Connexion téléphonique d'AnyConnect VPN à un exemple de configuration de routeur Cisco IOS

Contenu

Introduction

Ce document décrit comment configurer les périphériques de routeur de Cisco IOS® et de gestionnaire d'appel de sorte que les Téléphones IP de Cisco puissent établir des connexions VPN au routeur Cisco IOS. Ces connexions VPN sont nécessaires afin de sécuriser la transmission avec l'un ou l'autre de ces deux méthodes d'authentification client :

- Serveur ou base de données locale d'Authentification, autorisation et comptabilité (AAA)
- Certificat de téléphone

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Cisco IOS 15.1(2)T ou plus tard
- Ensemble de caractéristiques/permis : Universel (données et Sécurité et UC) pour le routeur de service intégré de Cisco IOS (ISR)-G2
- Ensemble de caractéristiques/permis : Sécurité avancée pour le Cisco IOS ISR
- Version 8.0.1.100000-4 de Cisco Unified Communications Manager (CUCM) ou plus tard
- Release 9.0(2)SR1S de téléphone IP - Protocole SCCP (Skinny Call Control Protocol) ou plus tard

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 releases utilisées dans cet exemple de configuration incluent :

- Release 15.1(4)M4 de routeur Cisco IOS
- Version 8.5.1.10000-26 de gestionnaire d'appel
- Release 9.1(1)SR1S de téléphone IP

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.

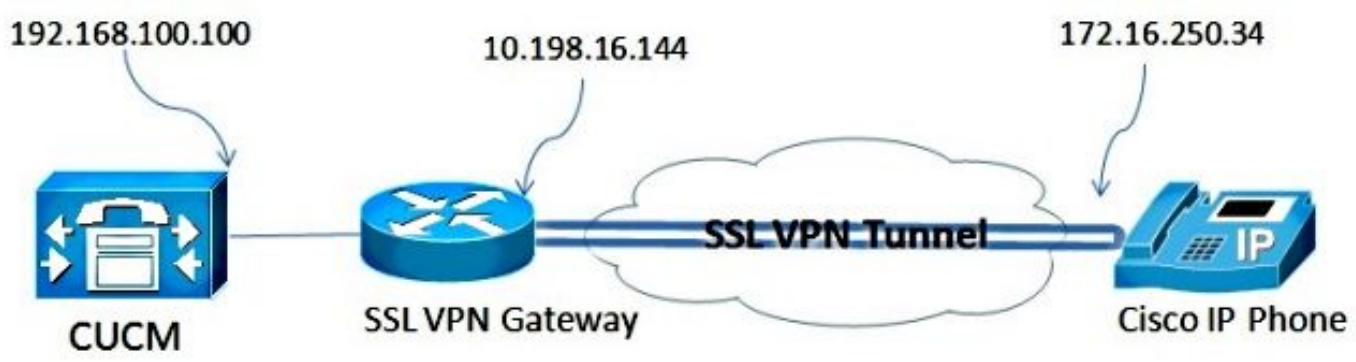
Configurez

Cette section couvre les informations requises afin de configurer les caractéristiques décrites dans ce document.

> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Topologie du réseau

La topologie utilisée dans ce document inclut un téléphone IP de Cisco, le routeur Cisco IOS comme passerelle VPN de Secure Sockets Layer (SSL), et CUCM comme passerelle de Voix.



Configuration du serveur de VPN SSL

Cette section décrit comment configurer la tête de réseau de Cisco IOS afin de permettre les connexions d'arrivée de VPN SSL.

Étapes communes de configuration

1. Générez la clé de Rivest-Shamir-Adleman (RSA) avec une longueur de 1024 octets :

   ```
   Router(config)#crypto key generate rsa general-keys label SSL modulus 1024
   ```
2. Créez le point de confiance pour le certificat auto-signé, et reliez la clé RSA SSL :

   ```
   Router(config)#crypto pki trustpoint server-certificate
   enrollment selfsigned
   usage ssl-server
   serial-number
   subject-name CN=10.198.16.144
   revocation-check none
   rsakeypair SSL
   ```
3. Une fois que le point de confiance est configuré, inscrivez-vous le certificat auto-signé avec cette commande :

   ```
   Router(config)#crypto pki enroll server-certificate
   % Include an IP address in the subject name? [no]: no
   Generate Self Signed Router Certificate? [yes/no]: yes

   Router Self Signed Certificate successfully created
   ```
4. Activez le module correct d'AnyConnect sur la tête de réseau. Le téléphone lui-même ne télécharge pas ce module. Mais, sans module, le tunnel VPN n'établit pas. Il est recommandé pour utiliser la dernière version de logiciel client disponible sur Cisco.com. Cet exemple utilise la version 3.1.3103.

