Exemple de configuration de l'équilibrage de charge d'un client VPN distant sur ASA 5500

Contenu

Introduction

L'équilibrage de charge est la capacité à partager des clients VPN Cisco à travers plusieurs dispositifs de sécurité adaptatifs (ASA) sans aucune intervention de l'utilisateur. L'équilibrage de charge garantit que l'adresse IP publique est facilement disponible aux utilisateurs. Par exemple, si l'ASA de Cisco qui héberge l'adresse IP publique tombe en panne, un autre ASA dans le nuage prend le relais de l'adresse IP publique.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Vous avez assigné des adresses IP sur vos ASA et avez configuré la passerelle par défaut.
- IPsec est configuré sur les ASA pour les utilisateurs de client vpn.
- Les utilisateurs VPN peuvent se connecter à toutes les ASA à l'utilisation de leur adresse IP publique individuellement assignée.

Clients éligibles

L'Équilibrage de charge est efficace seulement sur des sessions distantes initiées avec ces clients :

- Client VPN Cisco (version 3.0 ou plus tard)
- Cisco VPN 3002 Hardware Client (version 3.5 ou plus tard)
- CiscoASA 5505 en agissant en tant que client d'Easy VPN

Tous autres clients, y compris des connexions entre réseaux locaux, peuvent se connecter à des dispositifs de sécurité sur lesquels l'Équilibrage de charge est activé, mais ils ne peuvent pas participer à l'Équilibrage de charge.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Versions 4.6 et ultérieures de logiciel de client VPN
- Versions de logiciel 7.0.1 et ultérieures de Cisco ASA**Remarque:** Étend le support d'Équilibrage de charge à l'ASA 5510 et à l'ASA modèle plus tard que 5520 qui ont un permis Security Plus avec 8.0(2) la version.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Restrictions

- Le port virtuel d'adresse IP, de Protocole UDP (User Datagram Protocol) de batterie VPN, et le secret partagé doivent être identiques sur chaque périphérique dans la batterie virtuelle.
- Tous les périphériques dans la batterie virtuelle doivent être sur les mêmes sous-réseaux extérieurs et intérieurs IP.

Configuration

Affectation d'adresse IP

Assurez-vous que les adresses IP sont configurées sur l'extérieur et les interfaces internes et vous

pouvez arriver à l'Internet de votre ASA.

Remarque: Assurez-vous que l'ISAKMP est activé sur chacun des deux l'interface interne et externe. **La configuration** choisie **> comporte > VPN > IKE > paramètres globaux** afin de vérifier ceci.

Configuration du cluster

Cette procédure affiche comment utiliser le Cisco Adaptive Security Device Manager (ASDM) pour configurer l'Équilibrage de charge.

Remarque: Plusieurs des paramètres dans cet exemple ont des valeurs par défaut.

1. **La configuration** choisie **> comporte > VPN > Équilibrage de charge**, et le contrôle **participent à la batterie d'Équilibrage de charge** pour activer l'Équilibrage de charge VPN.
2. Terminez-vous ces étapes pour configurer les paramètres pour toutes les ASA participant à la batterie dans la case de groupe de configuration du cluster VPN :Tapez l'adresse IP de la batterie dans la zone de texte d'adresse IP de batterie.**Chiffrement IPSec d'enable de** clic.Tapez la clé de chiffrement dans la zone de texte secrète partagée par IPSec et introduisez- au clavierla de nouveau la zone de texte de secret de vérifier.
3. Configurez les options dans la case de groupe de configuration de serveur VPN :Sélectionnez une interface qui reçoit les connexions VPN entrantes dans la liste publique.Sélectionnez une interface qui est l'interface privée dans la liste privée.(*Facultatif*) changez la priorité que l'ASA a dans la batterie dans la zone de texte prioritaire.Tapez une adresse IP pour le Traduction d'adresses de réseau (NAT) assigné l'adresse IP si ce périphérique est derrière un Pare-feu qui utilise NAT.
4. Répétez les étapes sur toutes les ASA participantes dans le groupe.

L'exemple dans cette section utilise ces commandes CLI de configurer l'Équilibrage de charge :

```
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
```

Surveillance

La surveillance choisie **> comporte > VPN > des chargements de statistiques > de batterie VPN** pour surveiller la caractéristique d'Équilibrage de charge sur l'ASA.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **affichez l'Équilibrage de charge de vpn** — Vérifie la caractéristique d'Équilibrage de charge 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
```

Dépannez

Utilisez cette section pour dépanner votre configuration.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **mettez au point le vpnlb 250** — Utilisé pour dépanner la caractéristique d'Équilibrage de charge 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]
```

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems