Forum aux questions sur le Concentrateur Cisco VPN 3000

Contenu

Introduction

Ce document répond à des questions fréquentes (FAQ) au sujet du concentrateur VPN de la gamme Cisco 3000.

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

Généralités

Q. Que signifie le message d'erreur « Lost Service » ?

A. S'il n'y a aucun trafic envoyé entre le concentrateur VPN et le client VPN pendant une période, un paquet de détection d'homologue mort (DPD) est envoyé du concentrateur VPN au client VPN pour s'assurer que son homologue est toujours là. S'il y a un problème de connectivité entre les deux homologues où le client VPN ne répond pas au concentrateur VPN, le concentrateur VPN continue à envoyer des paquets DPD pendant une période. Ceci met fin au tunnel et produit l'erreur s'il ne reçoit pas une réponse pendant cette période. Référez-vous à l'ID de bogue Cisco CSCdz45586 (clients enregistrés uniquement).

L'erreur devrait ressembler à ceci :

```
SEV=4 AUTH/28 RPT=381 XXX.XXX.XXX.XX User [SomeUser] disconnected:
Duration: HH:MM:SS Bytes xmt: 19560 Bytes rcv: 17704 Reason:
Lost Service YYYY/MM/DD HH:MM:SS XXX.XXX.XXX.XXX
syslog notice
45549 MM/DD/YYYY HH:MM:SS SEV=4 IKE/123 RPT=XXX.XXX.XXX.XXX
Group [SomeDefault] User [SomeUser]
IKE lost contact with remote peer, deleting connection (keepalive type: DPD)
```

Cause : L'homologue IKE distant n'a pas répondu aux keepalives dans la période de temps prévue. La connexion à l'homologue IKE a donc été supprimée. Le message comprend le mécanisme keep-alive utilisé. Ce problème est seulement reproductible si l'interface publique est déconnectée pendant une session de tunnel active. Le client a besoin de surveiller leur connectivité réseau pendant que ces événements sont générés pour indiquer exactement la

cause du problème potentiel de connectivité réseau.

Désactivez IKE keepalive en allant à **%System Root%\Program Files\Cisco Systems\VPN Client\Profiles** sur le PC client qui connaît le problème, et modifiez le **fichier PCF** (si applicable) pour la connexion.

Remplacez **'ForceKeepAlives=0'** (valeur par défaut) par **'ForceKeepAlives=1'**.

Si le problème persiste, ouvrez une Demande d'assistance avec l'assistance technique Cisco et fournissez le « visualiseur de log » du client et les fichiers journal du concentrateur VPN lorsque le problème survient.

Q. Que signifie le message d'erreur « q_send » failures detected for EMQ1 queue ?

A. Ce message d'erreur se produit quand il y a un trop grand nombre d'événements/informations de débogage dans la mémoire tampon. Il n'a aucune incidence négative autre que la perte éventuelle de quelques messages d'événement. Essayez de réduire les événements au nombre minimal requis pour empêcher ce message.

Q. Mon groupe supprimé s'affiche toujours dans la configuration du concentrateur VPN. Comment puis-je le supprimer ?

A. Copiez la configuration dans un éditeur de texte (tel que Notepad) et manuellement éditez ou supprimez l'information du groupe affectée dénotée par **[ipaddrgrouppool #.0]**. Sauvegardez la configuration et téléchargez-la vers le concentrateur VPN. Un exemple est montré ici.

```
!--- Change to 14.1 or any other number that is not in use !--- any number other than 0).
[ipaddrgrouppool 14.0] rowstatus=1 rangename= startaddr=172.18.124.1 endaddr=172.18.124.2
```

Q. Est-il possible d'avoir plusieurs serveurs primaires SDI ?

A. Les concentrateurs VPN 3000 ne peuvent télécharger qu'un seul fichier secret de noeud à la fois. Dans SDI version pre-5.0, vous pouvez ajouter plusieurs serveurs SDI, mais ils doivent tout partager le même fichier secret de noeud (considérez-les comme les serveurs principal et de secours). Dans SDI version 5.0, vous pouvez seulement entrer le serveur SDI principal (les serveurs de secours sont mentionnés dans le fichier secret de noeud) et les serveurs de reproduction.

