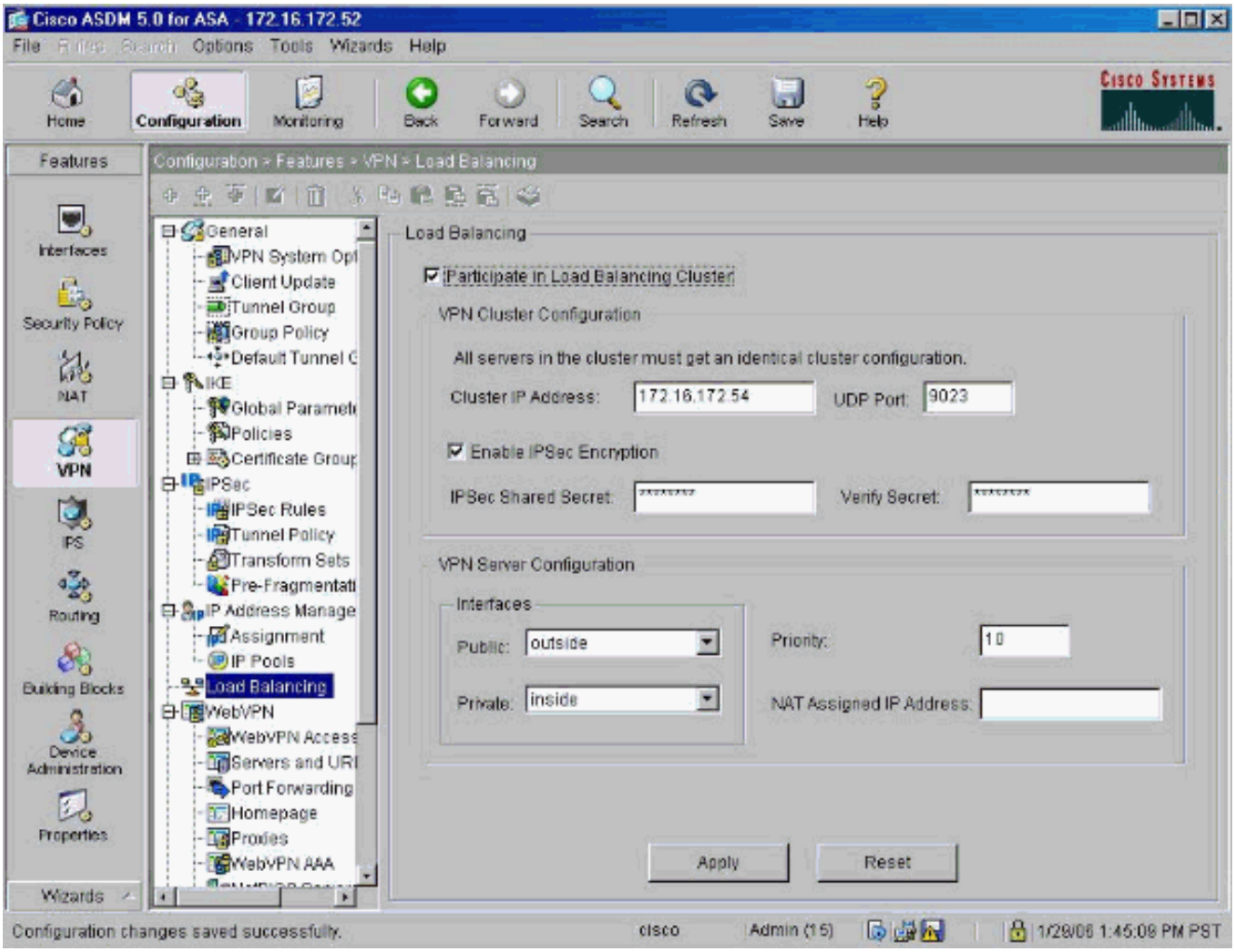
Nota: Asegúrese de que ISAKMP esté habilitado tanto en la interfaz interna como en la externa. Seleccione **Configuration > Features > VPN > IKE > Global Parameters** para verificar esto.

Configuración de agrupamiento

Este procedimiento muestra cómo utilizar Cisco Adaptive Security Device Manager (ASDM) para configurar el equilibrio de carga.

Nota: Muchos de los parámetros de este ejemplo tienen valores predeterminados.

1. Seleccione **Configuration > Features > VPN > Load Balancing**, y marque **Participar en el Clúster de Balanceo de Carga** para habilitar el balanceo de carga VPN.



2. Complete estos pasos para configurar los parámetros para todos los ASA que participan en

el clúster en el cuadro del grupo de configuración del clúster VPN:Escriba la dirección IP del clúster en el cuadro de texto Dirección IP del clúster.Haga clic en **Enable IPSec Encryption**.Escriba la clave de cifrado en el cuadro de texto Secreto compartido IPSec y vuelva a escribirla en el cuadro de texto Verificar secreto.

