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 attribué des adresses IP à vos ASA et configuré la passerelle par défaut.
- IPsec est configuré sur les ASA pour les utilisateurs du client VPN.
- Les utilisateurs VPN peuvent se connecter à tous les ASA à l'aide de leur adresse IP publique attribuée individuellement.

Clients éligibles

L'équilibrage de charge n'est efficace que sur les sessions distantes initiées avec ces clients :

- Client VPN Cisco (version 3.0 ou ultérieure)
- Client matériel Cisco VPN 3002 (version 3.5 ou ultérieure)
- CiscoASA 5505 en tant que client Easy VPN

Tous les autres clients, y compris les connexions LAN à LAN, peuvent se connecter à un dispositif de sécurité sur lequel l'équilibrage de charge est activé, mais ils ne peuvent pas participer à l'équilibrage de charge.

Components Used

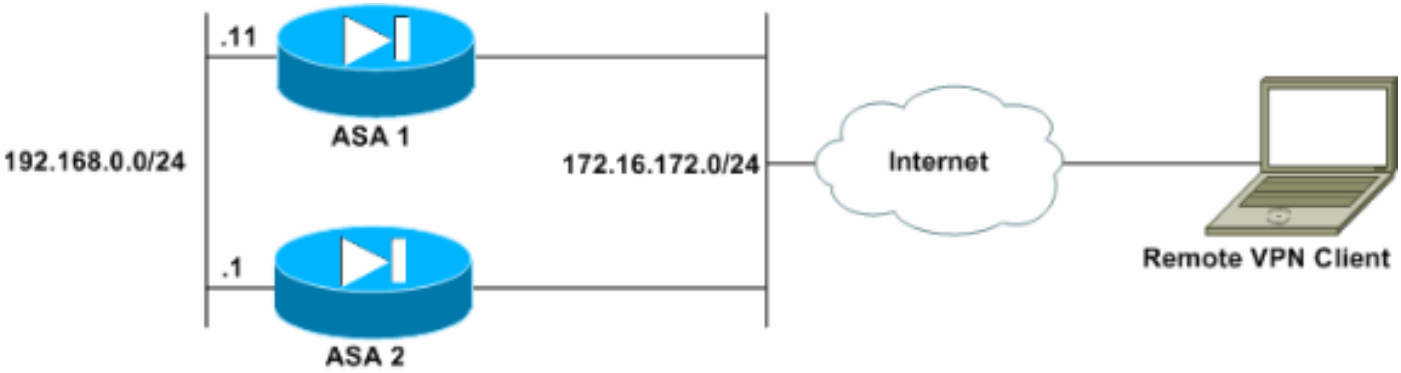
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel client VPN versions 4.6 et ultérieures
- Logiciel Cisco ASA versions 7.0.1 et ultérieures**Remarque :** étend la prise en charge de l'équilibrage de charge aux modèles ASA 5510 et ASA supérieurs à 5520 disposant d'une licence Security Plus avec la version 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.

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

- L'adresse IP du cluster virtuel VPN, le port UDP (User Datagram Protocol) et le secret partagé doivent être identiques sur chaque périphérique du cluster virtuel.
- Tous les périphériques du cluster virtuel doivent se trouver sur les mêmes sous-réseaux IP

internes et externes.

Configuration

Attribution d'une adresse IP

Assurez-vous que les adresses IP sont configurées sur les interfaces externe et interne et que vous pouvez accéder à Internet à partir de votre ASA.

