



Haute disponibilité

- Options de haute disponibilité, à la page 1
- Équilibrage de la charge VPN, à la page 3

Options de haute disponibilité

Distributed VPN Clustering (Mise en grappe VPN distribuée), Load balancing (Équilibrage de charge) et Failover (Basculement) sont des fonctionnalités de haute disponibilité qui fonctionnent différemment et ont des exigences différentes. Dans certains cas, vous pouvez utiliser plusieurs capacités dans votre déploiement. Les sections suivantes décrivent ces fonctionnalités. Reportez-vous à la version appropriée du [Guide de configuration ASDM pour les opérations générales d'ASA](#) pour en savoir plus sur Distributed VPN (VPN distribué) et Failover (Basculement). Les détails de l'équilibrage de la charge sont inclus ici.

VPN et mise en grappe sur le châssis Cisco Secure Firewall eXtensible Operating System (FXOS)

Une grappe ASA FXOS prend en charge l'un des deux modes mutuellement exclusifs pour le VPN de S2S, centralisé ou distribué :

- Mode VPN centralisé. Le mode par défaut. En mode centralisé, les connexions VPN sont établies avec l'unité de commande de grappe uniquement.

La fonctionnalité VPN est limitée à l'unité de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si l'unité de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues et les utilisateurs connectés au VPN subissent une interruption de service. Lorsqu'une nouvelle unité de contrôle est choisie, vous devez rétablir les connexions VPN.

Lorsque vous connectez un tunnel VPN à une adresse d'interface étendue, les connexions sont automatiquement transférées à l'unité de contrôle. Les clés et les certificats VPN sont répliqués sur toutes les unités.

- Mode de VPN distribué. Dans ce mode, les connexions VPN S2S IPsec IKEv2 sont réparties sur les membres d'une grappe ASA, ce qui offre une grande évolutivité. La distribution des connexions VPN entre les membres d'une grappe permet d'utiliser pleinement la capacité et le débit de la grappe, ce qui augmente considérablement la prise en charge des VPN au-delà des capacités VPN centralisées.

**Remarque**

Le mode de mise en grappe VPN centralisée prend en charge S2S IKEv1 et S2S IKEv2.

Le mode de mise en grappe du VPN distribué prend uniquement en charge S2S, IKEv2.

Le mode de mise en grappe du VPN distribué est pris en charge sur le Firepower 9300 uniquement.

Le VPN d'accès à distance n'est pas pris en charge en mode de mise en grappe de VPN centralisé ou distribué.

Équilibrage de la charge VPN

L'équilibrage de charge VPN est un mécanisme permettant de distribuer équitablement le trafic VPN d'accès à distance entre les périphériques d'un groupe d'équilibrage de charge VPN. L'équilibrage de charge VPN est basé sur une répartition simple du trafic sans prendre en compte le débit ou d'autres facteurs. Un groupe d'équilibrage de la charge VPN se compose d'au moins deux périphériques. L'un des périphériques sert de directeur et les autres périphériques sont des périphériques membres. Il n'est pas nécessaire que les périphériques d'un groupe soient exactement du même type ou aient des versions de logiciels ou des configurations identiques.

Tous les périphériques actifs dans un groupe d'équilibrage de la charge VPN transportent des charges de session. L'équilibrage de charge VPN dirige le trafic vers le périphérique le moins chargé du groupe, distribuant la charge sur tous les périphériques. Il utilise efficacement les ressources système et offre des performances accrues et une disponibilité élevée.

Basculement

Une configuration de basculement nécessite deux ASA identiques connectés l'un à l'autre par une liaison de basculement dédiée et, éventuellement, une liaison de basculement avec état. L'intégrité des unités actives et des interfaces est surveillée pour déterminer si les conditions spécifiques au basculement sont respectées. Si ces conditions sont remplies, le basculement se produit. Le basculement prend en charge les configurations VPN et pare-feu.

L'ASA prend en charge deux configurations de basculement : basculement actif/actif et basculement actif/en veille.

Avec le basculement actif/actif, les deux unités peuvent transmettre le trafic réseau. Il ne s'agit pas d'un véritable équilibrage de charge, bien qu'il puisse sembler avoir le même effet. En cas de basculement, l'unité active restante prend le relais en transmettant le trafic combiné, en fonction des paramètres configurés. Par conséquent, lors de la configuration du basculement actif/actif, vous devez vous assurer que le trafic combiné des deux unités demeure dans la capacité de chacune.