Q. J'obtiens le message d'erreur « SSL certificate will expire in 28 days ». Que dois-je faire ?

A. Le message indique que votre certificat de Secure Socket Layer (SSL) expirera dans 28 jours. Ce certificat est utilisé pour parcourir la gestion web par l'intermédiaire de HTTPS. Vous pouvez laisser ce certificat avec les paramètres par défaut ou vous pouvez configurer différentes options avant de générer le nouveau certificat. Sélectionnez **Configuration > System > Management Protocols > SSL** pour faire ceci. Sélectionnez **Administration > Certificate Management** et cliquez sur **Generate** pour renouveler le certificat.

Si vous êtes préoccupé par la sécurité sur votre concentrateur VPN et voudriez empêcher les accès non autorisés, désactivez le HTTP et/ou le HTTPS sur l'interface publique en allant à **Configuration > Policy Management > Traffic Management > Filters**. Si vous avez besoin d'obtenir

votre concentrateur VPN par Internet via HTTP ou HTTPS, vous pouvez spécifier l'accès en vous basant sur l'adresse source en allant à **Administration > Access Rights > Access Control List**. Vous pouvez utiliser le menu Help dans le coin supérieur droit de la fenêtre pour obtenir plus d'informations.

Q. Comment puis-je consulter les informations utilisateur dans la base de données d'utilisateurs interne ? Elle n'est pas visible lorsque je consulte le fichier de configuration.

A. Sélectionnez la **gestion > les droits d'accès > les paramètres d'accès**, choisissez le **fichier Encryption=None de config**, et sauvegardez le config pour visualiser des utilisateurs et des mots de passe. Vous devriez pouvoir lancer une recherche pour un utilisateur spécifique.

Q. Combien d'utilisateurs la base de données interne peut-elle enregistrer ?

A. Le nombre d'utilisateurs dépend de la version et est spécifié dans la section **Configuration > User Management** du guide de l'utilisateur pour votre version de concentrateur VPN 3000. Un total de 100 utilisateurs ou groupes (la somme d'utilisateurs et de groupes doit égaler 100 ou moins) est possible pour les versions 2.2 à 2.5.2 de VPN 3000. Dans les versions VPN 3000 3.0 et ultérieures, le nombre pour les concentrateurs 3005 et 3015 reste à 100. Pour les concentrateurs VPN 3030 et 3020, le nombre est 500, pour les concentrateurs VPN 3060 ou 3080, le nombre est 1000. En outre, l'utilisation d'un serveur d'authentification externe améliore l'évolutivité et la gestionnabilité.

Q. Quelle est la différence entre la passerelle de tunnel par défaut et la passerelle par défaut ?

A. Le concentrateur VPN 3000 utilise la passerelle tunnel par défaut pour router les utilisateurs au sein du réseau privé (généralement le routeur interne). Le concentrateur VPN utilise la passerelle par défaut pour router des paquet vers Internet (généralement le routeur externe).

Q. Si je place mon concentrateur VPN 3000 derrière un pare-feu ou un contrôle d'accès exécutant des listes de contrôle d'accès, quels ports et protocoles dois-je autoriser ?

A. Ce diagramme mentionne des ports et des protocoles.

Service	Numéro de protocole	Port de source	Destination port
Contrôle PPTP connection	6 (TCP)	1023	1723
Encapsulation de tunnel PPTP	47 (GRE)	S/O	S/O
Gestion des clés ISAKMP/IPSec	17 (UDP)	500	500
Encapsulation tunnel IPsec	50 (ESP)	S/O	S/O
IPSec NAT Transparency	17 (UDP)	10000 (default)	10000 (default)

Remarque: Le port de transparence de Traduction d'adresses de réseau (NAT) est configurable à n'importe quelle valeur entre 4001 et 49151. Dans les versions 3.5 ou ultérieures, vous pouvez configurer IPsec par dessus TCP en allant à **Configuration > System > Tunneling Protocols > IPSec > IPSec over TCP**. Vous pouvez entrer jusqu'à 10 ports TCP (1 - 65535) en les séparant par des virgules. Si cette option est configurée, assurez-vous que ces ports sont autorisés dans votre pare-feu ou votre routeur exécutant des listes de contrôle d'accès.

Q. Comment puis-je rétablir le concentrateur VPN aux paramètres d'usine ?

A. A partir de l'écran File Management, supprimez le fichier « config » puis redémarrez. Si ce fichier est supprimé accidentellement, une copie de secours « config.bak » est conservée.