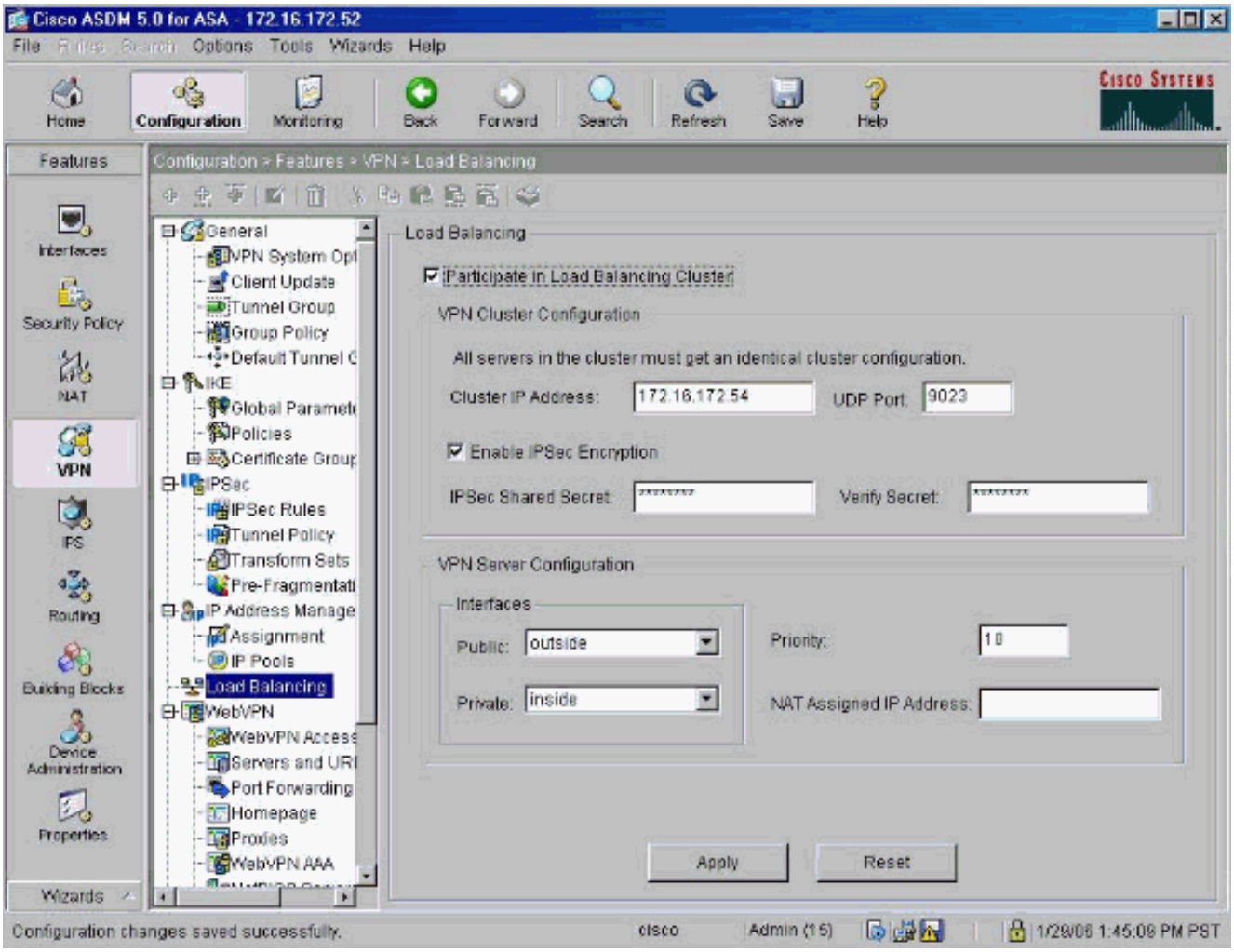
Remarque : assurez-vous que ISAKMP est activé sur l'interface interne et externe. Sélectionnez **Configuration > Features > VPN > IKE > Global Parameters** afin de vérifier ceci.

Configuration du cluster

Cette procédure montre comment utiliser Cisco Adaptive Security Device Manager (ASDM) pour configurer l'équilibrage de charge.

Remarque : De nombreux paramètres de cet exemple ont des valeurs par défaut.

1. Sélectionnez **Configuration > Features > VPN > Load Balancing**, puis cochez **Participer au cluster Load Balancing** pour activer l'équilibrage de charge VPN.



2. Complétez ces étapes pour configurer les paramètres de tous les ASA participant au cluster dans la zone VPN Cluster Configuration Group :Tapez l'adresse IP du cluster dans la zone

de texte Adresse IP du cluster.Cliquez sur **Activer le chiffrement IPSec**.Tapez la clé de chiffrement dans la zone de texte Secret partagé IPSec et saisissez-la à nouveau dans la zone de texte Vérifier le secret.

