Equilibrio de carga remoto del cliente VPN en el ejemplo de configuración 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.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Usted tiene IP Address asignados en sus ASA y configuró el default gateway.
- El IPSec se configura en los ASA para los usuarios de cliente VPN.
- Los usuarios de VPN pueden conectar con todos los ASA con el uso de su individualmente IP Address público asignado.

Clientes elegibles

El Equilibrio de carga es eficaz solamente en las sesiones remotas iniciadas con estos clientes:

- Cliente Cisco VPN (3.0 de la versión o más adelante)
- Cliente de hardware Cisco VPN 3002 (versión 3.5 o más adelante)
- CiscoASA 5505 al actuar como cliente VPN fácil

El resto de los clientes, incluyendo las conexiones de LAN a LAN, pueden conectar con un dispositivo de seguridad en el cual se habilite el Equilibrio de carga, pero no pueden participar en el Equilibrio de carga.

Componentes Utilizados

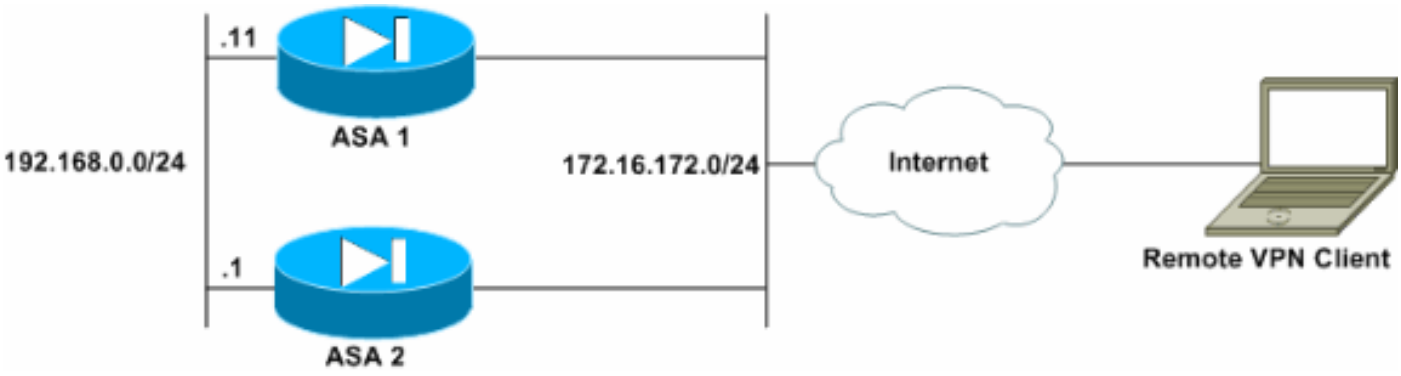
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versiones de software cliente VPN 4.6 y posterior
- Software Release 7.0.1 y Posterior de Cisco ASA**Nota:** Amplía el soporte del Equilibrio de carga a ASA 5510 y el ASA modela más adelante de 5520 que tengan una Seguridad más la licencia con 8.0(2) la versión.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

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 en el clúster virtual deben estar en las mismas subredes IP exteriores e interiores.

Configuración

Asignación de dirección de IP

Asegúrese de que los IP Addresses estén configurados en el exterior y las interfaces interiores y usted puede llegar a Internet de su ASA.