Q. Puis-je utiliser TACACS+ pour l'authentification administrative ? Que dois-je garder à l'esprit lorsque j'effectue cela ?

A. Oui, à partir de la version 3.0 du concentrateur VPN 3000, vous pouvez utiliser un TACACS+ pour l'authentification administrative. Après avoir configuré TACACS+, assurez-vous d'effectuer un test d'authentification avant de vous déconnecter. Une configuration incorrecte de TACACS+ peut vous empêcher de vous connecter. Ceci exige une connexion via le port de console afin de désactiver TACACS+ et rectifier le problème.

Q. Que puis-je faire en cas de mot de passe administratif oublié ?

A. Dans les versions 2.5.1 et ultérieures, connectez un PC au port de console du concentrateur VPN à l'aide d'un câble série direct RS-232 avec le PC réglé pour :

- 9600 bits par seconde
- 8 bits de données
- aucune parité
- 1 bit d'arrêt
- contrôle de flux matériel activé
- Émulation VT100

Redémarrez le concentrateur VPN. Après le test de diagnostic, une ligne de trois points (...) apparaît sur la console. Appuyez sur **CTRL-C** dans les trois secondes après l'apparition de ces points. Un menu s'affiche et vous permet de réinitialiser les mots de passe système à leur valeur par défaut.

Q. A quoi servent le nom de groupe et le mot de passe de groupe ?

A. Le nom de groupe et le mot de passe de groupe sont utilisés pour créer un hachage qui est ensuite utilisé pour créer une association de sécurité.

Q. Fait-il le proxy ARP de concentrateur VPN au nom des utilisateurs tunnelisés ?

A. Oui.

Q. Où dois-je placer le concentrateur VPN 3000 par rapport à mon pare-feu ?

A. Le concentrateur VPN 3000 peut être placé devant, derrière, en parallèle, ou dans la zone

démilitarisée (DMZ) d'un pare-feu. Il n'est pas recommandé d'avoir les interfaces publiques et privées dans le même LAN virtuel (VLAN).

Q. Y a-t-il une manière de désactiver le proxy ARP sur le concentrateur VPN Cisco 3000 ?

A. Le Protocole ARP (Address Resolution Protocol) de proxy ne peut pas être désactivé sur le concentrateur de Cisco VPN 3000.

Q. Où puis-je trouver une liste des bogues résolus pour le concentrateur VPN 3000 ?

A. Les utilisateurs peuvent employer le Bug Toolkit (clients enregistrés seulement) pour trouver les informations détaillées au sujet des bogues.

Q. Où puis-je trouver des exemples de configuration pour le concentrateur VPN 3000 ?

A. En plus de la documentation de concentrateur VPN 3000, plus d'exemples de configuration peuvent être trouvés sur la page de support de Concentrateur de la série Cisco VPN 3000.

Q. Comment puis-je augmenter la journalisation pour obtenir de meilleurs débogages pour des événements spécifiques ?

A. Vous pouvez aller à **Configuration > System > Events > Classes** et configurer les événements spécifiques (tels qu'IPsec ou PPTP) pour obtenir de meilleurs débogages. Le débogage doit seulement être allumé pour la durée de l'exercice de dépannage parce qu'il peut entraîner une dégradation des performances. Pour le débogage d'IPsec, allumez IKE, IKEDBG, IPSEC, IPSECDBG, AUTH et AUTHDBG. Si vous utilisez des certificats, ajoutez la classe CERT à la liste.

Q. Comment puis-je surveiller le trafic vers le concentrateur VPN 3000 ?

A. L'interface HTML qui vient avec le concentrateur VPN 3000 vous permet d'obtenir des fonctionnalités de surveillance de base si vous regardez sous **Monitoring > Sessions**. Le concentrateur VPN 3000 peut également être surveillé par le Protocole de gestion de réseau simple (SNMP) à l'aide du gestionnaire SNMP de votre choix. Alternativement, vous pouvez acheter la solution Cisco VPN/Gestion de la sécurité (VMS). Cisco VMS fournit des fonctionnalités clé pour vous assister si vous déployez le concentrateur VPN de la gamme 3000 et avez besoin d'une surveillance approfondie des VPN d'accès à distance et de site-à-site, basés sur IPsec, L2TP, et PPTP. Référez-vous à Solution de Gestion de la sécurité VPN pour plus de détails au sujet du VMS.