   Dans des versions plus anciennes de Cisco IOS, c'est la commande afin d'activer le module :
   ```
   Router(config)#webvpn install svc flash:anyconnect-win-3.1.03103-k9.pkg
   ```
   Cependant, dans la dernière version de Cisco IOS, c'est la commande :
   ```
   Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
   3.1.03103-k9.pkg sequence 1
   ```
5. Configurez la passerelle VPN. Le webvpn gateway est utilisé afin de terminer la connexion SSL de l'utilisateur.
   ```
   Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
   3.1.03103-k9.pkg sequence 1
   ```
   Remarque: L'un ou l'autre l'adresse IP utilisée ici doit être sur le même sous-réseau que

l'interface à laquelle les téléphones se connectent, ou la passerelle doit être originaire directement d'une interface sur le routeur. La passerelle est également utilisée afin de définir que le certificat est utilisé par le routeur afin de valider lui-même au client.

6. Définissez le groupe local qui est utilisé afin d'assigner des adresses IP aux clients quand elles se connectent :
```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

Configuration avec l'authentification d'AAA

Cette section décrit les commandes que vous devez afin de configurer le serveur d'AAA ou la base de données locale afin d'authentifier vos téléphones. Si vous prévoyez d'utiliser l'authentification réservée au certificat pour les téléphones, continuez à la section suivante.

Configurez la base de données utilisateur

La base de données locale du routeur ou un serveur externe d'AAA peut être utilisée pour l'authentification :

- Afin de configurer la base de données locale, entrez :
```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```
- Afin de configurer un serveur distant d'AAA RADIUS pour l'authentification, entrez :
```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

Configurez le contexte virtuel et la stratégie de groupe

Le contexte virtuel est utilisé afin de définir les attributs qui régissent la connexion VPN, comme :

- Quel URL à l'utiliser quand vous vous connectez
- Quel groupe à l'utiliser afin d'assigner les adresses du client
- Quelle méthode d'authentification à l'utiliser

Ces commandes sont un exemple d'un contexte qui utilise l'authentification d'AAA pour le client :

```
Router(config)#crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

Configuration avec de téléphone IP le certificat significatif localement - (LSC) pour l'authentification client

Cette section décrit les commandes que vous devez afin de configurer l'authentification client basée sur certificat pour les téléphones. Cependant, afin de faire ceci, la connaissance des divers types de Certificats de téléphone est exigée :

- **Certificat installé par fabricant (MIC) -** MICs sont inclus sur chacun des 7941, 7961, et Téléphones IP de Cisco de nouveau-modèle. MICs sont les Certificats 2,048-bit principaux qui sont signés par l'Autorité de certification (CA) de Cisco. 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. Puisque ce certificat est fourni par le fabricant lui-même, comme indiqué dans le nom, il n'est pas recommandé d'utiliser ce certificat pour l'authentification client.
- **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 le plus méthode sécurisée (par opposition à l'utilisation de MICs).
Attention : 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 afin d'utiliser MICs pour l'authentification de Transport Layer Security (TLS), ou pour n'importe quel autre but, font ainsi à leur propre risque.

Dans cet exemple de configuration, le LSC est utilisé afin d'authentifier les téléphones.

Conseil : La plupart de moyen sûr de connecter votre téléphone est d'utiliser la double authentification, qui combine le certificat et l'authentification d'AAA. Vous pouvez configurer ceci si vous combinez les commandes utilisées pour chacun au-dessous d'un contexte virtuel.

Configurez le point de confiance afin de valider le certificat client

Le routeur doit faire installer le certificat CAPF afin de valider le LSC du téléphone IP. Afin d'obtenir ce certificat et l'installer sur le routeur, terminez-vous ces étapes :

1. Allez à la page Web du système d'exploitation de gestion CUCM (SYSTÈME D'EXPLOITATION).
2. Choisissez la **Gestion de Sécurité > de certificat**.
   Remarque: Cet emplacement pourrait changer basé sur la version CUCM.
3. Trouvez le certificat étiqueté **CAPF**, et téléchargez le fichier **.pem**. Sauvegardez-le comme fichier de **.txt**
4. Une fois que le certifcate est extrait, créez un nouveau point de confiance sur le routeur, et authentifiez le point de confiance avec CAPF, comme affiché ici. Une fois incité pour le base-64 a encodé le certificat de CA, sélectionne et colle le texte dans le fichier téléchargé .pem avec le COMMENCER et les lignes de fin.

```
Router(config)#crypto pki trustpoint CAPF
enrollment terminal
authorization username subjectname commonname
revocation-check none
Router(config)#crypto pki authenticate CAPF
Router(config)#

<base-64 encoded CA certificate>

quit
```

Choses à noter :

- La méthode d'inscription est terminale parce que le certificat doit être manuellement installé sur le routeur.
- La commande d'**authorization username** est exigée afin d'indiquer au routeur quoi utiliser comme nom d'utilisateur quand le client établit le rapport. Dans ce cas, il utilise le nom commun (NC).
- Un contrôle de révocation doit être désactivé parce que les Certificats de téléphone n'ont pas un Liste des révocations de certificat (CRL) défini. Ainsi, à moins qu'elle soit désactivée, la connexion échoue et l'Infrastructure à clés publiques (PKI) met au point l'exposition cette sortie :

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilies request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

Configurez le contexte virtuel et la stratégie de groupe

La présente partie de la configuration est semblable à la configuration utilisée précédemment, excepté deux points :

- La méthode d'authentification
- Le point de confiance les utilisations de contexte afin d'authentifier les téléphones

