Référence de mise en oeuvre et de performance/évolutivité AnyConnect pour la préparation de COVID-19

Contenu

Introduction
Mise en oeuvre
Licence
Guides de démarrage rapide de la configuration initiale d'AnyConnect
Guides de configuration complets
Guides d'installation des certificats
Problèmes de performances et d'évolutivité
Symptômes et identification des problèmes
Utilisation élevée du CPU
Nombre maximal de connexions VPN
Références de la feuille de données
Atténuation potentielle
Activation de la transmission tunnel partagée
Implémenter l'équilibrage de charge VPN (ASA uniquement)
Optimisation de la configuration
Sélection du protocole de tunnel
Appliquer la QoS par tunnel (FTD uniquement)
Implémenter un BIOS Crypto Engine Accelerator (ASA uniquement)
Forum aux questions
Licence
Configuration
Surveillance
Dépannage
Obtention d'aide supplémentaire
Références

Introduction

Alors que les pays du monde entier se battent contre la pandémie mondiale COVID-19, de plus en plus d'entreprises mettent en oeuvre des politiques de travail à distance pour prévenir la propagation de la maladie. En conséquence, la demande de VPN d'accès à distance (RAVPN) pour permettre aux employés d'accéder aux ressources internes de l'entreprise augmente. Cet article fournit des références aux guides de configuration permettant de configurer rapidement RAVPN au sein du réseau ou d'identifier et de résoudre les problèmes de performances ou d'évolutivité.

Mise en oeuvre

La section suivante détaille la configuration et les déploiements d'accès à distance AnyConnect sur les différentes plates-formes Cisco, ainsi que les guides d'installation des certificats, car le déploiement des certificats fait partie intégrante de l'accès à distance Cisco en raison des exigences d'authentification des certificats pour RAVPN.

Licence

Les licences sont requises pour mettre fin aux connexions RAVPN sur un périphérique. Les plates-formes ASA ne prendront en charge que 2 homologues VPN sans licence. Les FTD ne permettent pas le déploiement de la configuration AnyConnect sur le périphérique sans licence. En raison de l'épidémie COVID-19, Cisco propose des licences temporaires gratuites pour aider les utilisateurs à mettre en oeuvre RAVPN sur leurs périphériques Cisco. Plus d'informations à ce sujet sont disponibles : Obtention d'une licence d'urgence COVID-19 AnyConnect

Guides de démarrage rapide de la configuration initiale d'AnyConnect

Suivez ces guides de démarrage rapide pour implémenter AnyConnect Remote Access avec les configurations les plus courantes :

- Configurer un client AnyConnect Secure Mobility avec la tunnellisation fractionnée sur un ASA
- Configuration VPN d'accès à distance AnyConnect sur FTD
- Configuration AnyConnect initiale pour FTD gérée par FMC (vidéo)

Pour obtenir des guides complets de configuration des produits, reportez-vous à la section ci-dessous.

Guides de configuration complets

ASA :

- Configuration ASDM ASA
- Configuration de l'interface de ligne de commande ASA

FTD :

- FTD géré par FDM
- FTD géré par FMC

IOS/IOS-XE :

- Routeur IOS pour SSLVPN
- Routeur IOS-XE pour VPN SSL (CSR uniquement)
- Routeur IOS/IOS-XE pour VPN IKEv2

Guides d'installation des certificats

- ASA
- FTD FDM
- FTD FMC
- IOS/IOS-XE

Problèmes de performances et d'évolutivité

Avec l'augmentation significative de l'utilisation de RAVPN, les utilisateurs d'AnyConnect peuvent rencontrer des problèmes de performances. Consultez les sections suivantes pour déterminer comment identifier ces problèmes et les stratégies d'atténuation pour y remédier.

Symptômes et identification des problèmes

Utilisation élevée du CPU

L'utilisation du processeur affecte directement les performances des utilisateurs VPN. L'utilisation du CPU augmentera à mesure que le trafic crypté ou décrypté sera plus important et traité par le périphérique. Le périphérique peut bénéficier d'un processeur élevé lorsque la plate-forme approche le débit VPN maximal qu'il peut gérer. Il est nécessaire de déterminer si l'utilisation élevée du CPU est due à la sursouscription du périphérique ou à un autre problème.

