Configurez le téléphone d'AnyConnect VPN avec l'authentification de certificat sur une ASA

Contenu

Introduction

Ce document fournit une configuration d'échantillon qui affiche comment configurer les périphériques de l'appliance de sécurité adaptable (ASA) et du CallManager pour fournir l'authentification de certificat pour les clients d'AnyConnect qui s'exécutent sur des Téléphones IP de Cisco. Après que cette configuration soit complète, les Téléphones IP de Cisco peuvent établir les connexions VPN à l'ASA qui se servent des Certificats afin de sécuriser la transmission.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Permis de la meilleure qualité SSL d'AnyConnect
- AnyConnect pour le permis de téléphone de Cisco VPN

Personne à charge sur la version ASA, vous verrez « AnyConnect pour le téléphone de Linksys » pour la release 8.0.x ASA ou « AnyConnect pour le téléphone de Cisco VPN » pour la release 8.2.x ASA ou plus tard.

Composants utilisés

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

- ASA - Version 8.0(4) ou plus tard
- Le téléphone IP modèle - 7942/7962/7945/7965/7975
- Téléphones - 8961/9951/9971 avec le micrologiciel de la version 9.1(1)
- Téléphone - Release 9.0(2)SR1S - Protocole SCCP (Skinny Call Control Protocol) ou plus tard
- Cisco Unified Communications Manager (CUCM) - Version 8.0.1.100000-4 ou plus tard

Les releases utilisées dans cet exemple de configuration incluent :

- ASA - Version 9.1(1)
- CallManager version 8.5.1.10000-26

Pour une liste complète de téléphones pris en charge dans votre version CUCM, terminez-vous ces étapes :

1. Ouvrez cet URL : *IP Address>:8443/cucreports/systemReports.do de serveur de* https:// *<CUCM*
2. Choisissez la **liste de caractéristique de téléphone d'Unified CM > génèrent un nouveaux état > caractéristique : Réseau privé virtuel**.

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.

Conventions

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

Types de certificat de téléphone

Cisco utilise des ces certificat saisit des téléphones :

- Certificat installé par fabricant (MIC) - MICs sont inclus sur chacun des 7941, 7961, et Téléphones IP de Cisco de plus nouveau modèle. MICs sont les Certificats 2048-bit principaux qui sont signés par l'Autorité de certification (CA) de Cisco. Quand une MIC est présente, il n'est pas nécessaire d'installer le certificat significatif a localement - (LSC). Pour que le CUCM fasse confiance au certificat MIC, il utilise les Certificats CA préinstallés CAP-RTP-001, CAP-RTP-002, et Cisco_Manufacturing_CA dans sa mémoire de confiance de certificat.
- LSC - Le LSC sécurise la connexion entre CUCM et le téléphone après que vous configuriez le mode de sécurité des périphériques pour l'authentification ou le cryptage.Le LSC possède la clé publique pour le téléphone IP de Cisco, qui est signée par la clé privée de la fonction de proxy d'autorité de certification CUCM (CAPF). C'est la méthode préférée (par opposition à l'utilisation de MICs) parce que seulement des Téléphones IP de Cisco qui provisioned

manuellement par un administrateur sont permis pour télécharger et vérifier le fichier CTL.**Remarque:** En raison du risque de sécurité accru, Cisco recommande l'utilisation de MICs seulement pour l'installation LSC et pas pour l'usage continu. Les clients qui configurent des Téléphones IP de Cisco pour utiliser MICs pour l'authentification de Transport Layer Security (TLS) ou pour n'importe quel autre but font ainsi à leur propre risque.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configurations

Ce document décrit ces configurations :

- Configuration ASA
- Configuration de CallManager
- Configuration du VPN sur le CallManager
- Installation de certificat sur des Téléphones IP

Configuration ASA

La configuration de l'ASA est presque identique que quand vous connectez un ordinateur client d'AnyConnect à l'ASA. Cependant, ces restrictions s'appliquent :

- Le groupe de tunnels doit avoir un groupe-URL. Cet URL sera configuré en cm sous l'URL de passerelle VPN.
- La stratégie de groupe ne doit pas contenir un tunnel partagé.

Cette configuration utilise un certificat précédemment configuré et installé ASA (auto-signée ou tiers) dans le point de confiance de Protocole SSL (Secure Socket Layer) du périphérique ASA. Pour plus d'informations, référez-vous aux documents suivants :

- Configurer des Certificats numériques
- Exemple de configuration de l'installation manuelle de certificats de fournisseurs tiers dans ASA 8.x pour une utilisation avec WebVPN
- ASA 8.x : Exemple de configuration de l'accès VPN avec le client VPN AnyConnect à l'aide d'un certificat auto-signé

La configuration appropriée de l'ASA est :

```
ip local pool SSL_Pool 10.10.10.1-10.10.10.254 mask 255.255.255.0
group-policy GroupPolicy_SSL internal
group-policy GroupPolicy_SSL attributes
split-tunnel-policy tunnelall
vpn-tunnel-protocol ssl-client

tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
address-pool SSL_Pool
```

```
default-group-policy GroupPolicy_SSL
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg
anyconnect enable

ssl trust-point SSL outside
```