Les commandes sont affichées ici :

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Starting CRL revocation check
Jun 17 21:49:46.695: CRYPTO_PKI: Matching CRL not found
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) CDP does not exist. Use SCEP to
query CRL.
Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilies request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076) Certificate validation failed
```

Configuration du gestionnaire d'appel

Cette section décrit les étapes de configuration du gestionnaire d'appel.

Exportez Auto-signée ou le certificat d'identité du routeur au CUCM

Afin d'exporter le certificat du routeur et importer le certificat dans le gestionnaire d'appel comme certificat de Téléphone-VPN-confiance, terminez-vous ces étapes :

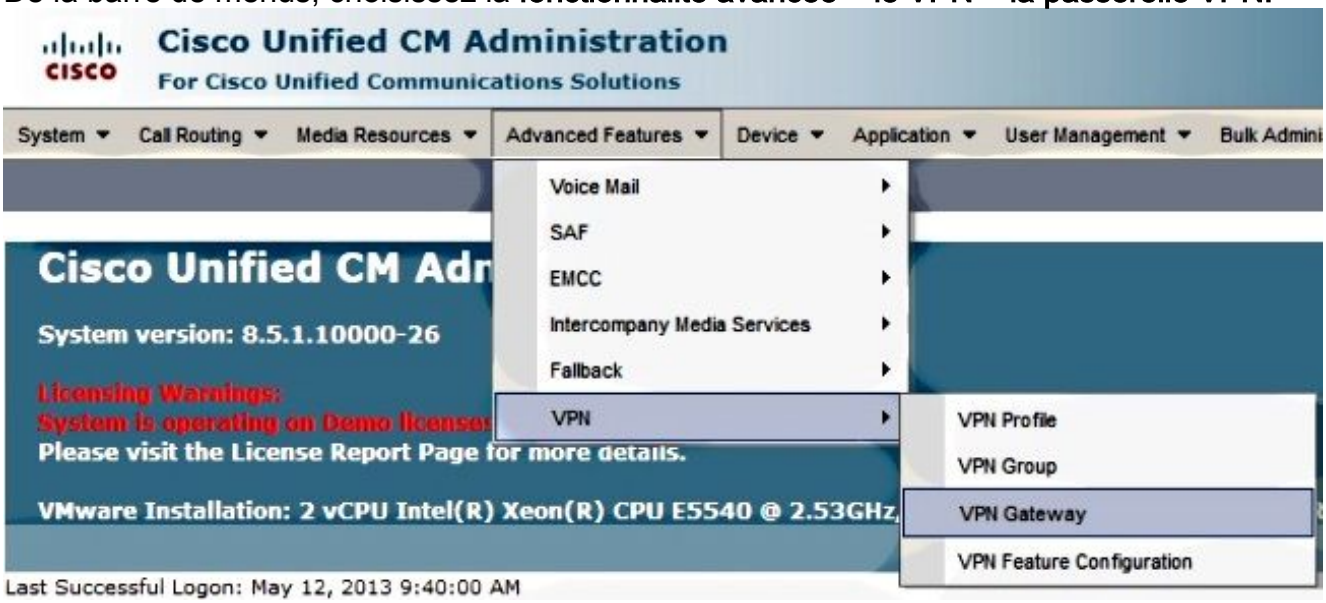
1. Vérifiez le certificat utilisé pour le SSL.
   ```
   Router#show webvpn gateway SSL
   SSL Trustpoint: server-certificate
   ```
2. Exportez le certificat.
   ```
   Router(config)#crypto pki export server-certificate pem terminal
   The Privacy Enhanced Mail (PEM) encoded identity certificate follows:
   -----BEGIN CERTIFICATE-----
   ```