Pour vérifier si le périphérique est doté d'un processeur élevé, il est conseillé d'exécuter les commandes suivantes :

show process cpu-usage non nul

show cpu usage

Exemple de rapport :

```
asa# show processes cpu-usage non-zero
PC         Thread       5Sec     1Min     5Min   Process
0x00000000019da592   0x00007fffd808b040     0.0%     0.0%     0.5%   Logger
0x0000000000844596   0x00007fffd807bd60     0.0%     0.0%     0.1%   CP Processing
0x0000000000c0dc8c   0x00007fffd8074960     0.1%     0.1%     0.1%   ARP Thread
   -          -        43.8%    43.8%    40.3%   DATAPATH-0-2209
   -          -        43.9%    43.8%    40.3%   DATAPATH-1-2210

asa# show cpu usage
CPU utilization for 5 seconds = 88%; 1 minute: 88%; 5 minutes: 82%
```

Dans l'exemple ci-dessus, il est observé que DATAPATH-0 et DATAPATH-1 consomment 87,7 % de l'utilisation totale du CPU. Dans ce cas, l'ASA est sursouscrit et est nécessaire pour déterminer si ce symptôme est dû à une grande quantité de trafic chiffré et déchiffré. Cette valeur peut ensuite être comparée à la valeur du débit VPN documentée dans la fiche technique de cette plate-forme.

Pour calculer la quantité totale de trafic VPN transitant par le périphérique par seconde, nous pouvons ajouter les ***octets d'entrée*** et les ***octets de sortie*** dans la section ***Statistiques globales*** de la commande ***show crypto accélération statistics***. Sur un ASA ou un FTD, effacez la sortie ***show crypto Accelator statistics*** à l'aide de la commande ***clear crypto accélator statistics***. Attendez un certain temps, puis exécutez la commande : ***show crypto Accelerator statistics*** comme illustré ci-dessous :

```
asa# show crypto accelerator statistics

Crypto Accelerator Status
```

```
------------------------
[Capability]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 2
   Max crypto throughput: 1000 Mbps
   Max crypto connections: 5000
[Global Statistics]
   Number of active accelerators: 2
   Number of non-operational accelerators: 0
   Input packets: 257353
   Input bytes: 271730225                          <----------------
   Output packets: 2740
   Output error packets: 0
   Output bytes: 57793                             <----------------
[…]
```

Prenez quelques instantanés à des intervalles spécifiques et obtenez un débit moyen en octets qui peut être converti en bits par seconde (bits/s). La formule à suivre est la suivante :

$$\frac{[InputBytes + OutputBytes] * 8}{1,000,000 * seconds} = Mbps$$

Dans l'exemple précédent, une commande ***clear crypto accélator statistics*** est exécutée à 0 seconde. 10 secondes plus tard, la commande ***show crypto accélération statistics*** a été exécutée pour obtenir le total des octets sur l'intervalle de 10 secondes. Ces valeurs sont ensuite utilisées pour calculer un bit/s de 217 Mbits/s qui a été traité sur un intervalle de 10 secondes. Plusieurs snapshots peuvent être nécessaires pour obtenir une moyenne plus précise.

Notez que ces valeurs augmenteront pour tout le trafic chiffré/décrypté (HTTPS, SSL, IPsec, SSH, etc.). Nous pouvons utiliser cette valeur pour déterminer le débit VPN moyen et le comparer à la feuille de données. Si le débit moyen est à peu près le même que celui de la feuille de données de la plate-forme, le périphérique est surabonné par le trafic chiffré et déchiffré.

En outre, cette méthode ne peut pas être utilisée pour déterminer le débit VPN sur les plates-formes firepower 2100, car les compteurs ne s'incrémentent pas pour le trafic VPN. Ceci est suivi dans CSCvt46830 .

Nombre maximal de connexions VPN

Lorsque le nombre maximal de connexions VPN est atteint, les utilisateurs peuvent connaître des périodes de perturbation où ils ne peuvent pas se connecter. Bien que l'activation de la licence AnyConnect Plus ou Apex déverrouille le nombre maximal d'homologues VPN, si ce maximum est atteint, aucun utilisateur supplémentaire ne sera autorisé sur le périphérique.