Configuration de CallManager

Afin d'exporter le certificat de l'ASA et importer le certificat dans le CallManager comme certificat de Téléphone-VPN-confiance, terminez-vous ces étapes :

1. Enregistrez le certificat généré avec CUCM.
2. Vérifiez le certificat utilisé pour le SSL.`ASA(config)#`**`show run ssl`**
   ```
   ssl trust-point SSL outside
   ```
3. Exportez le certificat.`ASA(config)#`**`crypto ca export SSL identity-certificate`** Le certificat d'identité encodé du Privacy Enhanced Mail (PEM) suit :
   ```
   -----BEGIN CERTIFICATE-----
   ZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMwMTM1MzEwWhcNMjMw
   MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwNlZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1
   NDAwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMYcrysjZ+MawKBx8Zk69SW4AR
   FSpV6FPcUL7xsovhw6hsJE/2VDgd3pkawc5jcl5vkcpTkhjbf2xC4C1q6ZQwpahde22sdf1
   wsidpQWq1DDrJD1We83L/oqmhkWJO7QfNrGZhOLv9xOpR7BFpZd1yFyzwAPkoBl1
   -----END CERTIFICATE-----
   ```
4. Copiez le texte du terminal et sauvegardez-le comme un fichier .pem.
5. Ouvrez une session au CallManager et choisissez la **gestion de SYSTÈME D'EXPLOITATION > la Gestion de Sécurité > de certificat > le certificat unifiés de téléchargement > Téléphone-VPN-confiance choisie** afin de télécharger le fichier du certificat enregistré dans l'étape précédente.

Configuration du VPN sur le CallManager

1. Naviguez vers la gestion de Cisco Unified CM.
2. De la barre de menus, choisissez la **fonctionnalité avancée > le VPN > la passerelle VPN**.
3. Dans la fenêtre de configuration de passerelle VPN, terminez-vous ces étapes :Dans la zone d'identification de passerelle VPN, écrivez un nom. Ceci peut être n'importe quel nom.Dans le champ description de passerelle VPN, écrivez une description (facultative).Dans le champ URL de passerelle VPN, écrivez le groupe-URL défini sur l'ASA.Dans les Certificats VPN dans ce domaine champ Location, sélectionnez le certificat qui a été téléchargé au CallManager précédemment pour le déplacer du truststore à cet emplacement.
4. De la barre de menus, choisissez la **fonctionnalité avancée > le VPN > le groupe VPN**.
5. Dans les toutes les passerelles VPN disponibles mettez en place, sélectionnez la passerelle VPN précédemment définie. Cliquez sur vers le bas la flèche afin de déplacer la passerelle sélectionnée aux passerelles VPN sélectionnées dans ce domaine de groupe VPN.
6. De la barre de menus, choisissez la **fonctionnalité avancée > le profil VPN > VPN**.
7. Afin de configurer le profil VPN, terminez-vous tous les champs qui sont identifiés par un astérisque (*).**Le réseau automatique d'enable les détectent :** Si activé, le téléphone VPN cingle aucune réponse n'est reçue, elle TFTP le serveur et si des automatique-initiés une connexion VPN.**Contrôle d'ID d'hôte d'enable :** Si activé, le téléphone VPN compare le FQDN de l'URL de passerelle VPN contre le CN/SAN du certificat. Le client ne se connecte pas s'ils ne s'assortissent pas ou si un certificat de masque avec un astérisque (*) est

utilisé.**Persistance de mot de passe d'enable :** Ceci permet au téléphone VPN pour cacher le nom d'utilisateur et le passsword pour la prochaine tentative VPN.
8. Dans la fenêtre commune de configuration de profil téléphonique, cliquez sur Apply le **config** afin d'appliquer la nouvelle configuration du VPN. Vous pouvez utiliser le « profil téléphonique commun de norme » ou créer un nouveau profil.
9. Si vous créiez un nouveau profil pour les téléphones/utilisateurs spécifiques, allez à la fenêtre de configuration de téléphone. Dans le domaine commun de profil téléphonique, choisissez le **profil téléphonique de terrain communal de norme**.
10. Enregistrez le téléphone au CallManager de nouveau afin de télécharger la nouvelle configuration.