```
<output removed>

-----END CERTIFICATE-----
```

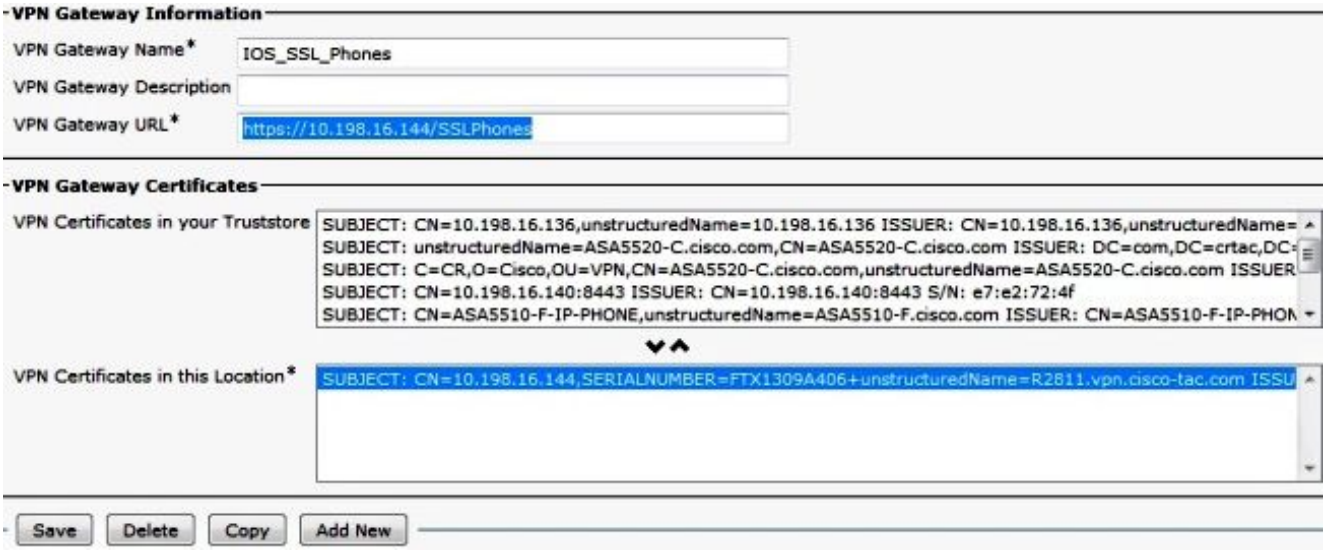
3. Copiez le texte du terminal et sauvegardez-le comme un fichier **.pem**.
4. Ouvrez une session au gestionnaire d'appel, et choisissez la **gestion de SYSTÈME D'EXPLOITATION > la Gestion de Sécurité > de certificat > le certificat unifiés de téléchargement > Téléphone-VPN-confiance choisie** afin de télécharger le fichier du certificat enregistré dans l'étape précédente.

Configurez la passerelle VPN, le groupe, et le profil dans le CUCM

1. Naviguez vers la **gestion de Cisco Unified CM**.
2. De la barre de menus, choisissez la **fonctionnalité avancée > le VPN > la passerelle VPN.**

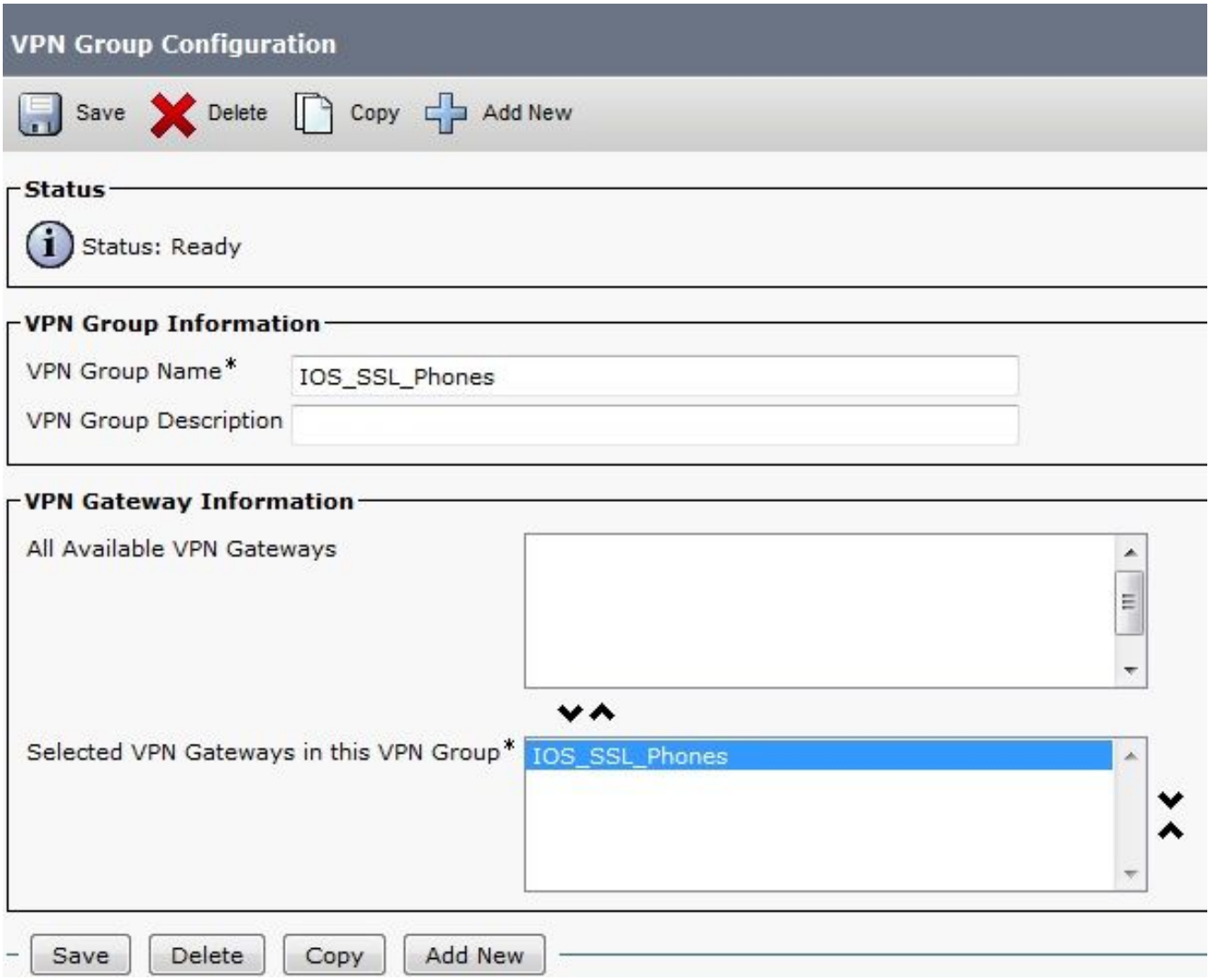


3. Dans la fenêtre de configuration de passerelle VPN, terminez-vous ces étapes :
   Dans la zone d'identification de passerelle VPN, écrivez un nom. Ceci peut être n'importe quel nom.Dans le champ description de passerelle VPN, écrivez une description (facultative).Dans le champ URL de passerelle VPN, écrivez le groupe-URL défini