

Processus de sélection du directeur de l'équilibrage de charge VPN ASA

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Algorithme d'équilibrage de charge](#)

[Processus d'élection du directeur](#)

[Mise en garde pour les scénarios de redémarrage](#)

[Processus de réélection du directeur](#)

[Périphérique Director supprimé du cluster](#)

[Le périphérique Director ne répond pas aux messages Hello des membres du cluster](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit le processus de sélection du directeur dans un scénario d'équilibrage de charge VPN avec le dispositif de sécurité adaptatif (ASA) de la gamme Cisco 5500-X.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur le Cisco ASA 5500-X qui exécute le logiciel version 9.2.

Note: Ce document s'applique également à toutes les versions logicielles, depuis que la fonctionnalité a été introduite pour la première fois dans la version 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.

Informations générales

L'équilibrage de charge VPN est un mécanisme utilisé afin de répartir équitablement le trafic réseau entre les périphériques d'un cluster virtuel. L'équilibrage de charge repose sur une distribution simple ; il ne tient pas compte de l'utilisation du débit ni d'autres facteurs. Un cluster d'équilibrage de charge se compose de deux ou plusieurs périphériques, un directeur et un ou plusieurs périphériques secondaires, et ces périphériques n'ont pas besoin d'être configurés de manière identique.

Algorithme d'équilibrage de charge

Voici une présentation de l'algorithme d'équilibrage de charge :

- Le périphérique directeur tient à jour une liste triée des membres du cluster secondaire dans l'ordre croissant des adresses IP internes.
- La charge est calculée sous la forme d'un pourcentage entier (nombre de sessions actives/maximum) fourni par chaque membre de cluster secondaire.
- Le périphérique directeur redirige le tunnel VPN IPSec/Secure Sockets Layer (SSL) vers un périphérique ayant la charge la plus faible en premier, jusqu'à ce qu'il soit supérieur d'un pour cent aux autres périphériques.
- Le périphérique directeur se redirige vers lui-même uniquement lorsque tous les membres du cluster secondaire sont supérieurs de 1 % à celui du périphérique directeur.

Voici un exemple avec un directeur et deux membres de cluster secondaires :

- Tous les noeuds commencent par une charge de zéro pour cent, et tous les pourcentages sont arrondis au demi pour cent le plus proche.
- Le périphérique directeur prend la connexion si tous les membres ont une charge supérieure de 1 % à celle du périphérique directeur.
- Si le périphérique directeur ne prend pas la connexion, la session est prise par le périphérique de sauvegarde qui a actuellement le plus faible pourcentage de charge.
- Si tous les membres ont le même pourcentage de charge, alors le périphérique de sauvegarde avec le moins de sessions prend la session.
- Si tous les membres ont le même pourcentage de charge et le même nombre de sessions, alors le périphérique de sauvegarde avec le moins d'adresses IP prend la session.

Processus d'élection du directeur

Le processus de sélection du directeur de l'équilibrage de charge VPN est exécuté sur le cluster externe au réseau. Il existe deux types de données échangées sur le réseau externe :

- Les paquets ARP (Address Resolution Protocol) pour l'adresse IP du cluster qui sont utilisés pour la découverte du directeur sont échangés. Le nombre maximal de paquets ARP envoyés pour l'adresse IP du cluster afin de découvrir le directeur est le suivant :

(10 - priorité) + 1

Ici, *priority* est configuré comme dans la sous-commande **priority** de la commande CLI **d'équilibrage de charge vpn**.

- Des paquets UDP sur l'extérieur pour les messages de requête/réponse Hello sont échangés. Le numéro de port est spécifié dans la sous-commande **cluster port** load-équilibrage et est par défaut **9023**.

Par exemple, si la *priorité* est cinq pour un périphérique d'équilibrage de charge, il tente d'envoyer jusqu'à six paquets ARP afin de voir si un périphérique directeur possède l'adresse IP du cluster. Si un périphérique directeur est détecté, l'ASA n'envoie plus de messages ARP et attend 15 secondes avant d'envoyer la requête Hello UDP. Le périphérique directeur répond ensuite par une réponse Hello UDP.

Mise en garde pour les scénarios de redémarrage

Dans une situation de redémarrage avec deux ASA dans un cluster d'équilibrage de charge :

- ASA-1 ou ASA-2 était le directeur avant le redémarrage.
- ASA-1 est redémarré.
- ASA-2 devient le directeur s'il n'était pas le directeur auparavant.
- ASA-1 rejoint simplement le cluster en tant que membre après le redémarrage.

L'algorithme d'équilibrage de charge peut être affecté par une configuration du commutateur sur lequel l'interface externe des périphériques du cluster est également connectée. Par exemple, un algorithme Spanning Tree peut provoquer un retard de connectivité lorsque le périphérique connecté au commutateur est redémarré.

Astuce : La commande [spanning-tree port fast](#) permet d'accélérer le processus.

Dans certains cas, un ASA récemment redémarré dont l'équilibrage de charge est activé peut tenter de devenir le périphérique directeur (même s'il existe déjà un périphérique directeur) parce qu'il ne peut pas atteindre le périphérique directeur actuel en raison d'un retard de connectivité dans le commutateur. Lorsqu'un conflit de direction est détecté à la suite d'une collision ARP, l'ASA avec une adresse MAC (Media Access Control) faible gagne, tandis que l'ASA avec une adresse MAC plus élevée abandonne le rôle de périphérique directeur.

Processus de réélection du directeur

Deux situations entraînent la réélection du périphérique directeur.

Périphérique Director supprimé du cluster

Lorsque vous désactivez la fonctionnalité sur l'ASA, un message de diffusion est envoyé à tous

les membres du cluster afin d'informer la modification, et le [processus de sélection](#) précédemment décrit est exécuté.

Le périphérique Director ne répond pas aux messages Hello des membres du cluster

Si le périphérique directeur ne répond pas à un message Hello de membre de cluster, il faut environ 20 secondes à un membre de cluster ASA pour détecter que le directeur n'est plus présent. Les messages Hello sont envoyés toutes les cinq secondes (non configurables). Si les membres du cluster ne reçoivent pas de réponse du périphérique directeur après quatre messages Hello, le processus de sélection est déclenché.

Dépannage

Note: Reportez-vous à l'article [Informations importantes sur les commandes de débogage](#) de Cisco avant d'utiliser les commandes **de débogage**.

Ces commandes de débogage peuvent être utiles lors de tentatives de dépannage de problèmes avec votre système :

- **debug fsm 255** - Utilisez cette commande afin d'activer le débogage général de Finite State Machine. Entrez la commande **no debug all** afin de désactiver.
- **debug menu vpnlb 3** - Utilisez cette commande afin d'activer la trace de débogage d'équilibrage de charge VPN. Entrez de nouveau la commande **debug menu vpnlb 3** afin de désactiver.
- **debug menu vpnlb 4** - Utilisez cette commande afin d'activer la trace de la fonction d'équilibrage de charge VPN. Entrez de nouveau la commande **debug menu vpnlb 4** afin de désactiver.

Informations connexes

- [Compréhension de l'équilibrage de charge](#)
- [Support et documentation techniques - Cisco Systems](#)