Avec le basculement actif/en veille, une seule unité transmet le trafic, tandis que l'autre attend en état de veille et ne transmet pas de trafic. Le basculement actif/en veille vous permet d'utiliser un second ASA pour prendre le relais des fonctions d'une unité défaillante. Lorsque l'unité active tombe en panne, elle passe à l'état de veille, tandis que l'unité en veille passe à l'état actif. L'unité qui devient active adopte les adresses IP (ou, pour le pare-feu transparent, l'adresse IP de gestion) et les adresses MAC de l'unité défaillante et commence à transmettre le trafic. L'unité maintenant en veille reprend les adresses IP de veille de l'unité active. En cas de défaillance d'une unité active, l'unité en veille prend le relais sans interruption du tunnel VPN client.

Équilibrage de la charge VPN

À propos de l'équilibrage de charge VPN

Si vous avez une configuration client distant dans laquelle vous utilisez deux périphériques de sécurité adaptables Cisco ou plus connectés au même réseau pour gérer les sessions à distance, vous pouvez configurer ces périphériques pour partager leur charge de session en créant un groupe d'équilibrage de charge VPN. L'équilibrage de charge VPN dirige le trafic vers le périphérique le moins chargé du groupe, distribuant la charge sur tous les périphériques. Il utilise efficacement les ressources système et offre des performances accrues et une disponibilité élevée.

Tous les périphériques d'un groupe d'équilibrage de charge VPN transportent des charges de session. Un périphérique du groupe, le *directeur*, dirige les demandes de connexion entrantes vers les autres périphériques, appelés *périphériques membres*. Le directeur surveille tous les périphériques du groupe, suit le niveau de charge de chaque périphérique et répartit la charge de session en conséquence. Le rôle de directeur n'est pas lié à un appareil physique; il peut se déplacer entre les périphériques. Par exemple, si le directeur actuel tombe en panne, l'un des périphériques membres du groupe assume ce rôle et devient immédiatement le nouveau directeur.

Le groupe d'équilibrage de charges VPN apparaît aux clients externes comme une adresse IP virtuelle unique. Cette adresse IP n'est pas liée à un périphérique physique particulier. Elle appartient au directeur actuel. Un client VPN qui tente d'établir une connexion se connecte d'abord à l'adresse IP virtuelle. Le directeur renvoie ensuite au client l'adresse IP publique de l'hôte disponible le moins chargé du groupe. Dans une deuxième transaction (transparente pour l'utilisateur), le client se connecte directement à cet hôte. De cette manière, le directeur de groupe d'équilibrage de charge du VPN dirige le trafic de manière uniforme et efficace entre les ressources.

En cas de défaillance d'un ASA dans le groupe, les sessions interrompues peuvent se reconnecter immédiatement à l'adresse IP virtuelle. Le directeur dirige ensuite ces connexions vers un autre périphérique actif du groupe. Si le directeur tombe en panne, un périphérique membre du groupe prend immédiatement et automatiquement le relais en tant que nouveau directeur. Même en cas de défaillance de plusieurs périphériques du groupe, les utilisateurs peuvent continuer à se connecter au groupe tant qu'un périphérique du groupe est opérationnel et disponible.

Pour chaque périphérique de grappe d'équilibrage de charge VPN, vous devez configurer les interfaces publiques/externes (lbpublic) et privées/internes (lbprivate).

- Interface publique : interface externe du périphérique utilisée pour la communication initiale avec l'adresse IP de la grappe. Cette interface est utilisée pour l'établissement de liaison Hello.
- Interface privée : interface interne du périphérique utilisée pour la messagerie entre les membres de la grappe d'équilibrage de charge. Ces messages comprennent des messages keepalive, des messages de topologie et des messages de hors-service liés à l'équilibrage de charge.

Algorithme d'équilibrage de charge VPN

Le directeur de groupe d'équilibrage de charge VPN conserve une liste triée des membres du groupe dans l'ordre croissant des adresses IP. La charge de chaque membre est calculée sous la forme d'un pourcentage entier (le nombre de sessions actives). Les sessions inactives Secure Client ne sont pas prises en compte dans la charge VPN SSL pour l'équilibrage de charge VPN. Le directeur redirige les tunnels IPsec et SSL vers le

périphérique ayant la charge la plus faible jusqu'à ce qu'il soit de 1 % supérieur à celui des autres. Lorsque tous les membres sont supérieurs de 1 % au directeur, le directeur redirige le trafic vers lui-même.

Par exemple, si vous avez un directeur et deux membres, le cycle suivant s'applique :



Remarque Tous les nœuds commencent par 0 %, et tous les pourcentages sont arrondis à la moitié.

1. Le directeur établit la connexion si tous les membres ont une charge de 1 % supérieure à celle du directeur.
2. Si le directeur ne prend pas la connexion, la session est prise en charge par le périphérique membre ayant le pourcentage de charge le plus bas.
3. Si tous les membres ont le même pourcentage de charge, le membre ayant le moins de sessions obtient la session.
4. Si tous les membres ont le même pourcentage de charge et le même nombre de sessions, le membre ayant l'adresse IP la plus basse obtient la session.