sur le routeur.Dans les Certificats VPN dans ce domaine champ Location, choisissez le certificat qui a été téléchargé au gestionnaire d'appel précédemment afin de le déplacer de la mémoire de confiance à cet
   emplacement.

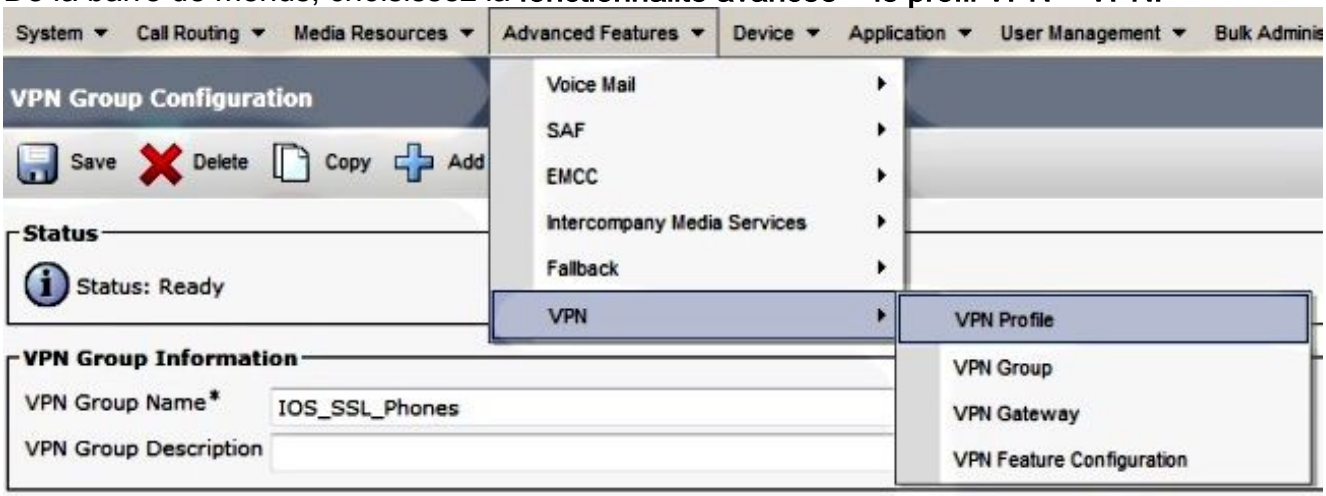


4. De la barre de menus, choisissez la **fonctionnalité avancée > le VPN > le groupe VPN.**

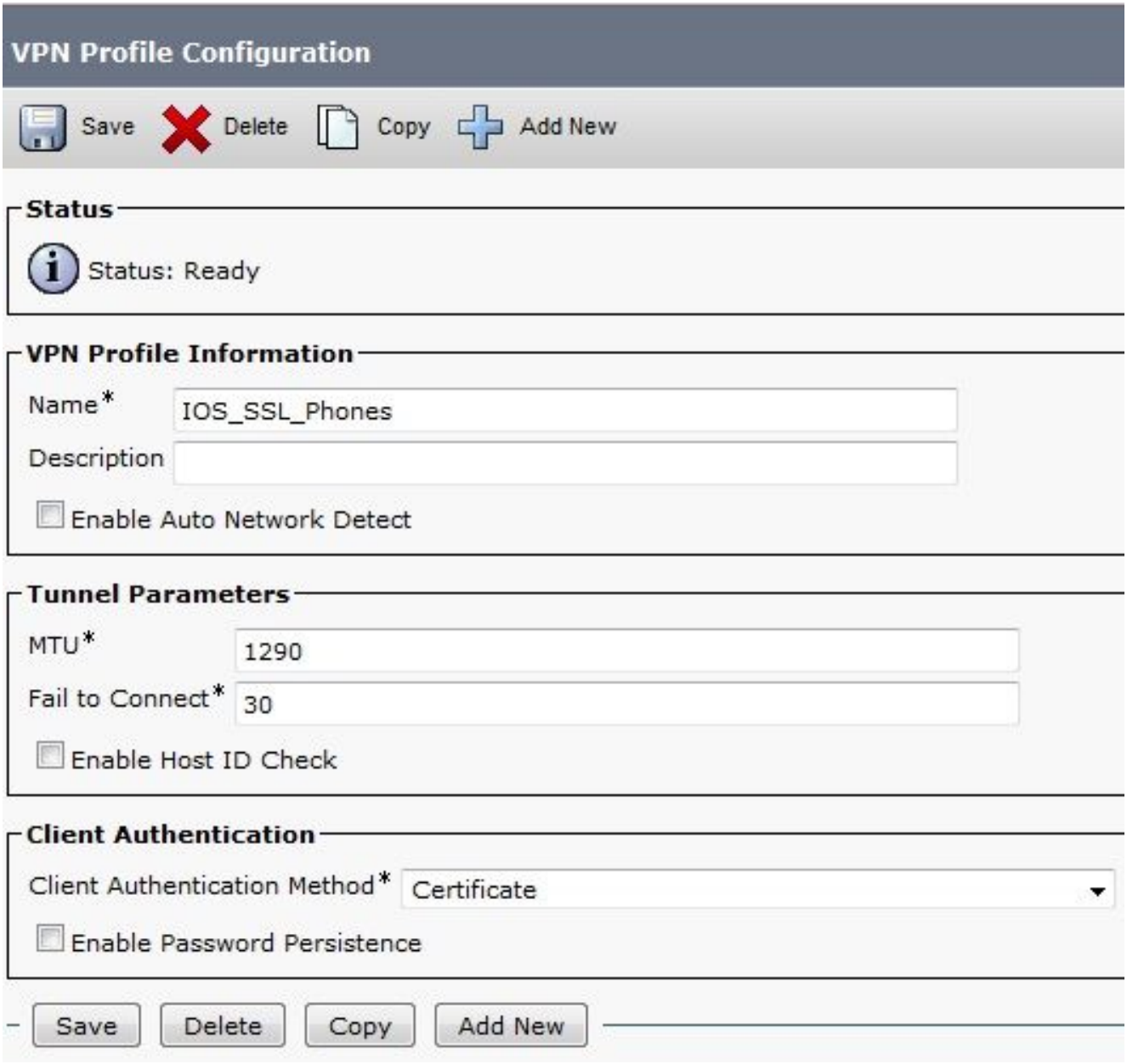
5. Dans les toutes les passerelles VPN disponibles mettez en place, choisissez la **passerelle VPN** précédemment définie. Cliquez sur vers le bas la flèche afin de déplacer la passerelle sélectionnée aux passerelles VPN sélectionnées dans ce domaine de groupe VPN.



6. De la barre de menus, choisissez la fonctionnalité avancée > le profil VPN > VPN.



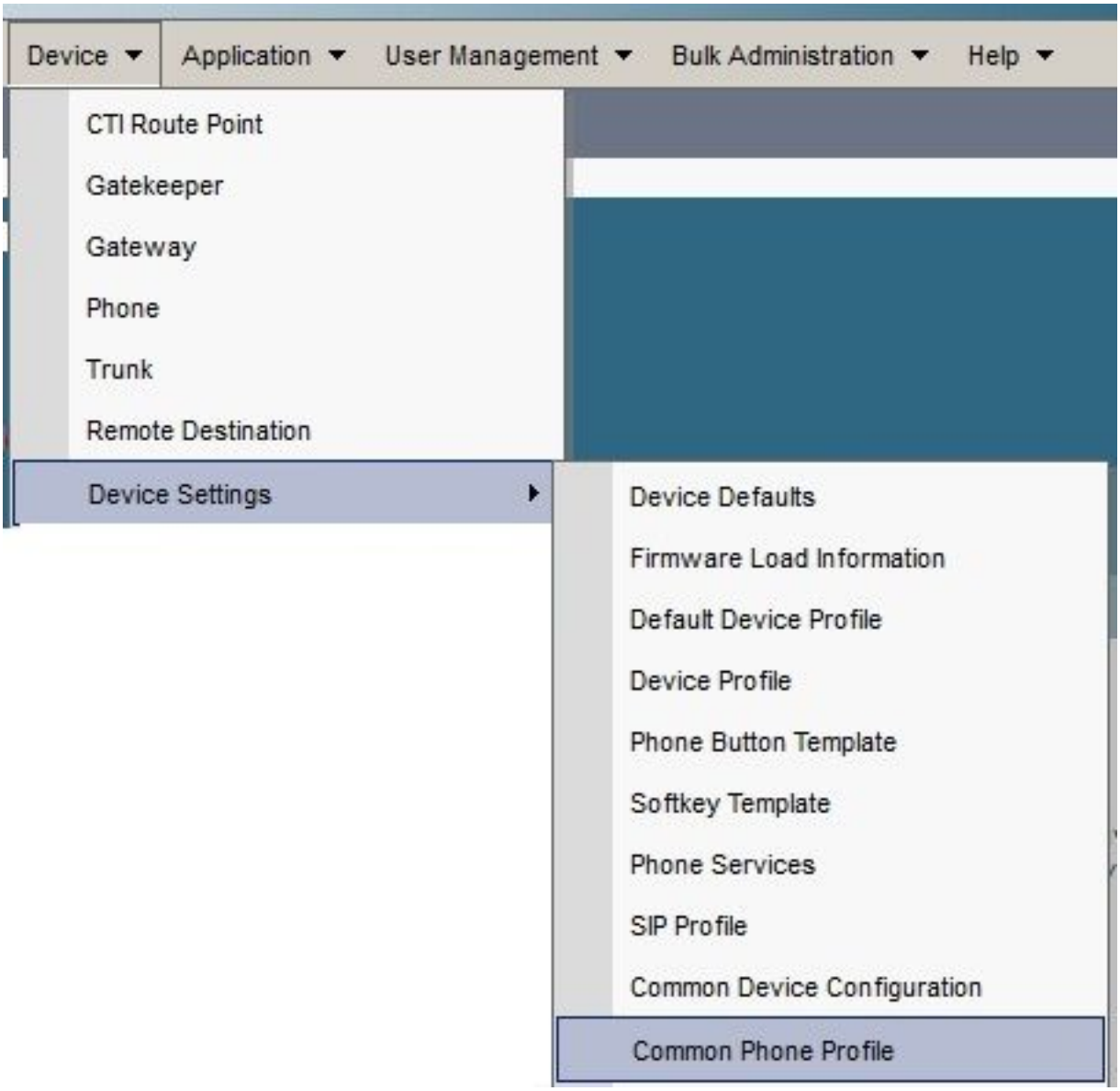
7. Afin de configurer le profil VPN, terminez-vous tous les champs qui sont identifiés par un astérisque (*).

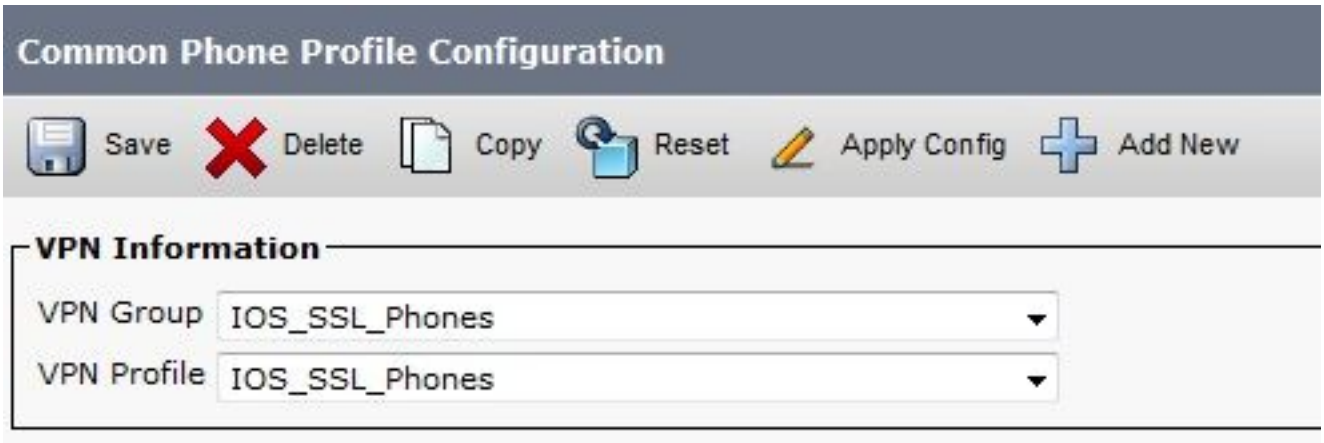