Pour vérifier le nombre maximal de connexions VPN disponibles sur le périphérique, vérifiez le résultat de ***show vpn-sessiondb*** :

```
asa# show vpn-sessiondb
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client            :     10 :        218 :          11 :        0
  SSL/TLS/DTLS               :     10 :        218 :          11 :        0
```

```
Clientless VPN               :      0 :         73 :           4
  Browser                    :      0 :         73 :           4
-------------------------------------------------------------------------
Total Active and Inactive    :     10             Total Cumulative :    291
Device Total VPN Capacity    :    250
Device Load                  :     4%
-------------------------------------------------------------------------

-------------------------------------------------------------------------
Tunnels Summary
-------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ----------------------------------------
Clientless                   :      0 :         73 :               4
AnyConnect-Parent            :     10 :        218 :              11
SSL-Tunnel                   :     10 :         77 :              10
DTLS-Tunnel                  :     10 :         65 :              10
-------------------------------------------------------------------------
Totals                       :     30 :        433
-------------------------------------------------------------------------
```

Pour déterminer le nombre total d'utilisateurs pris en charge par la plate-forme, consultez la fiche technique de votre périphérique ci-dessous.

Si les utilisateurs VPN ne sont pas en mesure de se connecter et que vous avez vérifié que le périphérique n'atteint pas le nombre maximal d'utilisateurs VPN, demandez une assistance supplémentaire au TAC.

Références de la feuille de données

Les fiches techniques suivantes mettent en évidence à la fois le nombre maximal d'utilisateurs VPN pris en charge par une plate-forme et le débit VPN maximal basé sur des tests. IKEv2 et DTLS AnyConnect devraient avoir un débit total (agrégé) similaire au débit VPN IPsec indiqué dans chaque section.

- ASAv
- ASA 5500
- ASA 5585
- Firepower 1000
- Firepower 2100
- Firepower 4100
- Firepower 9300

Atténuation potentielle

Activation de la transmission tunnel partagée

Par défaut, les stratégies de groupe sur l'ASA et le FTD implémentent le tunnel. Cela enverra tout le trafic généré par les clients RA sur le VPN à traiter par la tête de réseau. Étant donné que le chiffrement et le déchiffrement des paquets sont directement liés à l'utilisation du CPU, il est important de s'assurer que seul le trafic nécessaire est géré par la tête de réseau VPN, comme le permet la politique de sécurité de l'entreprise. Envisagez d'utiliser une stratégie de tunnel partagé plutôt qu'un tunnel complet pour éviter toute charge inutile de la tête de réseau VPN.

- Guide de fractionnement de tunnel ASA
- Guide de fractionnement du tunnel FTD (FMC)

Note: Tunnel All implémente une politique de sécurité des paramètres à l'échelle de l'entreprise, tandis que le fractionnement du tunnel s'appuie sur le périphérique client pour protéger le trafic Internet de l'utilisateur. Cisco fournit un outil de sécurité supplémentaire comme Umbrella afin de protéger les utilisateurs VPN lorsqu'une stratégie de tunnel partagé est utilisée.

Implémenter l'équilibrage de charge VPN (ASA uniquement)

L'équilibrage de charge VPN est une fonctionnalité prise en charge sur les plates-formes ASA qui permet à deux ASA ou plus de partager la charge de session VPN. Si les deux périphériques prennent en charge 500 homologues VPN, en configurant l'équilibrage de charge VPN entre eux, les périphériques prendront en charge un total de 1 000 homologues VPN entre eux. Cette fonctionnalité peut être utilisée pour augmenter le nombre d'utilisateurs VPN simultanés au-delà de ce qu'un seul périphérique peut gérer. Pour plus d'informations sur l'équilibrage de charge VPN, y compris l'algorithme d'équilibrage de charge, cliquez ici : Équilibrage de charge VPN

Optimisation de la configuration

Les services supplémentaires activés sur la plate-forme augmenteront la quantité de traitement et de charge sur le périphérique. Par exemple, IPS, déchiffrement SSL, NAT, etc. Envisagez de configurer le périphérique en tant que concentrateur VPN qui ne ferme que les sessions VPN.