Configurations de groupes d'équilibrage de charge VPN

Un groupe d'équilibrage de charge VPN peut être composé de l'ASA de la même version ou de versions mixtes sous réserve des restrictions suivantes :

- Les groupes d'équilibrage de charge VPN qui se composent des deux mêmes versions ASA peuvent exécuter l'équilibrage de charge VPN pour un mélange de sessions IPsec, Secure Client et de VPN SSL sans client.
- Les groupes d'équilibrage de charge VPN qui comprennent des versions mixtes de l'ASA peuvent prendre en charge les sessions IPsec. Dans une telle configuration, cependant, les ASA peuvent ne pas atteindre leur pleine capacité IPsec.

Le directeur du groupe attribue des demandes de session aux membres du groupe. L'ASA considère toutes les sessions, SSL VPN ou IPsec, comme égales, et les affecte en conséquence. Vous pouvez configurer le nombre de sessions VPN IPsec et SSL à autoriser, jusqu'au nombre maximal autorisé par votre configuration et votre licence.

Nous avons testé jusqu'à 10 nœuds dans un groupe d'équilibrage de charge VPN. Des groupes plus importants peuvent fonctionner, mais nous ne prenons pas en charge publiquement ces topologies.

Élection du directeur d'équilibrage de charge VPN

Processus d'élection du directeur

Chaque non-maître dans la grappe virtuelle gère une base de données de topologie locale. Cette base de données est mise à jour par le maître chaque fois que la topologie de la grappe est modifiée. Chaque non-maître passe à l'état d'élection de maître lorsqu'aucune réponse Hello n'est reçue du maître ou qu'aucune réponse keepalive n'est reçue du maître après un nombre maximal de tentatives.

Le membre effectue les fonctions suivantes pendant l'élection du directeur :

- Compare la priorité de chaque unité d'équilibrage de charge trouvée dans la base de données de topologie locale.

- Si deux unités ayant la même priorité sont trouvées, celle ayant l'adresse IP la plus basse est choisie.
- Si le membre lui-même est choisi, il réclame l'adresse IP virtuelle.
- Si l'un des autres membres est choisi, le membre envoie une demande Hello au maître choisi.
- Lorsque deux unités membres tentent de réclamer l'adresse IP virtuelle, le sous-système ARP détecte la condition d'adresse IP en double et envoie une notification pour demander au membre ayant l'adresse MAC la plus élevée d'abandonner le rôle de directeur.

Établissement de liaison Hello

Chaque membre envoie une demande Hello à l'adresse IP de la grappe virtuelle sur l'interface externe au démarrage. Si une demande Hello est reçue, le maître envoie sa propre demande Hello au membre. Le membre non-directeur renvoie une réponse Hello à la réception d'une demande Hello du directeur. Cela met fin à l'établissement de liaison Hello.

Une fois l'établissement de liaison Hello terminé, la connexion est lancée sur l'interface interne si le chiffrement est configuré. Si aucune réponse Hello n'est reçue par le membre après un nombre maximal de tentatives, le membre passe à l'état d'élection de maître.

Messages Keepalive

Une fois l'établissement de liaison Hello effectué entre un membre et le directeur, chaque unité membre envoie des demandes keepalive périodiques au maître avec ses informations de charge. Les demandes keepalive sont envoyées par une unité membre à des intervalles d'une seconde pendant le traitement normal s'il n'y a aucune réponse keepalive en attente du directeur. Cela signifie que la prochaine demande keepalive est envoyée la seconde suivante, tant que les réponses keepalive de la demande précédente ont été reçues. Si le membre n'a pas reçu de réponse keepalive du directeur pour la demande keepalive précédente, aucune demande keepalive n'est envoyée la seconde suivante. Au lieu de cela, la logique de délai d'expiration keepalive du membre démarre.

Le délai d'expiration keepalive fonctionne comme suit :

1. Si un membre attend une réponse keepalive du directeur, le membre n'envoie pas la demande keepalive normale d'une seconde.
2. Le membre attend pendant 3 secondes et envoie une demande keepalive à la 4e seconde.
3. Le membre répète l'étape 2 ci-dessus cinq (5) fois tant qu'il n'y a pas de réponse keepalive du directeur.
4. Ensuite, le membre déclare le directeur comme parti et commence un nouveau cycle d'élection de directeur.