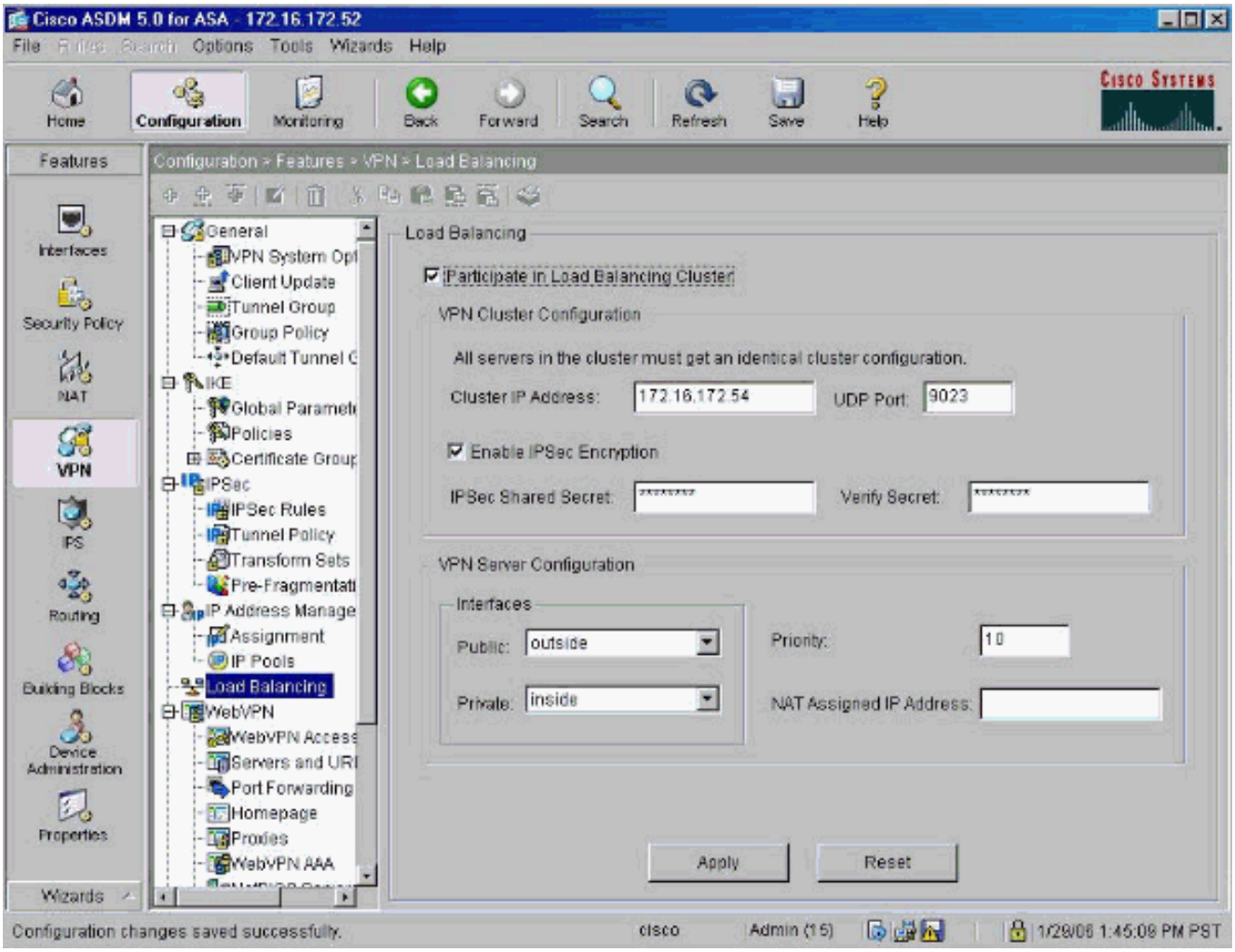
Nota: Asegúrese de que el ISAKMP esté habilitado en ambos las interfaces interior y exterior. Seleccione la **configuración > las características > el VPN > el IKE > los Parámetros globales** para verificar esto.

Configuración de agrupamiento

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

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

1. Seleccione la **configuración > las características > el VPN > el Equilibrio de carga**, y el control **participa en el cluster del Equilibrio de carga** para habilitar el Equilibrio de carga VPN.