Sélection du protocole de tunnel

Par défaut, les stratégies de groupe sur les ASA sont configurées pour tenter d'établir un tunnel DTLS. Si le trafic UDP 443 est bloqué entre la tête de réseau VPN et le client AnyConnect, il rebascule automatiquement vers TLS. Il est recommandé d'utiliser DTLS ou IKEv2 pour augmenter les performances de débit VPN maximum. DTLS offre de meilleures performances que TLS en raison d'une surcharge de protocole moindre. IKEv2 offre également un meilleur débit que TLS. En outre, l'utilisation de chiffrement AES-GCM peut améliorer légèrement les performances. Ces chiffrements sont disponibles dans TLS 1.2, DTLS 1.2 et IKEv2.

Appliquer la QoS par tunnel (FTD uniquement)

La QoS peut être mise en oeuvre pour limiter la quantité de trafic envoyé aux utilisateurs AnyConnect dans la direction sortante. Ce faisant, la tête de réseau VPN peut imposer à chaque client d'accès distant sa juste part de bande passante de sortie. Pour plus d'informations, cliquez ici : Configuration FTD

Implémenter un BIOS Crypto Engine Accelerator (ASA uniquement)

Le BIOS Crypto Engine Accelerator est utilisé pour réallouer les coeurs de chiffrement afin de favoriser un protocole de chiffrement par rapport à l'autre (SSL ou IPsec). L'objectif est d'optimiser le débit d'AnyConnect si la majorité des tunnels VPN utilisent IPsec ou SSL. La mise en oeuvre de cette commande peut entraîner une interruption de service et donc une fenêtre de maintenance est nécessaire. En outre, l'amélioration des performances (débit AnyConnect et utilisation du CPU) peut varier en fonction du profil de trafic. Si la tête de réseau VPN ne met fin qu'aux sessions SSL ou uniquement aux sessions IPsec, cette commande peut être prise en compte pour optimiser davantage la tête de réseau VPN. La référence de commande se trouve ici :

Référence des commandes

Pour vérifier l'allocation de noyau de chiffrement actuelle, exécutez la commande ***show crypto accélérator load-balance***. Cette commande n'affiche pas la quantité totale d'utilisation de chiffrement que le périphérique est capable de gérer - Elle indique le rapport du trafic ssl ou ipsec qui est alloué à chaque coeur. Pour trouver la quantité approximative d'utilisation sur le périphérique, reportez-vous à la section ci-dessus sur **Utilisation élevée du CPU** et comparez la valeur calculée à la valeur de la feuille de données de la plate-forme.

Sur une plate-forme ASA qui termine principalement l'accès à distance SSLVPN, il est recommandé que l'allocation de noyau de cryptage soit ajustée pour favoriser SSL avec la commande ***crypto engine accélérator-biais ssl***.

L'exemple suivant montre l'allocation de base sur un ASA5555 avec la commande ***crypto engine Accelerator-partial ssl*** pour favoriser les clients AnyConnect SSL :

```
asa# sh run all crypto engine
crypto engine accelerator-bias ssl
asa# show crypto accelerator load-balance

[..]
                  Crypto SSL Load Balancing Stats:
                  ================================

Engine      Crypto Cores             SSL Sessions            Active Session
                                                             Distribution (%)
======     ==============      ============================   ================
  0        IPSEC 1, SSL 7      Total: 166714  Active:   205         100.0%
[..]
```

La distribution de session active sera toujours de 100 %, quelle que soit l'utilisation actuelle du cryptage de la plate-forme.

Note: Le rééquilibrage du coeur de réseau cryptographique est disponible sur les plates-formes suivantes : ASA 5585, 5580, 5545/555, 4110, 4120, 4140, 4150, SM-24, SM-36, SM-44 et ASASM.

Forum aux questions

Licence

Q : Pourquoi ne puis-je pas télécharger le logiciel AnyConnect ?

A : Vous devez acheter la licence AnyConnect Plus ou Apex pour pouvoir télécharger le client AnyConnect. Après cela, vous devriez avoir droit. Si vous n'avez pas droit à la licence AnyConnect Apex ou Plus, ouvrez un dossier avec le droit de résoudre ce problème.

Q : Pourquoi le 99999 Acheté pour la licence AnyConnect apparaît-il dans mon compte de licence Smart ?

A : Cela est prévu avec certaines licences AnyConnect, telles que les licences AnyConnect Plus perpétuelles ou non baguées AnyConnect Plus ou Apex.

Q : Qu'est-ce qui détermine quand “ En cours d'utilisation ” décréter ?