Le réseau automatique d'enable les détectent : Si activé, le téléphone VPN cingle le serveur TFTP. Si aucune réponse n'est reçue, il des automatique-initiés une connexion VPN.**Contrôle d'ID d'hôte d'enable :** Si activé, le téléphone VPN compare le nom de domaine complet (FQDN) de l'URL de passerelle VPN contre le réseau de région CN/Storage (SAN) du certificat. Le client ne se connecte pas si ces éléments 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 mot de passe pour la prochaine tentative VPN.

Appliquez le groupe et le profil au téléphone IP avec le profil téléphonique commun

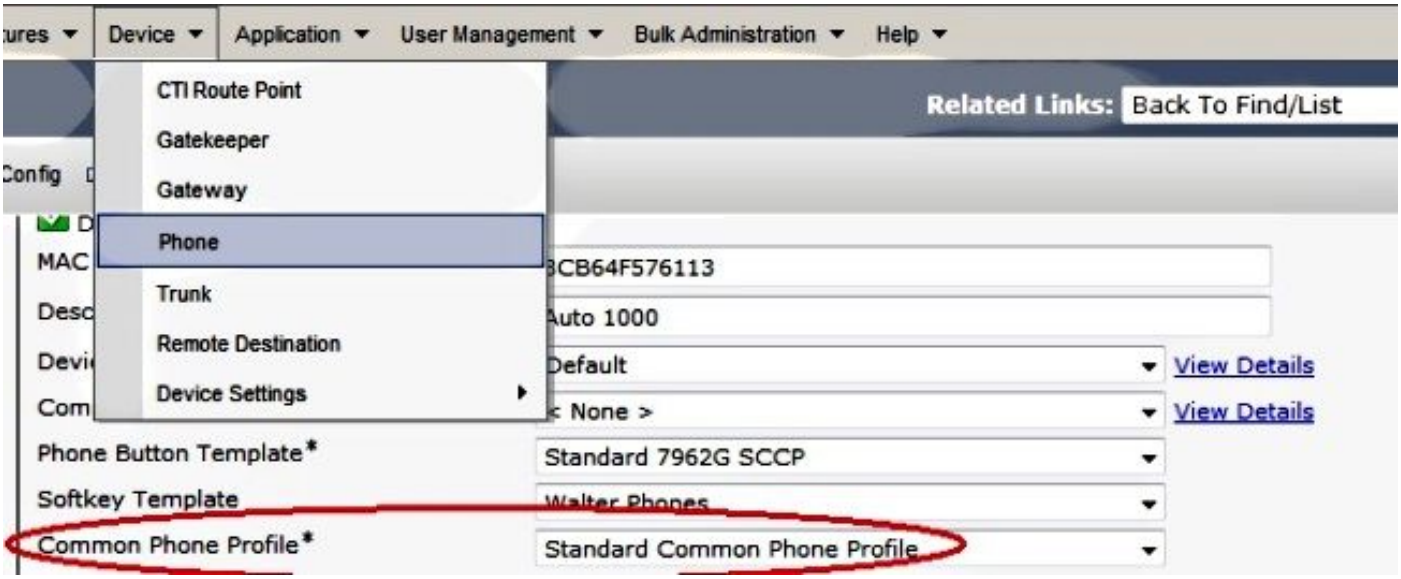
Dans la fenêtre commune de configuration de profil téléphonique, cliquez sur Apply le **config** afin d'appliquer la nouvelle configuration du VPN. Vous pouvez utiliser le **profil téléphonique commun** standard ou créer un nouveau profil.





Appliquez le profil téléphonique commun au téléphone IP

Si vous créiez un nouveau profil pour les téléphones/utilisateurs spécifiques, naviguez vers la fenêtre de **configuration de téléphone**. Dans le domaine commun de profil téléphonique, choisissez le **profil téléphonique commun standard**.



Installez localement - les Certificats significatifs (LSC) sur des Téléphones IP de Cisco

Le guide suivant peut être utilisé pour installer localement - les Certificats significatifs sur des Téléphones IP de Cisco. Cette étape est seulement nécessaire si l'authentification utilisant le LSC est utilisée. L'authentification utilisant le Manufacterer a installé le certificat (MIC) ou le nom d'utilisateur et mot de passe n'exige pas d'un LSC d'être installé.

Installez un LSC à un téléphone avec la security mode de batterie CUCM réglée Non-sécurisée.

Enregistrez le téléphone au gestionnaire d'appel de nouveau afin de télécharger la nouvelle configuration

C'est la dernière étape dans le processus de configuration.

Vérifiez

Vérification de routeur

Afin de vérifier les statistiques de la session VPN dans le routeur, vous pouvez utiliser ces commandes, et vérifiez les différences entre les sorties (mises en valeur) pour le nom d'utilisateur et délivrez un certificat l'authentification :

Pour l'authentification de nom d'utilisateur/mot de passe :