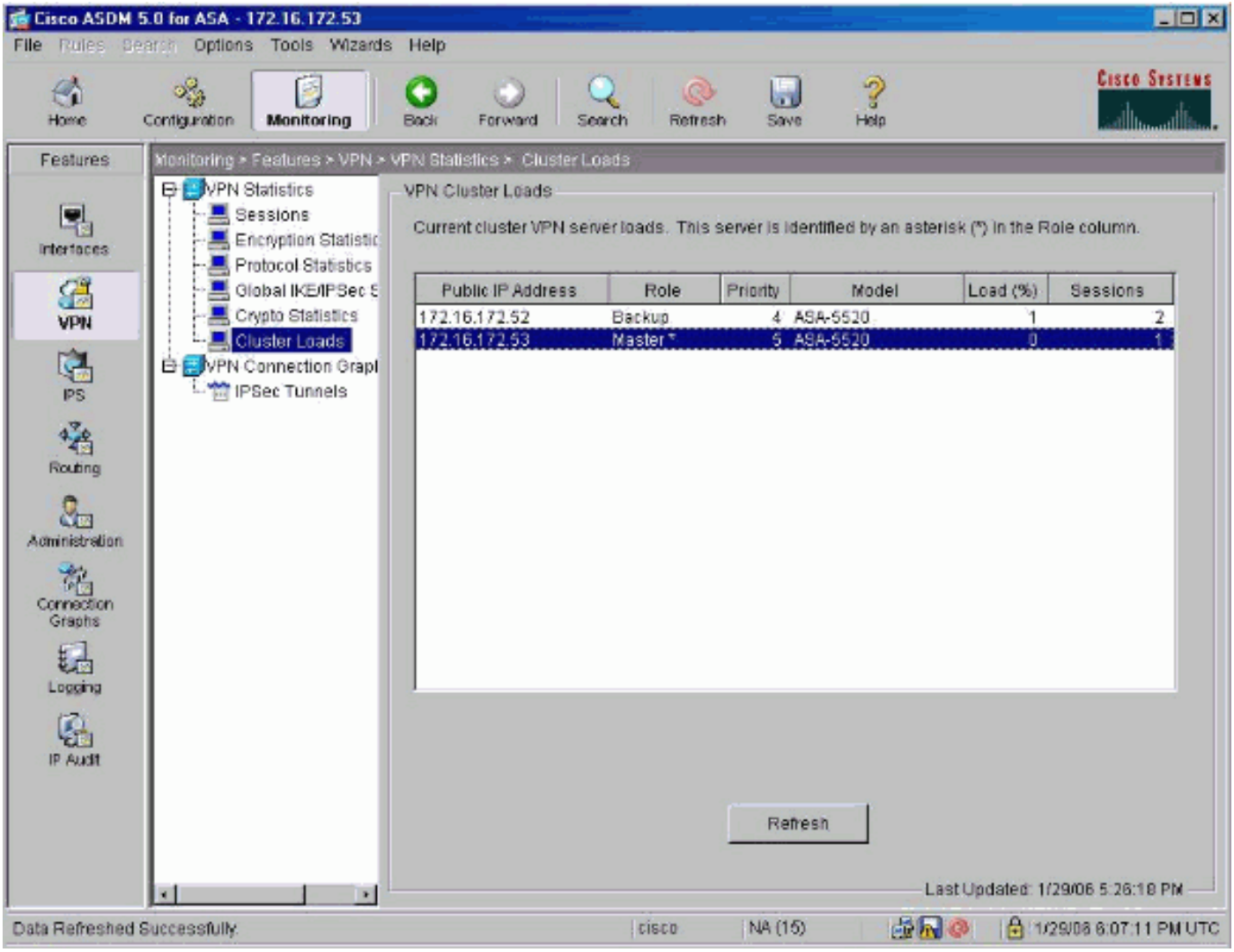
2. Complete estos pasos para configurar los parámetros para todos los ASA que participan en el cluster en la casilla de grupo de la configuración de clúster VPN:Teclee la dirección IP del cluster en el cuadro de texto de la dirección IP del cluster.Haga clic la **encripción de IPSec del permiso**.Teclee la clave de encripción en el cuadro de texto del secreto compartido de IPSec y tecleela otra vez en el cuadro de texto del secreto del verificar.
3. Configure las opciones en el cuadro de grupo de configuración del servidor VPN:Seleccione una interfaz que valide las conexiones VPN entrantes en la lista pública.Seleccione una interfaz que sea la interfaz privada en la lista privada.(*Opcional*) cambie la prioridad que el ASA tiene en el cluster en el cuadro de texto de la prioridad.Teclee una dirección IP para el IP Address asignado del Network Address Translation (NAT) si este dispositivo está detrás de un Firewall que utilice el NAT.
4. Relance los pasos en todos los ASA participantes en el grupo.

El ejemplo en esta sección utiliza estos comandos CLI de configurar el Equilibrio 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

La supervisión selecta **> ofrece > VPN > los VPN statistics (Estadísticas de la VPN) > las cargas del cluster** para monitorear la característica del Equilibrio 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.

- **muestre el balanceo de carga del vpn** — Verifica la característica del Equilibrio 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
```

Troubleshooting

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 de Debug antes de usar un **comando debug**.

- **haga el debug del vpnlb 250** — Utilizado para resolver problemas la característica del Equilibrio 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