A : Cette valeur diminue chaque fois qu'un périphérique utilisant la licence AnyConnect est enregistré. Par exemple, si vous enregistrez FMC, ajoutez la licence AnyConnect Plus à un périphérique, la valeur En cours d'utilisation de la licence AnyConnect Plus diminuera. Cette valeur **NE** diminue **PAS** en fonction des sessions utilisateur actuelles. L'enregistrement des périphériques ASAv **NE** décréte **PAS** le nombre ” “ en cours d'utilisation. C'est un problème cosmétique connu. Vous ne pouvez pas enregistrer plus de périphériques que le nombre d'utilisateurs autorisés qui ont acheté.

Q : Qu'est-ce qui détermine la valeur Achetée ?

A : La valeur d'achat est déterminée par le nombre d'utilisateurs autorisés achetés avec la licence. Par exemple, une licence AnyConnect Plus de 25 utilisateurs aura un nombre de 25 Achetés.

Q : Comment activer le chiffrement fort ?

A : Afin d'activer le chiffrement fort, vous devez cocher la case “ Autoriser la fonctionnalité contrôlée par l'exportation sur les produits enregistrés avec ce ” de jeton lors de la création du jeton d'enregistrement.

Q : Comment puis-je passer de PAK à Smart Licensing ?

A : Un dossier doit être ouvert avec l'autorisation pour cela.

Q : Si j'ai une licence utilisateur « X », que se passera-t-il si « X+1 » ou plus d'utilisateurs se connectent au périphérique ?

A : Avec la licence Apex et Plus, la capacité utilisateur VPN totale du périphérique est déverrouillée. Tant que le périphérique n'atteint pas sa limite utilisateur vpn maximale, il continue à accepter les connexions. Il n'y a aucune application sur le périphérique pour les sessions utilisateur VPN et elle est basée sur l'honneur. Il est de votre responsabilité d'acheter des licences utilisateur autorisées supplémentaires si l'utilisation de la session vpn pour le périphérique doit être augmentée. Pour vérifier le nombre maximal d'utilisateurs pris en charge par le périphérique, consultez la fiche technique du périphérique sur le site Web de Cisco ou exécutez ***show vpn-sessiondb*** et examinez le ” de capacité VPN totale du périphérique “. Pour les ASA, vous pouvez également exécuter les commandes ***show version*** ou ***show vpn-sessiondb license-summary***.

Q : Comment vérifier que la licence est activée sur mon périphérique ?

A : Sur les FTD, vous ne pourrez pas déployer la configuration AnyConnect si la licence n'est pas activée. Sur les ASA, vous pouvez consulter la ***commande show version*** ou ***show vpn-sessiondb license-summary*** pour déterminer le nombre d'utilisateurs autorisés. Sans licence activée, le maximum sera de 2 utilisateurs. Remarque sur l'ASA, les commandes mentionnées ci-dessus n'afficheront pas les informations de licence Plus/Apex. Ceci est suivi avec la demande d'amélioration CSCuw74731.

Configuration

Q : Quelles plates-formes ASA puis-je utiliser pour l'équilibrage de charge VPN ? Puis-je utiliser différentes plates-formes matérielles ASA ou différentes versions logicielles dans un cluster d'équilibrage de charge VPN ?

R : Oui, un cluster d'équilibrage de charge VPN peut se composer de différents modèles ASA physiques ou virtuels, y compris ASAv. Cependant, il est généralement recommandé que le cluster soit homogène. Si différentes versions de logiciel sont utilisées dans un cluster d'équilibrage de charge vpn, seules les sessions IPsec sont prises en charge. Pour plus d'informations, reportez-vous à : Directives et limitations pour l'équilibrage de charge VPN.

Q : Comment configurer le fractionnement en canaux ? Et pouvez-vous exclure certains types de trafic d'applications, tels qu'Office 365, d'être tunnelisé dans une configuration à tunnel partagé ?

A : Voir l'article de la communauté Cisco AnyConnect Split Tunneling pour des exemples de configuration de différents cas d'utilisation. Vous pouvez également utiliser une combinaison de fractionnement en canaux et de fractionnement en canaux dynamiques pour obtenir un fractionnement en canaux basé sur les applications. Pour obtenir un exemple d'optimisation de la transmission tunnel partagée AnyConnect pour Office 365 et WebEx, consultez Comment optimiser Anyconnect pour les connexions Microsoft Office365 et Cisco Webex.