Configuration d'authentification de certificat

Afin de configurer l'authentification de certificat, terminez-vous ces étapes dans le CallManager et l'ASA :

1. De la barre de menus, choisissez la **fonctionnalité avancée > le profil VPN > VPN**.
2. Confirmez le champ de méthode d'authentification client est placé **pour délivrer un certificat.**
3. Procédure de connexion au CallManager. De la barre de menus, choisissez la **gestion de SYSTÈME D'EXPLOITATION > la Sécurité > la Gestion > la découverte de certificat unifiées**.
4. Exportez les certificats corrects pour la méthode d'authentification sélectionnée de certificat :MICs : Cisco_Manufacturing_CA - Authentifiez les Téléphones IP avec une MICLSC : Fonction de proxy d'autorité de certification de Cisco (CAPF) - Authentifiez les Téléphones IP avec un LSC
5. Trouvez le certificat, Cisco_Manufacturing_CA ou CAPF. Téléchargez le fichier .pem et l'sauvegardez comme fichier de .txt
6. Créez un nouveau point de confiance sur l'ASA et authentifiez le point de confiance avec le certificat enregistré précédent. Quand vous êtes incité pour le certificat de CA encodé par base-64, choisi et collez le texte dans le fichier téléchargé .pem avec le COMMENCER et les lignes de fin. Un exemple est montré : `ASA (config)#`**`crypto ca trustpoint CM-Manufacturing`**
   `ASA(config-ca-trustpoint)#`**`enrollment terminal`**
   `ASA(config-ca-trustpoint)#`**`exit`**
   `ASA(config)#`**`crypto ca authenticate CM-Manufacturing`**
   `ASA(config)#`

   `<base-64 encoded CA certificate>`

   `quit`
7. Confirmez l'authentification sur le groupe de tunnels est placé pour délivrer un certificat l'authentification.`tunnel-group SSL webvpn-attributes`
   `authentication certificate`
   `group-url https://asa5520-c.cisco.com/SSL enable`

Installation de certificat sur des Téléphones IP

Les Téléphones IP peuvent fonctionner avec MICs ou LSC, mais le processus de configuration est différent pour chaque certificat.

Installation MIC

Par défaut, tous les téléphones qui prennent en charge le VPN sont préchargés avec MICs. Les 7960 et 7940 téléphones ne sont pas livré avec une MIC, et exigent d'une procédure d'installation

spéciale pour que le LSC s'enregistre sécurisé.

Remarque: Cisco recommande que vous utilisiez MICs pour l'installation LSC seulement. Cisco prend en charge des LSC pour authentifier la connexion de TLS avec CUCM. Puisque des certificats racine MIC peuvent être compromis, les clients qui configurent des téléphones pour utiliser MICs pour l'authentification de TLS ou pour n'importe quel autre but font ainsi à leur propre risque. Cisco n'assume aucune responsabilité si MICs sont compromis.

Installation LSC

1. Service de l'enable CAPF sur CUCM.
2. Après que le service CAPF soit lancé, assignez les instructions de téléphone de générer un LSC dans CUCM. Ouvrez une session à la gestion de Cisco Unified CM et choisissez le **Device > Phone**. Sélectionnez le téléphone que vous avez configuré.
3. Dans la section Informations de la fonction de proxy d'autorité de certification (CAPF), assurez que toutes les configurations sont correctes et l'exécution est placée à une future date.
4. Si l'authentication mode est placée à la chaîne null ou au certificat existant, aucune action supplémentaire n'est exigée.
5. Si l'authentication mode est placée à une chaîne, manuellement les **configurations > la configuration de sécurité** choisies **> ** # > LSC > mise à jour** dans la console de téléphone.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vérification ASA

```
ASA5520-C(config)#show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : CP-7962G-SEPXXXXXXXXXXXX
Index : 57
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption : AnyConnect-Parent: (1)AES128 SSL-Tunnel: (1)AES128
DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1Bytes Tx : 305849
Bytes Rx : 270069Pkts Tx : 5645
Pkts Rx : 5650Pkts Tx Drop : 0
Pkts Rx Drop : 0Group Policy :
GroupPolicy_SSL Tunnel Group : SSL
Login Time : 01:40:44 UTC Tue Feb 5 2013
Duration : 23h:00m:28s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
Tunnel ID : 57.1
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : AnyConnect Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 1759 Bytes Rx : 799
Pkts Tx : 2 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 57.2
Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 50529
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 835 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 57.3
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 51096
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : DTLS VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 303255 Bytes Rx : 269270
Pkts Tx : 5642 Pkts Rx : 5649
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

Vérification CUCM

Dépannez

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

Bogues relatives

- L'ID de bogue Cisco CSCtf09529, ajoutent le soutien de la caractéristique VPN dans CUCM pour 8961, 9951, 9971 téléphones
- L'ID de bogue Cisco CSCuc71462, Basculement du téléphone IP VPN prend 8 minutes
- ID de bogue Cisco CSCtz42052, soutien de VPN SSL de téléphone IP des numéros de port non par défaut
- L'ID de bogue Cisco CSCth96551, non tous les caractères ASCII sont pris en charge pendant l'utilisateur du téléphone VPN + la procédure de connexion de mot de passe.
- L'ID de bogue Cisco CSCuj71475, entrée manuelle TFTP a eu besoin pour le téléphone IP VPN
- Appels manqués, placés, ou reçus de ne pas se connecter de l'ID de bogue Cisco CSCum10683, des Téléphones IP

Informations connexes

- Support et documentation techniques - Cisco Systems