SSLVPN avec l'exemple de configuration de Téléphones IP

Contenu

Introduction

Ce document décrit comment configurer des Téléphones IP au-dessus de Secure Sockets Layer VPN (VPN SSL), également connu sous le nom de webvpn. Deux Cisco Unified Communications Managers (CallManagers) et trois types de Certificats sont utilisés avec cette solution. Les CallManagers sont :

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified Communications Manager Express (Cisco Unified CME)

Les types de certificat sont :

- Certificats Auto-signés
- Tiers délivre un certificat, comme confient, Thawte, et GoDaddy
- Autorité de certification (CA) des dispositifs de sécurité du Cisco IOS ®/Adaptive (ASA)

Le concept clé à comprendre est que, une fois la configuration sur la passerelle de VPN SSL et le CallManager sont terminés, vous doit joindre les Téléphones IP localement. Ceci permet aux téléphones de joindre le CUCM et d'utiliser les informations correctes et des Certificats VPN. Si les téléphones ne sont pas joints localement, ils ne peuvent pas trouver la passerelle de VPN SSL et n'ont pas les Certificats corrects pour se terminer la prise de contact de VPN SSL.

Les configurations les plus communes sont CUCM/Unified CME avec les Certificats auto-signés par ASA et les Certificats auto-signés par Cisco IOS. En conséquence, il est le plus facile les configurer.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Communications Manager (CUCM) ou Cisco Unified Communications Manager Express (Cisco Unified CME)
- VPN SSL (webvpn)
- Appliance de sécurité adaptable Cisco (ASA)
- Le certificat tape, comme auto-signé, la tierce partie, et les autorités de certification

Composants utilisés

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

- Licence premium ASA.
- Permis de téléphone d'AnyConnect VPN.
  - Pour l'ASA libérez 8.0.x, le permis est AnyConnect pour le téléphone de Linksys.
  - Pour l'ASA libérez 8.2.x ou plus tard, le permis est AnyConnect pour le téléphone de Cisco VPN.
- Passerelle de VPN SSL : ASA 8.0 ou plus tard (avec un AnyConnect pour le permis de téléphone de Cisco VPN), ou version du logiciel Cisco IOS 12.4T ou plus tard.
  - La version du logiciel Cisco IOS 12.4T ou plus tard n'est pas formellement prise en charge comme documenté dans le guide de configuration de VPN SSL.
  - Dans le Logiciel Cisco IOS version 15.0(1)M, la passerelle de VPN SSL est une caractéristique poste-comptée d'autorisation sur Cisco 880, Cisco 890, Cisco 1900, Cisco 2900, et Cisco 3900 Plateformes. Un permis valide est exigé pour une session réussie de VPN SSL.
- CallManager : CUCM 8.0.1 ou plus tard, ou Unified CME 8.5 ou plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

> Remarques :
>
> Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus

d'informations sur les commandes utilisées dans cette section.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Configuration de base de VPN SSL ASA

La configuration de base de VPN SSL ASA est décrite dans ces documents :

- ASA 8.x : Exemple de configuration de l'accès VPN avec le client VPN AnyConnect à l'aide d'un certificat auto-signé
- Configurer des connexions AnyConnect VPN Client

Une fois que cette configuration est complète, un PC distant de test devrait pouvoir se connecter à la passerelle de VPN SSL, se connecte par l'intermédiaire d'AnyConnect, et cingle le CUCM. Assurez que l'ASA a un AnyConnect pour le permis de téléphone IP de Cisco. (Utilisez la commande de **ver d'exposition**.) Le port 443 de TCP et UDP doit être ouvert entre la passerelle et le client.

Remarque: le VPN SSL Chargement-équilibré n'est pas pris en charge pour des téléphones VPN.

CUCM : VPN SSL ASA avec la configuration Auto-signée de Certificats

Référez-vous au VPN SSL de téléphone IP à l'ASA utilisant AnyConnect pour plus d'informations détaillées.

L'ASA doit avoir un permis pour AnyConnect pour le téléphone de Cisco VPN. Après que vous configuriez le VPN SSL, vous configurez alors votre CUCM pour le VPN.

1. Employez cette commande afin d'exporter le certificat auto-signé de l'ASA :

   `ciscoasa(config)# crypto ca export trustpoint name identity-certificate` Cette commande affiche un certificat d'identité PEM-encodé au terminal.
2. Copiez et collez le certificat à un éditeur de texte, et sauvegardez-le comme un fichier .pem. Soyez sûr d'inclure les lignes de CERTIFICAT de COMMENCER et de CERTIFICAT d'EXTRÉMITÉ, ou le certificat n'importera pas correctement. Ne modifiez pas le format du certificat parce que ceci posera des problèmes quand les essais de téléphone authentifier à l'ASA.
3. Naviguez vers la **gestion de Cisco Unified > la Gestion de Sécurité > de certificat > le certificat de téléchargement/chaîne de certificat du système d'exploitation** afin de charger le fichier du certificat à la section Gestion de CERTIFICAT du CUCM.
4. Téléchargez les Certificats CallManager.pem, CAPF.pem, et Cisco_Manufacturing_CA.pem de la même zone utilisée pour charger les Certificats auto-signés de l'ASA (voir l'étape 1), et sauvegardez-les à votre appareil de bureau.
   1. Par exemple, afin d'importer le CallManager.pem à l'ASA, utilisez ces commandes :

```
ciscoasa(config)# crypto ca trustpoint certificate-name
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate certificate-name
```

2. Quand vous êtes incité à copier et coller le certificat correspondant pour le point de confiance, ouvrez le fichier que vous vous êtes enregistré du CUCM, alors de la copie et collez le certificat Base64-encoded. Soyez sûr d'inclure le CERTIFICAT de COMMENCER et le CERTIFICAT d'EXTRÉMITÉ raye (avec des traits d'union).
3. **L'extrémité de** type, appuient sur alors le **retour**.
4. Une fois incité à recevoir le certificat, tapez **oui**, alors appuyez sur **entrent**.
5. Répétez les étapes 1 4 pour les deux autres Certificats (CAPF.pem, Cisco_Manufacturing_CA.pem) du CUCM.

5. Configurez le CUCM pour les configurations du VPN correctes, comme décrit dans CUCM IPphone VPN config.pdf.

   Remarque: La passerelle VPN configurée sur le CUCM doit apparier l'URL qui est configuré sur la passerelle VPN. Si la passerelle et l'URL ne s'assortissent pas, le téléphone ne peut pas résoudre l'adresse, et vous ne verrez pas qu'en met au point sur la passerelle VPN.

- Sur le CUCM : L'URL de passerelle VPN est https://192.168.1.1/VPNPhone
- Sur l'ASA, utilisez ces commandes :

```
ciscoasa# configure terminal
ciscoasa(config)# tunnel-group VPNPhones webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://192.168.1.1/VPNPhone
enable
ciscoasa(config-tunnel-webvpn)# exit
```

- Vous pouvez utiliser ces commandes sur Adaptive Security Device Manager (ASDM) ou sous le profil de connexion.

CUCM : Le VPN SSL ASA avec la tierce partie délivre un certificat la configuration

Cette configuration est très semblable à la configuration décrite dans CUCM : ASA SSLVPN avec la section de configuration Auto-signée de Certificats, sauf que vous utilisent de tiers Certificats. Configurez le VPN SSL sur l'ASA avec de tiers Certificats comme décrit dans ASA 8.x installez manuellement les Certificats de constructeur de tiers pour l'usage avec l'exemple de configuration de webvpn.

Remarque: Vous devez copier la pleine chaîne de certificat de l'ASA sur le CUCM et inclure tous les intermédiaire et certificats racine. Si le CUCM n'inclut pas la pleine chaîne, les téléphones n'ont pas les Certificats nécessaires à authentifier et échoueront la prise de contact de VPN SSL.

Configuration de base de VPN SSL IOS

Remarque: Des Téléphones IP sont indiqués en tant que non pris en charge dans le VPN SSL IOS ; les configurations sont dans le meilleur effort seulement.

La configuration de base de VPN SSL de Cisco IOS est décrite dans ces documents :

- Exemple de configuration d'un client VPN SSL (SVC) sur IOS avec SDM
- Exemple de configuration client VPN AnyConnect sur un routeur IOS avec pare-feu de stratégie basée sur les zones

Une fois que cette configuration est complète, un PC distant de test devrait pouvoir se connecter à la passerelle de VPN SSL, se connecte par l'intermédiaire d'AnyConnect, et cingle le CUCM. Dans le Cisco IOS 15.0 et plus tard, vous devez avoir un permis valide de VPN SSL de se terminer cette tâche. Le port 443 de TCP et UDP doit être ouvert entre la passerelle et le client.

CUCM : VPN SSL IOS avec la configuration Auto-signée de Certificats

Cette configuration est semblable à la configuration décrite dans CUCM : ASA SSLVPN avec la tierce partie délivre un certificat la configuration et le CUCM : ASA SSLVPN avec les sections de configuration Auto-signées de Certificats. Les différences sont :

1. Employez cette commande afin d'exporter le certificat auto-signé du routeur :

```
R1(config)# crypto pki export trustpoint-name pem terminal
```

2. Employez ces commandes afin d'importer les Certificats CUCM :

```
R1(config)# crypto pki trustpoint certificate-name
R1(config-ca-trustpoint)# enrollment terminal
R1(config)# crypto ca authenticate certificate-name
```

La configuration de contexte de webvpn devrait afficher ce texte :

```
gateway webvpn_gateway domain VPNPhone
```

Configurez le CUCM comme décrit dans CUCM : ASA SSLVPN avec la section de configuration Auto-signée de Certificats.

CUCM : Le VPN SSL IOS avec la tierce partie délivre un certificat la configuration

Cette configuration est semblable à la configuration décrite dans CUCM : ASA SSLVPN avec la section de configuration Auto-signée de Certificats. Configurez votre webvpn avec un tiers certificat.

> Remarque: Vous devez copier la pleine chaîne de certificat de webvpn sur le CUCM et inclure tous les intermédiaire et certificats racine. Si le CUCM n'inclut pas la pleine chaîne, les téléphones n'ont pas les Certificats nécessaires à authentifier et échoueront la prise de contact de VPN SSL.

Unified CME : Le VPN SSL ASA/Router avec les Certificats Auto-signés/tierce partie délivre un certificat la configuration

La configuration pour l'Unified CME est semblable aux configurations du CUCM ; par exemple, les configurations de point final de webvpn sont identiques. La seule différence important est les configurations de l'agent d'appel d'Unified CME. Configurez le groupe VPN et la règle VPN pour l'Unified CME comme décrit en configurant le client de VPN SSL pour des Téléphones IP de SCCP.

Remarque: L'Unified CME prend en charge seulement le Protocole SCCP (Skinny Call Control Protocol) et ne prend en charge pas le Protocole SIP (Session Initiation Protocol) pour des téléphones VPN.

Remarque: Il n'y a aucun besoin d'exporter les Certificats de l'Unified CME à l'ASA ou au routeur. Vous devez seulement exporter les Certificats de l'ASA ou le webvpn gateway de routeur à l'Unified CME.

Afin d'exporter les Certificats du webvpn gateway, référez-vous à la section ASA/router. Si vous utilisez un tiers certificat, vous devez inclure la pleine chaîne de certificat. Afin d'importer les Certificats à l'Unified CME, utilisez la même méthode qu'utilisée aux Certificats d'importation dans un routeur :

```
CME(config)# crypto pki trustpoint certificate-name
CME(config-ca-trustpoint)# enrollment terminal
CME(config)# crypto ca authenticate certificate-name
```

Téléphones IP UC 520 avec la configuration de VPN SSL

Le téléphone IP modèle UC 520 de gamme de Cisco Unified Communications 500 est très différent des configurations CUCM et CME.

- Puisque le téléphone IP UC 520 est le CallManager et le webvpn gateway, il n'y a aucun besoin de configurer des Certificats entre les deux.
- Configurez le webvpn sur un routeur comme vous normalement avec les Certificats auto-signés ou les Certificats de tierce partie.
- Le téléphone IP UC 520 a construit dans le client de webvpn, et vous pouvez le configurer juste comme vous un PC normal vous connecteriez au webvpn. Entrez dans la passerelle, puis la combinaison de nom d'utilisateur/mot de passe.
- Le téléphone IP UC 520 est compatible avec les téléphones de la STATION THERMALE 525G de téléphone IP de Cisco Small Business.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.