Q : Je vois l'erreur « Avertissement de certificat non approuvé » lors de la connexion à une tête de réseau ASA avec AnyConnect. Pourquoi cela se produit-il ?

A : Cela est probablement dû au fait que la tête de réseau utilise un certificat auto-signé. Pour résoudre ce problème, un certificat SSL peut être acheté auprès d'une autorité de certification et installé sur l'ASA de tête de réseau. Pour connaître les étapes de mise en oeuvre détaillées, reportez-vous à : Configurer ASA : Installation et renouvellement du certificat numérique SSL.

Q : Les certificats génériques sont-ils pris en charge sur les têtes de réseau Cisco RAVPN ?

A : Oui, les caractères génériques et les certificats avec des noms de domaine alternatifs (SAN) DNS sont pris en charge.

Q : Un seul périphérique peut-il utiliser à la fois l'équilibrage de charge et le basculement ?

A : Le basculement actif/veille est pris en charge avec l'équilibrage de charge VPN. Le périphérique de secours prend immédiatement le relais sans impact sur le tunnel VPN en cas de défaillance de l'unité active. L'équilibrage de charge VPN n'est pas pris en charge avec une configuration de basculement actif/actif.

Surveillance

Q : Quelle MIB SNMP puis-je utiliser pour surveiller l'utilisation du processeur ASA ?

R : CISCO-PROCESS-MIB peut être utilisé pour surveiller l'utilisation du processeur ASA. Pour obtenir la liste complète des MIB prises en charge, reportez-vous à la liste de support MIB des appliances de sécurité adaptatives. Également pour obtenir la liste des MIB et OID SNMP pris en charge pour un ASA spécifique, vous pouvez émettre la commande suivante : ***show snmp-server oidlist.***

Q : Comment contrôler le nombre d'utilisateurs actuellement connectés à une tête de réseau VPN ?

A : Utilisez ***show vpn-sessiondb*** à partir de l'interface de ligne de commande pour vérifier le nombre actuel d'utilisateurs sur un ASA, un FTD ou une MIB SNMP.

CISCO-REMOTE-ACCESS-MONITOR-MIB.

Dépannage

Q : Certains de nos utilisateurs VPN AnyConnect semblent subir des déconnexions fréquentes. Comment résoudre de tels problèmes :

A : Pour le dépannage de la déconnexion VPN et d'autres problèmes courants d'AnyConnect, reportez-vous au Guide de dépannage du client VPN AnyConnect - Problèmes courants.

Q : Lorsqu'un certain nombre d'utilisateurs se connectent à la tête de réseau VPN, aucun autre utilisateur ne peut se connecter. La licence est activée sur le périphérique et ***show vpn-sessiondb*** indique que le périphérique peut gérer plus d'utilisateurs. Quel pourrait être le problème ?

A : Vérifiez le pool d'adresses locales VPN pour ces utilisateurs pour vous assurer que le nombre d'utilisateurs connectés ne dépasse pas le nombre d'adresses disponibles. Vous pouvez vérifier à l'aide de la commande ***show ip local pool [pool-name]***. Une autre cause potentielle sur les plates-formes plus anciennes est que la commande ***vpn-sessiondb max-anyconnect-premium-or-essentials-limit*** a une valeur faible. Vous pouvez vérifier cela avec la commande ***show run all vpn-sessiondb***. Si c'est le cas, la valeur peut être augmentée ou la commande peut être supprimée pour empêcher cette limite.

Obtention d'aide supplémentaire

Pour obtenir de l'aide supplémentaire, contactez le TAC. Un contrat d'assistance valide est requis : Coordonnées du service d’assistance Cisco à l’échelle mondiale

Vous pouvez également visiter la communauté VPN Cisco ici.

En outre, vous pouvez consulter les podcasts du TAC Security Show

Références

Vous trouverez ci-dessous des liens supplémentaires vers d'autres ressources utiles pour les déploiements AnyConnect et la gestion des problèmes liés à COVOD-19 en général.

- La sécurité Cisco répond à l'augmentation du nombre de travailleurs distants - Communauté Cisco
- Guide de commande AnyConnect
- FAQ sur les licences AnyConnect
- FAQ AnyConnect VPN, ASA et FTD pour les télétravailleurs sécurisés