Foire aux questions sur l'équilibrage de charge VPN

- [Mode contexte multiple](#)
- [Épuisement de l'ensemble d'adresses IP](#)
- [Ensembles d'adresses IP uniques](#)
- [Utilisation de l'équilibrage de la charge et du basculement VPN sur le même périphérique](#)
- [Équilibrage de la charge VPN sur plusieurs interfaces](#)
- [Nombre maximal de sessions simultanées pour les groupes d'équilibrage de la charge VPN](#)

Mode contexte multiple

- Q.** L'équilibrage de la charge VPN est-il pris en charge en mode de contexte multiple?
- A.** Ni l'équilibrage de la charge VPN ni le basculement avec état ne sont pris en charge en mode de contexte multiple.

Épuisement de l'ensemble d'adresses IP

- Q.** L'ASA prend-elle en compte l'épuisement de l'ensemble d'adresses IP dans le cadre de sa méthode d'équilibrage de la charge VPN?
- A.** Non. Si la session VPN d'accès à distance est dirigée vers un périphérique qui a épuisé ses ensembles d'adresses IP, la session ne s'établit pas. L'algorithme d'équilibrage de la charge est basé sur la charge et est calculé comme un pourcentage entier (nombre de sessions actives et nombre maximal) que chaque membre fournit.

Ensembles d'adresses IP uniques

- Q.** Pour mettre en œuvre l'équilibrage de la charge VPN, les ensembles d'adresses IP pour les clients Secure Client ou IPsec sur différents ASA doivent-ils être uniques?
- A.** Oui. Les ensembles d'adresses IP doivent être uniques pour chaque périphérique.

Utilisation de l'équilibrage de la charge et du basculement VPN sur le même périphérique

- Q.** Un seul périphérique peut-il utiliser à la fois l'équilibrage de la charge et le basculement VPN?
- A.** Oui. Dans cette configuration, le client se connecte à l'adresse IP du groupe et est redirigé vers l'appareil de sécurité adaptable Cisco le moins chargé dans le groupe. Si ce périphérique tombe en panne, l'unité de secours prend le relais immédiatement et il n'y a aucune incidence sur le tunnel VPN.

Équilibrage de la charge VPN sur plusieurs interfaces

- Q.** Si nous activons le VPN SSL sur plusieurs interfaces, est-il possible de mettre en œuvre l'équilibrage de la charge VPN pour les deux interfaces?
- A.** Vous ne pouvez définir qu'une seule interface pour participer au groupe d'équilibrage de charge VPN en tant qu'interface publique. L'objectif est d'équilibrer les charges de processeur. Plusieurs interfaces convergent sur le même processeur, de sorte que le concept d'équilibrage de la charge VPN sur plusieurs interfaces n'améliorera pas les performances.

Nombre maximal de sessions simultanées pour les groupes d'équilibrage de la charge VPN

- Q.** Envisagez un déploiement de deux Firepower 1150, chacun avec une licence VPN SSL de 100 utilisateurs. Dans un groupe d'équilibrage de charge VPN, le nombre total maximal d'utilisateurs autorise-t-il

200 sessions simultanées, ou seulement 100 ? Si nous ajoutons un troisième périphérique ultérieurement avec une licence pour 100 utilisateurs, pouvons-nous prendre en charge 300 sessions simultanées?

- A. Avec l'équilibrage de charge VPN, tous les périphériques sont actifs, de sorte que le nombre maximal de sessions que votre groupe peut prendre en charge est le nombre total de sessions pour chacun des périphériques du groupe, dans ce cas 300.

Licences pour l'équilibrage de charge VPN

L'équilibrage de charges VPN nécessite une licence de cryptage renforcé (3DES/AES). L'ASA vérifie l'existence de cette licence de chiffrement avant d'activer l'équilibrage de charges VPN. S'il ne détecte pas de licence 3DES ou AES active, l'ASA empêche l'activation de l'équilibrage de charge VPN et empêche également la configuration interne de 3DES par le système d'équilibrage de charge VPN, à moins que la licence ne le permette.

Conditions préalables à l'équilibrage de la charge VPN

Veuillez consulter également les [Directives et limites pour l'équilibrage de charge VPN](#), à la page 7.

- L'équilibrage de charge VPN est désactivé par défaut. Vous devez activer explicitement l'équilibrage de charge VPN.
- Vous devez d'abord configurer les interfaces publique (externe) et privée (interne). Les références ultérieures dans cette section utilisent les noms outside et inside.

Pour ce faire, accédez à **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces**.

- Vous devez avoir préalablement configuré l'interface à laquelle l'adresse IP virtuelle fait référence. Établissez une adresse IP virtuelle commune, un port UDP (si nécessaire) et un secret partagé IPsec pour le groupe.
- Tous les périphériques qui font partie d'un groupe doivent partager les mêmes valeurs propres à la grappe : adresse IP, paramètres de chiffrement, clé de chiffrement et port.
- Pour utiliser le chiffrement de groupe d'équilibrage de charge VPN, activez d'abord IKEv1 sur l'interface interne à l'aide de la commande **crypto ikev1 enable**, avec l'interface interne spécifiée ; sinon, vous obtiendrez un message d'erreur lorsque vous tenterez de configurer le chiffrement de groupe d'équilibrage de charge VPN.
- La fonctionnalité d'autorité de certification locale n'est pas prise en charge si vous utilisez le basculement avec état actif/actif ou l'équilibrage de charge VPN. L'autorité de certification locale ne peut pas être subordonnée à une autre autorité de certification ; elle ne peut servir que d'autorité de certification racine.