Q. La gamme de concentrateurs de Cisco VPN 3000 a-t-elle un pare-feu intégré ? Si oui, quelles fonctionnalités sont supportées ?

A. Tandis que la gamme a intégré des capacités de port/filtrage statiques et NAT, Cisco vous suggère d'utiliser un périphérique comme le Cisco Secure PIX Firewall pour le pare-feu de l'entreprise.

Q. Quelles options de routage et protocoles VPN sont supportés par le concentrateur VPN de la gamme Cisco 3000 ?

A. La gamme supporte les options de routage suivantes :

- Protocole d'informations de routage (RIP)
- RIP2
- Open Shortest Path First (OSPF)
- routes statique
- Virtual Router Redundancy Protocol (VRRP)

Les protocoles VPN supportés incluent le Protocole de tunnellisation point à point (PPTP), le L2TP, le L2TP/IPsec, et l'IPsec avec ou sans un périphérique NAT entre le VPN 3000 et le client final. L'IPsec via NAT est connu sous le nom de transparence NAT.

Q. Quels mécanismes/systèmes d'authentification la gamme de concentrateurs VPN Cisco 3000 supporte pour les PC du client ?

A. Le Domaine NT, le RAYON ou le proxy RADIUS, la RSA Security SecurID (SDI), les Certificats numériques, et l'authentification interne sont pris en charge.

Q. Puis-je faire une Traduction d'adresses de réseau (NAT) statique pour les utilisateurs passant par le concentrateur VPN 3000 ?

A. Vous ne pouvez faire qu'une Traduction d'adresses de port (PAT) pour les utilisateurs sortants. Vous ne pouvez pas faire de NAT statique sur le concentrateur VPN 3000.

Q. Comment puis-je assigner une adresse IP fixe à un Protocole de tunnellisation point à point (PPTP) ou à un utilisateur d'IPsec spécifiques par le concentrateur VPN 3000 ?

A. Cette liste explique comment assigner des adresses IP statiques :

- **Utilisateurs PPTP**Dans la section IP Adress Management, en plus de choisir votre pool ou vos options de protocole de configuration dynamique d'hôte (DHCP), cochez l'option **Use Client Address**. Puis, définissez l'utilisateur et l'adresse IP dans le concentrateur VPN 3000. Cet utilisateur obtient toujours l'adresse IP configurée dans le concentrateur VPN en se connectant.
- **Utilisateurs d'IPsec**Dans la section IP Address Management, en plus de choisir votre pool ou vos options de DHCP, cochez l'option **Use Address from Authentication Server**. Puis, définissez l'utilisateur et l'adresse IP dans le concentrateur VPN 3000. Cet utilisateur obtient toujours l'adresse IP configurée dans le concentrateur VPN en se connectant. Tous les autres qui appartiennent au même groupe ou à d'autres groupes obtiennent une adresse IP du pool global ou du DHCP.Avec le logiciel du concentrateur Cisco VPN 3000 version 3.0 et ultérieures, vous avez l'option de configurer un pool d'adresse par groupe. Cette fonctionnalité peut vous aider également à assigner une adresse IP statique à un utilisateur spécifique. Si vous configurez un pool pour un groupe, l'utilisateur avec une IP statique obtient l'adresse IP qui lui est affectée, et les autres membres du même groupe obtiennent des adresses IP à partir du groupe de pool. Ceci s'applique seulement quand vous utilisez le concentrateur VPN

comme serveur d'authentification.

Remarque: Si vous utilisez un serveur d'authentification externe, alors vous devez utiliser le serveur externe pour assigner les adresses correctement.

Q. Quels sont les problèmes de compatibilité connus entre les Produits PPTP de Microsoft et le concentrateur VPN 3000 ?

A. Cette information est basée sur les versions 3.5 et ultérieures du logiciel des concentrateurs VPN de la gamme 3000 ; Concentrateurs VPN de la gamme 3000, modèles 3005, 3015, 3020, 3030, 3060, 3080 ; et systèmes d'exploitation Microsoft Windows 95 et ultérieurs.