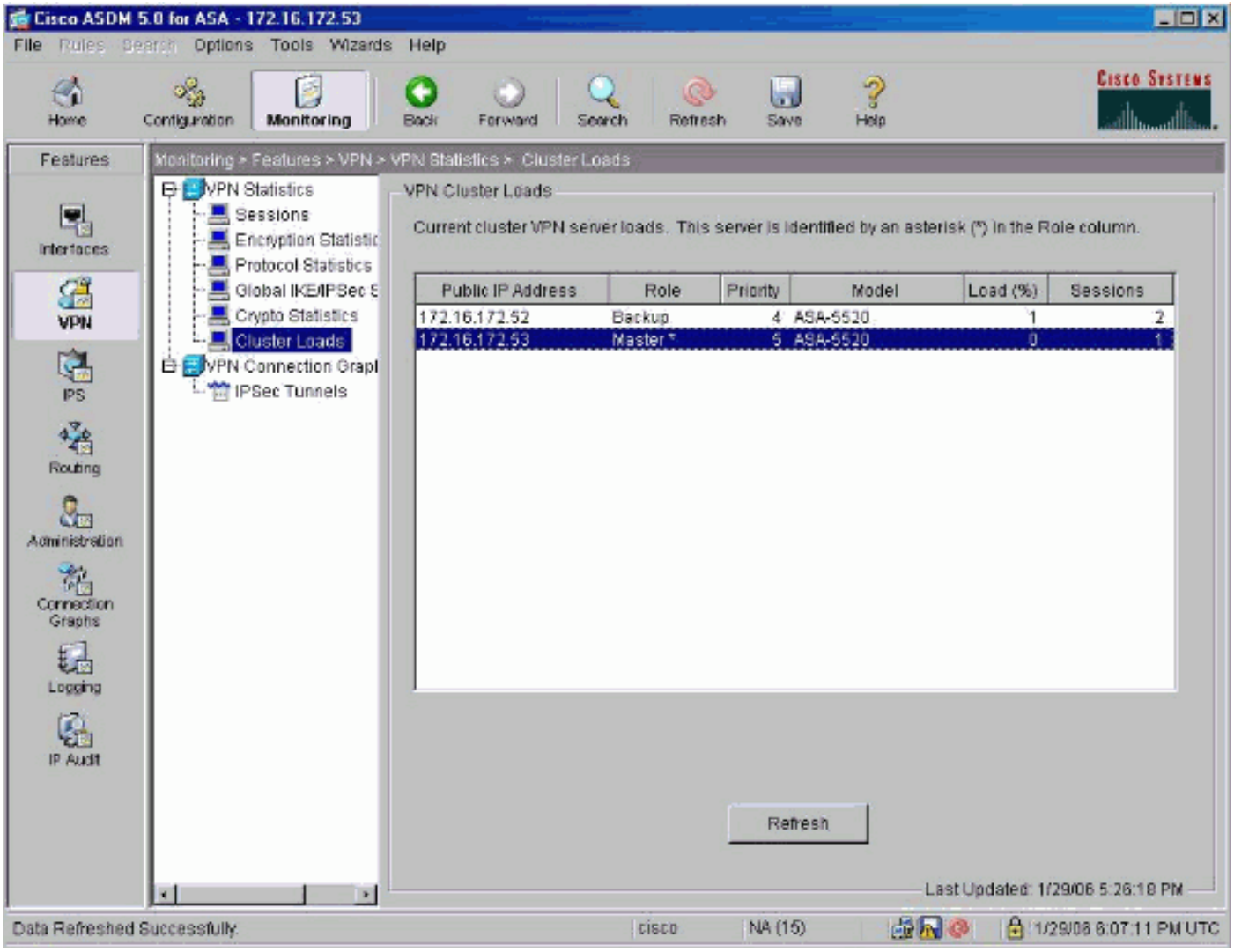
3. Configure las opciones en el cuadro del grupo de configuración del servidor VPN:Seleccione una interfaz que acepte las conexiones VPN entrantes en la lista Pública.Seleccione una interfaz que sea la interfaz privada en la lista Privado.(*Opcional*) Cambie la prioridad que el ASA tiene en el clúster en el cuadro de texto Prioridad.Escriba una dirección IP para la dirección IP asignada de traducción de direcciones de red (NAT) si este dispositivo está detrás de un firewall que utiliza NAT.
4. Repita los pasos en todos los ASA participantes del grupo.

El ejemplo de esta sección utiliza estos comandos CLI para configurar el balanceo de carga:

```
VPN-ASA2(config)#vpn load-balancing
VPN-ASA2(config-load-balancing)#priority 10
VPN-ASA2(config-load-balancing)#cluster key cisco123
VPN-ASA2(config-load-balancing)#cluster ip address 172.16.172.54
VPN-ASA2(config-load-balancing)#cluster encryption
VPN-ASA2(config-load-balancing)#participate
```

Control

Seleccione **Monitoring > Features > VPN > VPN Statistics > Cluster Loads** para monitorear la función de balanceo de carga en el ASA.



Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **show vpn load-balance**: verifica la función de balanceo de carga VPN.

```
Status: enabled
Role: Backup
Failover: n/a
Encryption: enabled
Cluster IP: 172.16.172.54
Peers: 1

Public IP Role Pri Model Load (%) Sessions
-------------------------------------------------------------
* 172.16.172.53 Backup 5 ASA-5520 0 1
172.16.172.52 Master 4 ASA-5520 n/a n/a
```

Troubleshoot

Use esta sección para resolver problemas de configuración.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

- **debug vpnlb 250**: se utiliza para resolver problemas de la función de balanceo de carga VPN.

```
VPN-ASA2#
VPN-ASA2# 5718045: Created peer[172.16.172.54]
5718012: Sent HELLO request to [172.16.172.54]
5718016: Received HELLO response from [172.16.172.54]
7718046: Create group policy [vpnlb-grp-pol]
7718049: Created secure tunnel to peer[192.168.0.11]
5718073: Becoming slave of Load Balancing in context 0.
5718018: Send KEEPALIVE request failure to [192.168.0.11]
5718018: Send KEEPALIVE request failure to [192.168.0.11]
5718018: Send KEEPALIVE request failure to [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718035: Received TOPOLOGY indicator from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
7718023: Received KEEPALIVE response from [192.168.0.11]
7718019: Sent KEEPALIVE request to [192.168.0.11]
```

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems