Exemple de configuration de SSLVPN avec des téléphones IP

Contenu

Introduction

Ce document décrit comment configurer des téléphones IP sur un VPN SSL (Secure Sockets Layer VPN), également appelé WebVPN. Deux Cisco Unified Communications Manager (CallManager) et trois types de certificats sont utilisés avec cette solution. Les CallManager sont les suivants :

- Gestionnaire de communications unifiées de Cisco (version CUCM)
- Cisco Unified Communications Manager Express (Cisco Unified CME)

Les types de certificat sont les suivants :

- Certificats auto-signés
- Certificats tiers, tels qu'Entrust, Thawte et GoDaddy
- Autorité de certification Cisco IOS®/Adaptive Security Appliance (ASA)

Le concept clé à comprendre est que, une fois la configuration sur la passerelle VPN SSL et CallManager terminée, vous devez joindre localement les téléphones IP. Cela permet aux téléphones de rejoindre le CUCM et d'utiliser les informations et certificats VPN corrects. Si les téléphones ne sont pas connectés localement, ils ne trouvent pas la passerelle VPN SSL et ne disposent pas des certificats appropriés pour effectuer la connexion VPN SSL.

Les configurations les plus courantes sont CUCM/Unified CME avec certificats auto-signés ASA et certificats auto-signés Cisco IOS. Par conséquent, ils sont les plus faciles à 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)
- Appareil de sécurité adaptatif Cisco (ASA)
- Types de certificats, tels que les autorités de certification autosignées, tierces et

Components Used

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

- Licence ASA Premium.
- Licence de téléphone VPN AnyConnect.
  - Pour ASA version 8.0.x, la licence est AnyConnect pour Linksys Phone.
  - Pour ASA version 8.2.x ou ultérieure, la licence est AnyConnect pour téléphone VPN Cisco.
- Passerelle VPN SSL : ASA 8.0 ou version ultérieure (avec une licence AnyConnect pour Cisco VPN Phone), ou le logiciel Cisco IOS version 12.4T ou ultérieure.
  - La version 12.4T ou ultérieure du logiciel Cisco IOS n'est pas officiellement prise en charge comme indiqué dans le Guide de configuration VPN SSL.
  - Dans la version 15.0(1)M du logiciel Cisco IOS, la passerelle VPN SSL est une fonction de gestion des licences sur les plates-formes Cisco 880, Cisco 890, Cisco 1900, Cisco 2900 et Cisco 3900. Une licence valide est requise pour une session VPN SSL réussie.
- CallManager : CUCM 8.0.1 ou version ultérieure, ou Unified CME 8.5 ou version ultérieure.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

> **Remarques :**
>
> Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.
>
> L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge

certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Configuration VPN SSL ASA de base

La configuration VPN SSL ASA de base 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
- Configuration des connexions client VPN AnyConnect

Une fois cette configuration terminée, un PC de test distant doit pouvoir se connecter à la passerelle VPN SSL, se connecter via AnyConnect et envoyer une requête ping au CUCM. Assurez-vous que l'ASA dispose d'une licence AnyConnect pour téléphone IP Cisco. (Utilisez la commande **show ver**.) Les ports TCP et UDP 443 doivent être ouverts entre la passerelle et le client.

Note: Le VPN SSL équilibré en charge n'est pas pris en charge pour les téléphones VPN.

CUCM: Configuration VPN SSL ASA avec certificats auto-signés

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

L'ASA doit disposer d'une licence pour AnyConnect pour le téléphone VPN Cisco. Après avoir configuré le VPN SSL, vous configurez ensuite CUCM pour le VPN.

1. Utilisez 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 codé en pem sur le terminal.
2. Copiez et collez le certificat dans un éditeur de texte, puis enregistrez-le en tant que fichier .pem. Veillez à inclure les lignes DÉBUT CERTIFICAT et FIN CERTIFICAT, sinon le certificat ne sera pas importé correctement. Ne modifiez pas le format du certificat, car cela entraînera des problèmes lorsque le téléphone tente de s'authentifier auprès de l'ASA.
3. Accédez à **Cisco Unified Operating System Administration > Security > Certificate Management > Upload Certificate/Certificate Chain** afin de charger le fichier de certificat dans la section CERTIFICATE MANAGEMENT de CUCM.
4. Téléchargez les certificats CallManager.pem, CAPF.pem et Cisco_Manufacturing_CA.pem à partir de la même zone utilisée pour charger les certificats auto-signés à partir de l'ASA (voir Étape 1), puis enregistrez-les sur votre bureau.
   1. Par exemple, afin d'importer le fichier CallManager.pem dans l'ASA, utilisez les commandes suivantes :

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

2. Lorsque vous êtes invité à copier et coller le certificat correspondant au point de confiance, ouvrez le fichier que vous avez enregistré à partir du CUCM, puis copiez et collez le certificat codé en base64. Veillez à inclure les lignes BEGIN CERTIFICATE et END CERTIFICATE (avec des traits d'union).
3. Tapez **end**, puis appuyez sur **Return**.
4. Lorsque vous êtes invité à accepter le certificat, tapez **yes**, puis appuyez sur **Entrée**.
5. Répétez les étapes 1 à 4 pour les deux autres certificats (CAPF.pem, Cisco_Manufacturing_CA.pem) à partir de CUCM.

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

   Note: La passerelle VPN configurée sur CUCM doit correspondre à l'URL configurée sur la passerelle VPN. Si la passerelle et l'URL ne correspondent pas, le téléphone ne peut pas résoudre l'adresse et aucun débogage ne s'affiche sur la passerelle VPN.

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

```
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 l'ASDM (Adaptive Security Device Manager) ou sous le profil de connexion.

CUCM: VPN SSL ASA avec configuration de certificats tiers

Cette configuration est très similaire à la configuration décrite dans CUCM : Section Configuration de ASA SSLVPN avec certificats auto-signés, sauf que vous utilisez des certificats tiers. Configurez le VPN SSL sur l'ASA avec des certificats tiers comme décrit dans l'exemple de configuration d'ASA 8.x Installer manuellement des certificats de fournisseurs tiers pour une utilisation avec WebVPN.

Note: Vous devez copier la chaîne de certificats complète de l'ASA vers le CUCM et inclure tous les certificats intermédiaires et racine. Si CUCM n'inclut pas la chaîne complète, les téléphones ne disposent pas des certificats nécessaires pour s'authentifier et échoueront la connexion VPN SSL.

Configuration VPN SSL IOS de base

Note: Les téléphones IP sont désignés comme non pris en charge dans le VPN SSL IOS ; les configurations sont au mieux uniquement.

La configuration VPN SSL de base 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 cette configuration terminée, un PC de test distant doit pouvoir se connecter à la passerelle VPN SSL, se connecter via AnyConnect et envoyer une requête ping au CUCM. Dans Cisco IOS 15.0 et versions ultérieures, vous devez disposer d'une licence VPN SSL valide pour effectuer cette tâche. Les ports TCP et UDP 443 doivent être ouverts entre la passerelle et le client.

CUCM: Configuration VPN SSL IOS avec certificats auto-signés

Cette configuration est similaire à la configuration décrite dans CUCM : Configuration ASA SSLVPN avec certificats tiers et CUCM : Sections de configuration ASA SSLVPN avec certificats auto-signés. Les différences sont les suivantes :

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

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

2. Utilisez 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 WebVPN doit afficher le texte suivant :

```
gateway webvpn_gateway domain VPNPhone
```

Configurez CUCM comme décrit dans CUCM : Section Configuration de ASA SSLVPN avec certificats auto-signés.

CUCM: VPN SSL IOS avec configuration de certificats tiers

Cette configuration est similaire à la configuration décrite dans CUCM : Section Configuration de ASA SSLVPN avec certificats auto-signés. Configurez votre WebVPN avec un certificat tiers.

> **Note**: Vous devez copier la chaîne de certificats WebVPN complète dans CUCM et inclure tous les certificats intermédiaires et racine. Si CUCM n'inclut pas la chaîne complète, les téléphones ne disposent pas des certificats nécessaires pour s'authentifier et échoueront la connexion VPN SSL.

Unified CME : VPN SSL ASA/Router avec configuration de certificats auto-signés/de certificats tiers

La configuration de Unified CME est similaire aux configurations de CUCM ; par exemple, les configurations des points de terminaison WebVPN sont identiques. La seule différence significative est la configuration de l'agent d'appel Unified CME. Configurez le groupe VPN et la

stratégie VPN pour Unified CME comme décrit dans Configuration du client VPN SSL pour les téléphones IP SCCP.

> **Note**: Unified CME prend uniquement en charge le protocole SCCP (Skinny Call Control Protocol) et ne prend pas en charge le protocole SIP (Session Initiation Protocol) pour les téléphones VPN.

> **Note**: Il n'est pas nécessaire d'exporter les certificats de Unified CME vers l'ASA ou le routeur. Vous devez uniquement exporter les certificats de la passerelle WebVPN ASA ou du routeur vers Unified CME.

Afin d'exporter les certificats à partir de la passerelle WebVPN, référez-vous à la section ASA/routeur. Si vous utilisez un certificat tiers, vous devez inclure la chaîne de certificats complète. Afin d'importer les certificats dans Unified CME, utilisez la même méthode que celle utilisée pour importer les certificats 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 configuration VPN SSL

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

- Puisque le téléphone IP UC 520 est à la fois CallManager et la passerelle WebVPN, il n'est pas nécessaire de configurer des certificats entre les deux.
- Configurez le WebVPN sur un routeur comme vous le feriez normalement avec des certificats auto-signés ou des certificats tiers.
- Le téléphone IP UC 520 dispose d'un client WebVPN intégré et vous pouvez le configurer comme vous le feriez pour un PC normal pour vous connecter à WebVPN. Saisissez la passerelle, puis la combinaison nom d'utilisateur/mot de passe.
- Le téléphone IP UC 520 est compatible avec les téléphones IP Cisco Small Business SPA 525G.

Vérification

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

Dépannage

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