- **Accès réseau à distance (DUN) 1.2 sous Windows 95**Le chiffrement MPPE n'est pas pris en charge sous DUN 1.2. Pour vous connecter à l'aide de MPPE, installez DUN Windows 95 1.3. Vous pouvez télécharger la mise à niveau Microsoft DUN 1.3 sur le site Web de Microsoft.
- **Windows NT 4.0**Windows NT est entièrement supporté pour des connexions du Protocole de tunnellisation point à point (PPTP) vers le concentrateur VPN. Le Service Pack 3 (SP3) ou ultérieur est requis. Si vous exécutez SP3, vous devez installer la performance et les correctifs de securité PPTP. Référez-vous au site Web de Microsoft pour des informations sur la Mise à jour de performances et de sécurité pour WinNT 4.0 .Notez que le Service Pack 5 128 bits ne gère pas correctement les clés MPPE, et le PPTP peut échouer dans la transmission de données. Quand ceci se produit, le journal d'événements affiche ce message :`103 12/09/1999 09:08:01.550 SEV=6 PPP/4 RPT=3 80.50.0.4 User [ testuser ] disconnected. Experiencing excessive packet decrypt failure.`Pour résoudre ce problème, téléchargez la mise à jour pour que la façon obtienne le plus défunt Service Pack 6a de Windows NT et le Service Pack 6a de Windows NT 4.0 disponible. Référez-vous à l'article de Microsoft Les clés MPPE non gérées correctement pour une demande de MS-CHAP 128 bits pour plus d'informations.

Q. Quel est le nombre maximal de filtres autorisés sur un concentrateur VPN 3000 ?

A. Le nombre maximal de filtres que vous pouvez ajouter sur une unité du VPN 30xx (même 3030 ou 3060) est fixé at 100. Les utilisateurs peuvent trouver des informations supplémentaires au sujet de ce problem en consultant l'ID de bogue Cisco CSCdw86558 (clients enregistrés uniquement).

Q. Quel est le nombre maximal de routes dans la gamme de concentrateurs VPN 30xx ?

A. Le nombre maximal de routes est :

- Le concentrateur VPN 3005 possédait auparavant un maximum de 200 routes. Ce nombre a maintenant été augmenté à 350 routes. Référez-vous à l'ID de bogue Cisco CSCeb35779 (clients enregistrés uniquement) pour plus de détails.
- Le concentrateur VPN 3030 a été testé jusqu'à 10 000 routes.
- La limite de la table de routage sur les concentrateurs VPN 3030, 3060 et 3080 est proportionnelle aux ressources/mémoire disponibles dans chaque périphérique.

- Le concentrateur VPN 3015 n'a aucune limite maximale prédéfinie. Ceci est vrai pour le Protocole d'informations de routage (RIP) et le protocole Open Shortest Path First (OSPF).
- Le concentrateur VPN 3020 - En raison d'une limitation de Microsoft, les PC équipés de Windows XP ne sont pas capables de recevoir un grand nombre de routes statiques sans classe (CSR). Le concentrateur VPN 3000 limite le nombre de CSR qui sont insérées dans un message de réponse DHCP INFORM une fois configuré pour le faire. Le concentrateur VPN 3000 limite le nombre de routes à 28-42, selon la classe.

Q. Comment puis-je effacer complètement les statistiques d'interface sur le concentrateur VPN 3000 ?

A. **Surveillance > statistiques > MIB-II > Ethernets** choisis et remis à l'état initial les statistiques pour effacer des statistiques pour la session en cours. Rappelez-vous que ceci n'efface pas totalement les statistiques. Vous devez redémarrer pour réinitialiser réellement les statistiques (contre la réinitialisation à des fins de surveillance).

Q. Quels ports dois-je autoriser sur le concentrateur VPN pour la communication de Protocole d'heure réseau (NTP) ?

A. Permettez le port 123 de TCP et UDP.

Q. Quelles sont les fonctions des ports UDP 625xx ?

A. Ces ports sont utilisés pour la communication du client VPN entre la cale/Deterministic NDIS Extender (DNE) réels et la pile TCP/IP du PC, et sont destinés à un usage développemental interne uniquement. Par exemple, le port 62515 est utilisé par le client VPN pour envoyer l'information au journal du client VPN. D'autres fonctions de port sont montrées ici.