Directives et limites pour l'équilibrage de charge VPN

Clients admissibles

L'équilibrage de charge VPN est efficace uniquement pour les sessions distantes lancées avec les clients suivants :

- Secure Client (version 3.0 et ultérieure)

- ASA 5505 (en tant que client VPN facile)
- Firepower 1010 (en tant que client VPN facile)
- Périphériques clients IOS EZVPN prenant en charge la redirection IKE (IOS 831/871)

Points à considérer

L'équilibrage de charge VPN fonctionne avec les clients IPsec et les sessions client VPN SSL. Tous les autres types de connexion VPN (L2TP, PPTP, L2TP/IPsec), y compris les connexions de site à site, peuvent se connecter à un ASA sur lequel l'équilibrage de charge VPN est activé, mais ils ne peuvent pas participer à l'équilibrage de charge VPN.

Lorsque plusieurs nœuds ASA sont regroupés pour l'équilibrage de charge et que l'utilisation des URL de groupe est souhaitée pour les connexions Secure Client, les nœuds ASA individuels doivent :

- Configurez chaque profil de connexion d'accès à distance avec une URL de groupe pour chaque adresse virtuelle d'équilibrage de charge VPN (IPv4 et IPv6).
- Configurez une URL de groupe pour l'adresse publique d'équilibrage de charge VPN de ce nœud.

Groupes d'équilibrage de charge

L'ASA prend en charge 10 périphériques par groupe d'équilibrage de charge VPN.

Mode contextuel

L'équilibrage de charge VPN n'est pas pris en charge en mode de contexte multiple.

FIPS

Le chiffrement de grappe n'est pas pris en charge avec FIPS.

Vérification du certificat

Lors de la vérification du certificat pour l'équilibrage de charge VPN avec Secure Client, si la connexion est redirigée par une adresse IP, le client effectue toutes ses vérifications de nom à l'aide de cette adresse IP. Assurez-vous que l'adresse IP de redirection est répertoriée dans le nom commun des certificats ou le nom alternatif du sujet. Si l'adresse IP n'est pas présente dans ces champs, le certificat sera considéré comme non fiable.

Suivant les directives définies dans la RFC 2818, si un **subject alt name** (nom alternatif du sujet) est inclus dans le certificat, nous utilisons uniquement le **subject alt name** (nom alternatif du sujet) pour les vérifications de nom, et nous ignorons le nom commun. Assurez-vous que l'adresse IP du serveur présentant le certificat est définie dans le **subject alt name** (nom alternatif du sujet) du certificat.

Pour un ASA autonome, l'adresse IP est l'adresse IP de cet ASA. Dans une situation de groupe d'équilibrage de charge VPN, cela dépend de la configuration du certificat. Si le groupe utilise un seul certificat, celui-ci doit comporter des extensions SAN pour l'adresse IP virtuelle et le FQDN du groupe, et doit contenir des extensions Subject Alternative Name incluant l'adresse IP et le FQDN de chaque ASA. Si le groupe utilise plusieurs certificats, le certificat de chaque ASA doit comporter des extensions SAN pour l'adresse IP virtuelle, le FQDN du groupe, ainsi que l'adresse IP et le FQDN de l'ASA concerné.

Équilibrage de charge de VPN géographique

Dans un environnement d'équilibrage de charge VPN géographique où les résolutions DNS sont modifiées à intervalles réguliers, vous devez examiner attentivement la façon de définir la valeur de durée de vie (TTL). Pour que la configuration d'équilibrage de charge DNS fonctionne correctement avec Secure Client, le mappage nom-adresse de l'ASA doit rester identique entre le moment où l'ASA est sélectionné et celui où le tunnel est entièrement établi. Si trop de temps s'écoule avant que les informations d'authentification soient saisies, la recherche redémarre et une adresse IP différente peut devenir l'adresse résolue. Si le mappage DNS passe à un autre ASA avant la saisie des informations d'authentification, le tunnel VPN échoue.

L'équilibrage de charge géographique pour le VPN utilise souvent un sélecteur de site global Cisco (GSS). Le GSS utilise DNS pour l'équilibrage de charge, et la valeur de durée de vie (TTL) pour la résolution DNS est par défaut de 20 secondes. Vous pouvez réduire considérablement la probabilité d'échecs de connexion si vous augmentez la valeur TTL sur le GSS. L'augmentation à une valeur beaucoup plus élevée permet de disposer de suffisamment de temps pour la phase d'authentification lorsque l'utilisateur saisit les informations d'authentification et établit le tunnel.