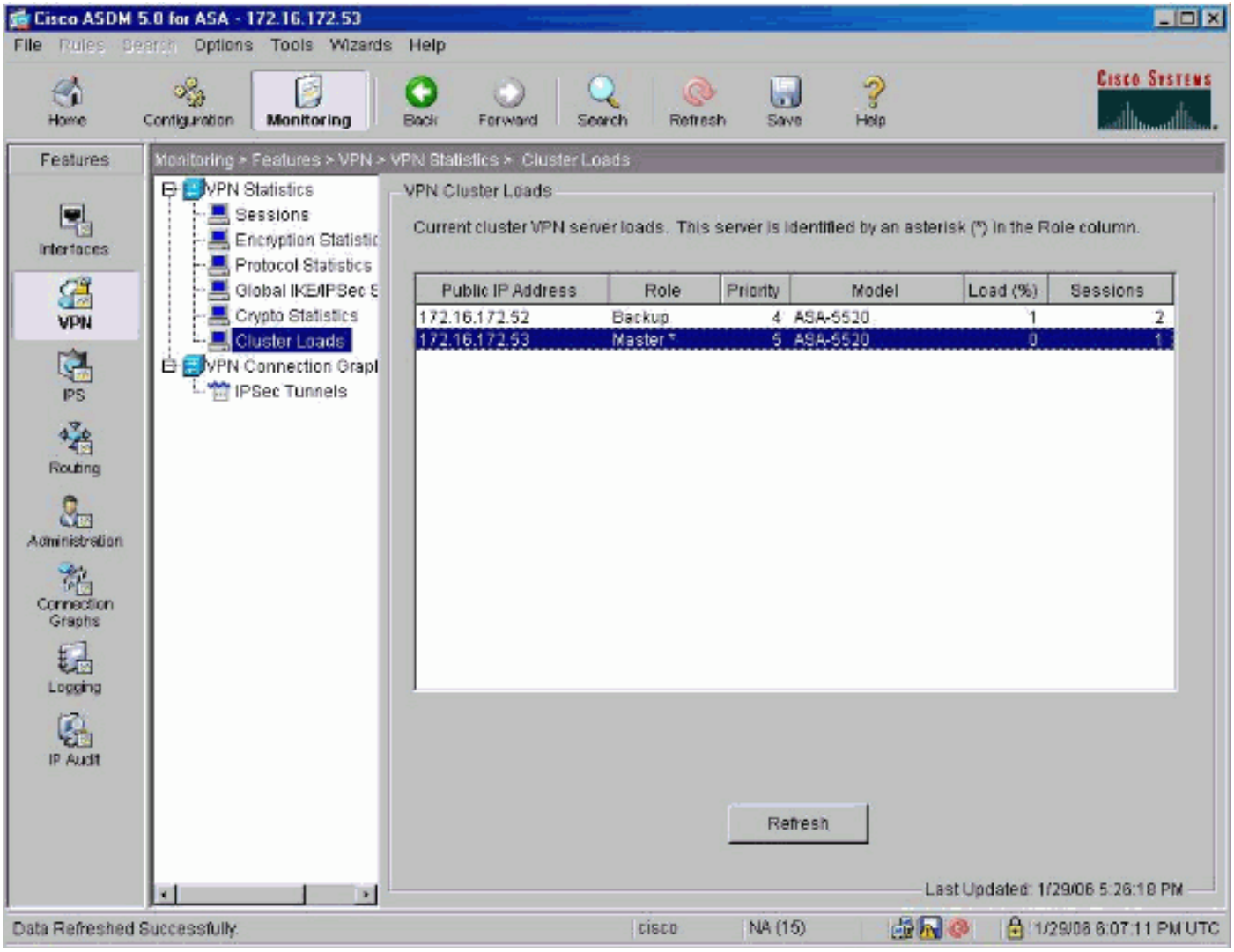
3. Configurez les options dans la zone VPN Server Configuration group :Sélectionnez une interface qui accepte les connexions VPN entrantes dans la liste Public.Sélectionnez une interface privée dans la liste Privée.(*Facultatif*) Modifiez la priorité de l'ASA dans le cluster dans la zone de texte Priorité.Tapez une adresse IP pour l'adresse IP attribuée à la traduction d'adresses de réseau (NAT) si ce périphérique se trouve derrière un pare-feu qui utilise la NAT.
4. Répétez les étapes sur tous les ASA participants du groupe.

L'exemple de cette section utilise ces commandes CLI pour 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

Sélectionnez **Monitoring > Features > VPN > VPN Statistics > Cluster Loads** pour surveiller la fonctionnalité d'équilibrage de charge sur l'ASA.



Vérification

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 .**

- **show vpn load-équilibrage** - Vérifie la fonctionnalité 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
```

Dépannage

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 : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug vpnlb 250** - Utilisé pour dépanner la fonctionnalité 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