- 62514 - Service de Cisco Systems, Inc. VPN au gestionnaire de Cisco Systems IPsec
- 62515 - Gestionnaire de Cisco Systems IPsec au service de Cisco Systems, Inc. VPN
- 62516 - Service de Cisco Systems, Inc. VPN au XAUTH
- 62517 - XAUTH au service de Cisco Systems, Inc. VPN
- 62518 - Service de Cisco Systems, Inc. VPN au CLI
- 62519 - CLI vers Cisco Systems, Inc. Service VPN
- 62520 - Service de Cisco Systems, Inc. VPN à UI
- 62521 - UI au service de Cisco Systems, Inc. VPN
- 62522 - Messages du journal
- 62523 - Gestionnaire de connexion au service de Cisco Systems, Inc. VPN
- 62524 - PPPTool au service de Cisco Systems, Inc. VPN

Q. Puis-je retirer la barre flottante WebVPN ?

A. Vous ne pouvez pas retirer la barre d'outils flottante ni éviter de la charger lorsque que vous établissez une session WebVPN. C'est parce que quand vous fermez cette fenêtre, la session est terminée immédiatement et quand vous essayez de vous connecter à nouveau, la fenêtre est chargée à nouveau. C'est la manière dont les sessions WebVPN ont été conçues initialement. Vous pouvez fermer la fenêtre principale mais il n'est pas possible de fermer la fenêtre flottante.

Logiciel

Q. Le webvpn prend en charge-il l'Outlook Web Access (OWA) 2003 ?

A. Le soutien OWA 2003 du webvpn sur le concentrateur VPN 3000 est maintenant disponible avec des téléchargements de version 4.1.7 (clients enregistrés seulement).

Q. Où puis-je obtenir les dernières révisions de logiciel pour le concentrateur VPN 3000 ?

A. Tous les concentrateurs VPN Cisco 3000 sont livrés avec le code le plus récent, mais les utilisateurs peuvent consulter Téléchargements (clients enregistrés uniquement) pour voir si un logiciel plus récent est disponible.

Référez-vous à la page de documentation Concentrateur VPN de la gamme Cisco 3000 pour la documentation la plus récente sur le concentrateur VPN 3000.

Q. Ai-je besoin d'un serveur TFTP pour mettre à niveau le concentrateur VPN 3000 ? Y a-t-il une autre façon de mettre à jour la boîte ?

A. En plus d'utiliser le TFTP, vous pouvez améliorer le concentrateur VPN en téléchargeant le dernier logiciel sur votre disque dur. Puis, à partir d'un navigateur sur le système où le logiciel est localisé, allez à **Administration > Software Update** et recherchez le logiciel téléchargé sur votre disque dur (comme pour ouvrir un fichier). Quand vous l'avez trouvé, sélectionnez l'onglet **Upload**.

Q. Que signifie le « k9 » dans les derniers noms de code (tels que « vpn3000-3.0.4.Rel-k9.bin- ») ?

A. La désignation de « k9 » pour le nom de l'image a substitué la désignation 3DES initialement utilisée (par exemple, vpn3000-2.5.2.F-3des.bin). Ainsi, le « k9 » signifie maintenant que c'est une image 3DES.

Q. Dois-je utiliser l'option de Compression de données sous le groupe IPsec pour tous mes utilisateurs ?

A. La Compression de données augmente la mémoire réquise et l'utilisation du processeur pour chaque session d'utilisateur et diminue par conséquent le débit global du concentrateur VPN. Pour cette raison, Cisco recommande que vous activiez la compression de données seulement si chaque membre du groupe est un utilisateur distant qui se connecte avec un modem. Si le moindre membre du groupe se connecte en haut débit, n'activez pas la compression de données pour le groupe. Au lieu de cela, divisez le groupe en deux groupes, un pour les utilisateurs de modem et l'autre pour les utilisateurs de connexions haut débit. Activez la compression de données seulement pour le groupe des utilisateurs de modem.

Autres fonctionnalités avancées

Q. L'Équilibrage de charge fonctionne-t-il avec des connexions entre réseaux locaux ?

A. L'Équilibrage de charge est efficace seulement sur des sessions à distance initiées avec le client logiciel Cisco VPN (version 3.0 et ultérieures). Tous les autres clients (PPTP, L2TP) et connexions entre réseaux locaux peuvent se connecter à un concentrateur VPN sur lequel l'équilibrage de charge est activé, mais ils ne peuvent pas participer à l'équilibrage de charge.