Pour augmenter le temps de saisie des informations d'authentification, vous pouvez également envisager de désactiver la connexion au démarrage.

Associations de sécurité IKE/IPSec

Les sessions de chiffrement de grappe ne se synchronisent pas en mode veille dans une topologie d'équilibreur de charge VPN.

Configuration de l'équilibrage de charge du VPN

Si vous avez une configuration client distant dans laquelle vous utilisez deux périphériques ASA ou plus connectés au même réseau pour gérer les sessions à distance, vous pouvez configurer ces périphériques pour partager leur charge de session. L'équilibrage de charge VPN dirige le trafic de session vers le périphérique le moins chargé du groupe, distribuant la charge sur tous les périphériques. L'équilibrage de charge VPN utilise efficacement les ressources système et offre des performances accrues et une disponibilité élevée.

Pour utiliser l'équilibrage de charge VPN, procédez comme suit sur chaque périphérique du groupe :

- Configurez le groupe d'équilibrage de charge VPN en établissant des attributs de groupe d'équilibrage de charge VPN communs. Cela inclut une adresse IP virtuelle, un port UDP (si nécessaire) et un secret partagé IPsec pour le groupe. Tous les participants du groupe doivent avoir une configuration de groupe identique, à l'exception de la priorité du périphérique dans le groupe.
- Configurez un périphérique participant en activant l'équilibrage de charge VPN sur le périphérique et en définissant les propriétés spécifiques au périphérique. Ces valeurs varient d'un appareil à l'autre.

Configurer l'équilibrage de charge VPN avec l'Assistant Haute disponibilité et évolutivité :

Procédure

- | | |
|----------------|---|
| Étape 1 | Sélectionnez Wizards (Assistants) > High Availability and Scalability Wizard (Assistant de haute disponibilité et d'évolutivité) . |
| Étape 2 | Dans l'écran Configuration Type (Type de configuration), cliquez sur Configure VPN Cluster Load Balancing (Configurer l'équilibrage de charge de la grappe VPN), puis sur Next (Suivant). |

- Étape 3** Choisissez l'adresse IP unique qui représente l'ensemble du groupe d'équilibrage de charge VPN. Précisez une adresse IP qui se trouve dans la plage d'adresses de sous-réseau public partagée par tous les ASA du groupe.
- Étape 4** Précisez le port UDP pour le groupe d'équilibrage de charge VPN auquel ce périphérique participe. La valeur par défaut est 9023. Si une autre application utilise ce port, saisissez le numéro de port de destination UDP que vous souhaitez utiliser pour l'équilibrage de charge VPN.
- Étape 5** Pour activer le chiffrement IPsec et vous assurer que toutes les informations d'équilibrage de charge VPN transmises entre les périphériques sont chiffrées, cochez la case **Enable IPsec Encryption** (Activer le chiffrement IPsec).
- Étape 6** Précisez et vérifiez le **secret partagé IPsec**. La valeur que vous saisissez s'affiche sous forme d'astérisques consécutifs.
- Étape 7** Précisez la priorité attribuée à ce périphérique dans le groupe. La plage est de 1 à 10. La priorité indique la probabilité que ce périphérique devienne le directeur de groupe, soit au démarrage, soit en cas de défaillance d'un directeur existant. Plus la priorité est élevée (par exemple, 10), plus grande est la probabilité que ce périphérique devienne le directeur.
- Remarque**
Si les périphériques du groupe d'équilibrage de charge VPN sont mis sous tension à des moments différents, le premier périphérique mis sous tension adopte le rôle de directeur. Chaque périphérique du groupe vérifie quand il est mis sous tension pour s'assurer que le groupe dispose d'un directeur. S'il n'y en a pas, ce périphérique adopte le rôle. Les périphériques mis sous tension et ajoutés au groupe deviennent ultérieurement des membres du groupe. Si tous les périphériques du groupe sont mis sous tension simultanément, le périphérique dont la priorité est la plus élevée devient le directeur. Si deux périphériques ou plus du groupe sont mis sous tension simultanément et que les deux ont le paramètre de priorité le plus élevé, celui qui a l'adresse IP la plus basse devient le directeur.
- Étape 8** Choisissez **Public Interface of This Device** (Interface publique de ce périphérique).
- Étape 9** Choisissez **Private Interface of This Device** (Interface privée de ce périphérique).
- Étape 10** Cochez la case **Send FQDN to client instead of an IP address when redirecting** (Envoyer le nom de domaine complet au client au lieu d'une adresse IP lors de la redirection) pour que le directeur envoie un nom de domaine complet utilisant l'hôte et le nom de domaine du périphérique au lieu de l'adresse IP externe lors de la redirection des connexions du client VPN vers ce périphérique.
- Étape 11** Cliquez sur **Next** (suivant). Passez en revue votre configuration dans l'écran Summary (Résumé).
- Étape 12** Cliquez sur **Finish** (Terminer).
- La configuration du groupe d'équilibrage de charge VPN est envoyée à l'ASA.

Prochaine étape

Lorsque plusieurs nœuds ASA sont regroupés pour l'équilibrage de la charge et que l'utilisation des URL de groupe est souhaitée pour les connexions Secure Client, les nœuds ASA individuels doivent :

- Configurez chaque profil de connexion d'accès à distance avec une URL de groupe pour chaque adresse virtuelle d'équilibrage de charge VPN (IPv4 et IPv6).
- Configurez une URL de groupe pour l'adresse publique d'équilibrage de charge VPN de ce nœud.

Les URL de groupe sont configurées dans le volet **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Secure Client Connection Profiles (Profils**

de connexion) > *connection profile name (nom du profil de connexion)* > **Add or Edit (Ajouter ou modifier)**
> **Advanced (Avancé)** > **Group Alias / Group URL (Alias de groupe / URL de groupe)**.

Configurer l'équilibrage de charge du VPN (sans l'assistant)

Procédure

-
- Étape 1** Sélectionnez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Load Balancing (Équilibrage de charge)**.
- Étape 2** Cochez **Participate in Load Balancing** (Participer à l'équilibrage de charge) pour indiquer que cet ASA participe à la grappe d'équilibrage de charge.
- Vous devez activer l'équilibrage de charge de cette manière sur chaque ASA qui y participe.
- Étape 3** Configurez les champs suivants dans la zone **VPN Cluster Configuration (Configuration de la grappe VPN)**. Ces valeurs doivent être identiques pour l'ensemble de la grappe virtuelle. Tous les serveurs de la grappe doivent avoir une configuration de grappe identique.
- **Adresse IPv4 de la grappe** : spécifie l'adresse IPv4 unique qui représente l'ensemble de la grappe virtuelle IPv4. Choisissez une adresse IP qui se trouve dans la plage d'adresses du sous-réseau public partagée par tous les ASA de la grappe virtuelle.
 - **Port UDP** : spécifie le port UDP de la grappe virtuelle à laquelle cet appareil participe. La valeur par défaut est 9023. Si une autre application utilise ce port, saisissez le numéro de port de destination UDP que vous souhaitez utiliser pour l'équilibrage de charge.
 - **Cluster IPv6 Address (adresse IP de la grappe)** : spécifie l'adresse IPv6 unique qui représente l'ensemble de la grappe virtuelle IPv6. Choisissez une adresse IP qui se trouve dans la plage d'adresses du sous-réseau public partagée par tous les ASA de la grappe virtuelle. Les clients disposant d'adresses IPv6 peuvent établir des connexions Secure Client au moyen de l'adresse IPv6 publique de la grappe ASA ou d'un serveur GSS. De même, les clients disposant d'adresses IPv6 peuvent établir des connexions VPN Secure Client au moyen de l'adresse IPv4 publique de la grappe ASA ou d'un serveur GSS. L'un ou l'autre type de connexion peut être réparti dans la grappe ASA.
- Remarque**
Dans les champs Cluster IPv4 Address (Adresse IPv4 de la grappe) et Cluster IPv6 Address (Adresse IPv6 de la grappe), vous pouvez également préciser le nom de domaine pleinement qualifié de la grappe virtuelle, à condition qu'un groupe de serveurs DNS soit configuré avec au moins un serveur DNS et que la recherche DNS soit activée sur l'une des interfaces de l'ASA.
- **Enable IPsec Encryption (Activer le chiffrement IPsec)** : active ou désactive le chiffrement IPsec. Si vous cochez cette case, vous devez également préciser et confirmer un secret partagé. Les ASA de la grappe virtuelle communiquent au moyen de tunnels LAN-à-LAN utilisant IPsec. Pour vous assurer que tous les renseignements d'équilibrage de charge échangés entre les périphériques sont chiffrés, cochez cette case.
 - **IPsec Shared Secret (Secret partagé IPsec)** : spécifie le secret partagé entre les homologues IPsec lorsque vous avez activé le chiffrement IPsec. La valeur que vous saisissez dans la zone s'affiche sous forme d'astérisque consécutif.
 - **Verify Secret (vérifier le secret)** : saisir de nouveau le secret partagé. Confirme la valeur du secret partagé saisie dans la zone IPsec Shared Secret (Secret partagé IPsec).