Q. Comment puis-je déchiffrer les mots de passe à partir du fichier de configuration ?

A. Allez à la **configuration > au système > aux protocoles de gestion > au XML** et puis à la **gestion | file management sélectionnez XML format**. Utilisez le même nom, ou un nom différent, et ouvrez le fichier afin d'afficher les mots de passe.

Q. Puis-je utiliser à la fois le Virtual Router Redundancy Protocol (VRRP) et l'équilibrage de charge ?

A. Vous ne pouvez pas utiliser l'équilibrage de charge avec le VRRP. Dans une configuration VRRP, le périphérique de secours demeure inactif à moins que le concentrateur VPN actif échoue. Dans une configuration d'équilibrage de charge configuration, il n'y a aucun périphérique inactif.

Q. Tout le trafic par VPN des clients d'accès à distance doit-il s'attaquer par un tunnel chiffré au concentrateur VPN à l'entreprise ou au fournisseur de services ? Par exemple, l'accès Internet simple peut-il aller publiquement, directement par la connexion Internet de l'ISP ?

A. Oui. Ce concept est connu sous le nom de « split tunneling ». Le split tunelling permet un accès sécurisé aux ressources de l'entreprise par un tunnel crypté tandis qu'il permet l'accès à Internet directement via les ressources de l'ISP (ceci élimine le réseau de l'entreprise du chemin pour l'accès à Internet). Le concentrateur VPN de la gamme Cisco 3000 jusqu'au client VPN Cisco et au client matériel du VPN 3002 peuvent supporter le split tunneling. Pour davantage de sécurité, cette fonctionnalité est contrôlable par l'administrateur du concentrateur VPN et non par l'utilisateur.

Q. L'utilisation du split tunneling est-elle sans danger ?

A. La Segmentation de tunnel te permet pour avoir la commodité de parcourir l'Internet tandis que connectée par le tunnel VPN. Cependant, cela présente un certain risque si l'utilisateur VPN connecté au réseau de l'entreprise est vulnérable aux attaques. Il est recommandé que les utilisateurs utilisent un pare-feu personnel dans ce cas. Les notes de publication pour chaque version de client VPN traitent de l'interopérabilité avec les pare-feux personnels.

Q. Comment l'équilibrage de charge fonctionne-t-il sur le concentrateur VPN Cisco 3000 ?

A. Le chargement est calculé comme pourcentage dérivé des connexions actives divisées par les connexions configurées par maximum. Le maître essaye toujours d'avoir la charge la moins élevée car il est chargé de la charge supplémentaire (inhérente) de mettre à jour toutes les sessions administratives entre réseaux locaux, en calculant tout autre chargement de cluster member, et il est responsable de toutes les redirections de clients.

Pour un cluster fonctionnel venant d'être configuré, le maître a environ un 1 pourcent de charge avant que toutes les connexions aient été établies. Par conséquent, le maître redirige les connexions vers le concentrateur de secours jusqu'à ce que le pourcentage de charge du concentrateur de secours soit plus important que le pourcentage de charge du maître. Par exemple, deux concentrateurs VPN 3030 en état « inactif », le maître a un 1 pourcent de charge. On donne 30 connexions au secondaire (2 pourcents de charge) avant que le master n'accepte des connexions.

Afin de vérifier que le master accepte des connexions, allez à **Configuration > System > General > Sessions** et abaissez le nombre maximal de connexions à un nombre artificiellement peu élevé pour augmenter rapidement la charge placée sur concentrateur VPN de secours.

Q. Combien de périphériques de headend le moniteur VPN peut-il dépister ?

A. Le Moniteur VPN peut suivre 20 périphériques en tête de réseau. Dans un scénario « hub-and-spoke », des connexions à partir de sites distants sont surveillées en tête de réseau. Il n'y a aucun besoin de surveiller tous les sites et utilisateurs distants puisque ces informations peuvent être tracéee sur le concentrateur de routage. Ces périphériques en tête de réseau peuvent supporter jusqu'à 20 000 utilisateurs distants ou 2 500 sites distants. Un périphérique VPN à double interface qui sort vers les sites en étoile compte comme deux des 20 périphériques maximum qui peuvent être surveillés.

Informations connexes

- Page d'assistance du concentrateur VPN Cisco 3000
- Page de support pour le Client Cisco VPN 3000
- Support et documentation techniques - Cisco Systems