Étape 4 Configurez les champs de la zone **VPN Server Configuration** (Configuration du serveur VPN) pour un ASA spécifique :

- **Interface publique** : spécifie le nom ou l'adresse IP de l'interface publique pour cet appareil.
- **Interface privée** : spécifie le nom ou l'adresse IP de l'interface privée pour cet appareil.
- **Priorité** : spécifie la priorité affectée à cet appareil dans la grappe. La plage est de 1 à 10. La priorité indique la probabilité que ce périphérique devienne le maître virtuel de la grappe, soit au démarrage, soit en cas d'échec d'un maître existant. Plus vous définissez la priorité (par exemple, 10), plus il est probable que ce périphérique devienne le maître de la grappe virtuelle.

Remarque

Si les périphériques de la grappe virtuelle sont mis sous tension à des moments différents, le premier périphérique mis sous tension assume le rôle de maître de la grappe virtuelle. Étant donné que chaque grappe virtuelle nécessite un maître, chaque périphérique de la grappe virtuelle vérifie, lorsqu'il est mis sous tension, que la grappe dispose d'un maître virtuel. S'il n'y en a pas, ce périphérique prend en charge le rôle. Les périphériques mis sous tension et ajoutés plus tard à la grappe deviennent des périphériques de secours. Si tous les périphériques de la grappe virtuelle sont mis sous tension simultanément, le périphérique dont le paramètre de priorité est le plus élevé devient le maître de la grappe virtuelle. Si au moins deux périphériques de la grappe virtuelle sont mis sous tension simultanément et ont le paramètre de priorité le plus élevé, celui qui a l'adresse IP la plus basse devient le maître de la grappe virtuelle.

- **NAT Assigned IPv4 Address** (Adresse IPv4 attribuée par la NAT) : spécifie l'adresse IP à laquelle l'adresse IP de ce périphérique est traduite par la NAT. Si la NAT n'est pas utilisée (ou si le périphérique ne se trouve pas derrière un pare-feu utilisant la NAT), laissez le champ vide.
- **NAT Assigned IPv6 Address** (adresse IPv6 attribuée par NAT) : spécifie l'adresse IP à laquelle l'adresse IP de ce périphérique est traduite par la NAT. Si la NAT n'est pas utilisée (ou si le périphérique ne se trouve pas derrière un pare-feu utilisant la NAT), laissez le champ vide.
- **Send FQDN to client** (Envoyer le nom de domaine complet au client) : cochez cette case pour que le maître de grappe VPN envoie un nom de domaine complet en utilisant l'hôte et le nom de domaine du périphérique de grappe au lieu de l'adresse IP externe lors de la redirection des connexions du client VPN vers ce périphérique de grappe.

Par défaut, l'ASA envoie uniquement les adresses IP dans la redirection de l'équilibrage de charge à un client. Si les certificats utilisés reposent sur des noms DNS, ils ne seront pas valides lorsque les connexions sont redirigées vers un périphérique de secours.

En tant que maître de la grappe VPN, cet ASA peut envoyer le nom de domaine pleinement qualifié (FQDN) d'un périphérique de la grappe (un autre ASA de la grappe), au moyen d'une recherche DNS inverse, au lieu de son adresse IP externe, lors de la redirection des connexions du client VPN vers ce périphérique de la grappe.

Toutes les interfaces réseau externes et internes des périphériques d'équilibrage de charge d'une grappe doivent se trouver sur le même réseau IP.

Remarque

Lors de l'utilisation d'IPv6 et de l'envoi de FQDN au client, ces noms doivent pouvoir être résolus par l'ASA au moyen du DNS.

Prochaine étape

Lorsque plusieurs nœuds ASA sont regroupés pour l'équilibrage de la charge et que l'utilisation des URL de groupe est souhaitée pour les connexions Secure Client, les nœuds ASA individuels doivent :

- Configurez chaque profil de connexion d'accès à distance avec une URL de groupe pour chaque adresse de cluster virtuelle d'équilibrage de charge (IPv4 et IPv6).
- Configurez une URL de groupe pour l'adresse publique d'équilibrage de charge VPN de ce nœud.

Les URL de groupe sont configurées dans le volet **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Secure Client Connection Profiles (Profils de connexion) > connection profile name (nom du profil de connexion) > Add or Edit (Ajouter ou modifier) > Advanced (Avancé) > Group Alias / Group URL (Alias de groupe / URL de groupe)**.

Historique des fonctionnalités pour l'équilibrage de charge VPN

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Équilibrage de charges VPN avec SAML	9.17(1)	L'ASA prend désormais en charge l'équilibrage VPN avec l'authentification SAML.
Équilibrage de la charge VPN	7.2(1)	Cette fonctionnalité a été introduite.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.