```
Router#show webvpn session user phones context SSL
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username : phones                Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
Context : SSL Policy Group : SSLPhones
Last-Used : 00:00:29 Created : 15:40:21.503 GMT
Fri Mar 1 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
Rekey Time : 3600 Rekey Method :
```

```
Lease Duration : 43200
Tunnel IP : 10.10.10.1 Netmask : 255.255.255.0
Rx IP Packets : 106 Tx IP Packets : 145
CSTP Started : 00:11:15 Last-Received : 00:00:29
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 51534
DTLS Port : 52768
Router#

Router#show webvpn session context all
WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
phones             172.16.250.34              1         00:30:38  00:00:20
```

Pour l'authentification de certificat :

```
Router#show webvpn session user SEP8CB64F578B2C context all
Session Type : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username : SEP8CB64F578B2C      Num Connection : 1
Public IP : 172.16.250.34 VRF Name : None
CA Trustpoint  : CAPF
Context : SSL Policy Group :
Last-Used : 00:00:08 Created : 13:09:49.302 GMT
Sat Mar 2 2013
Session Timeout : Disabled Idle Timeout : 2100
DPD GW Timeout : 300 DPD CL Timeout : 300
Address Pool : SSL MTU Size : 1290
Rekey Time : 3600 Rekey Method :
Lease Duration : 43200
Tunnel IP : 10.10.10.2 Netmask : 255.255.255.0
Rx IP Packets : 152 Tx IP Packets : 156
CSTP Started : 00:06:44 Last-Received : 00:00:08
CSTP DPD-Req sent : 0 Virtual Access : 1
Msie-ProxyServer : None Msie-PxyPolicy : Disabled
Msie-Exception :
Client Ports : 50122
DTLS Port : 52932


Router#show webvpn session context all
WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
SEP8CB64F578B2C    172.16.250.34              1         3d04h    00:00:16
```

Vérification CUCM

Confirmez que le téléphone IP est inscrit au gestionnaire d'appel avec l'adresse attribuée le routeur fourni à la connexion SSL.

Dépannez

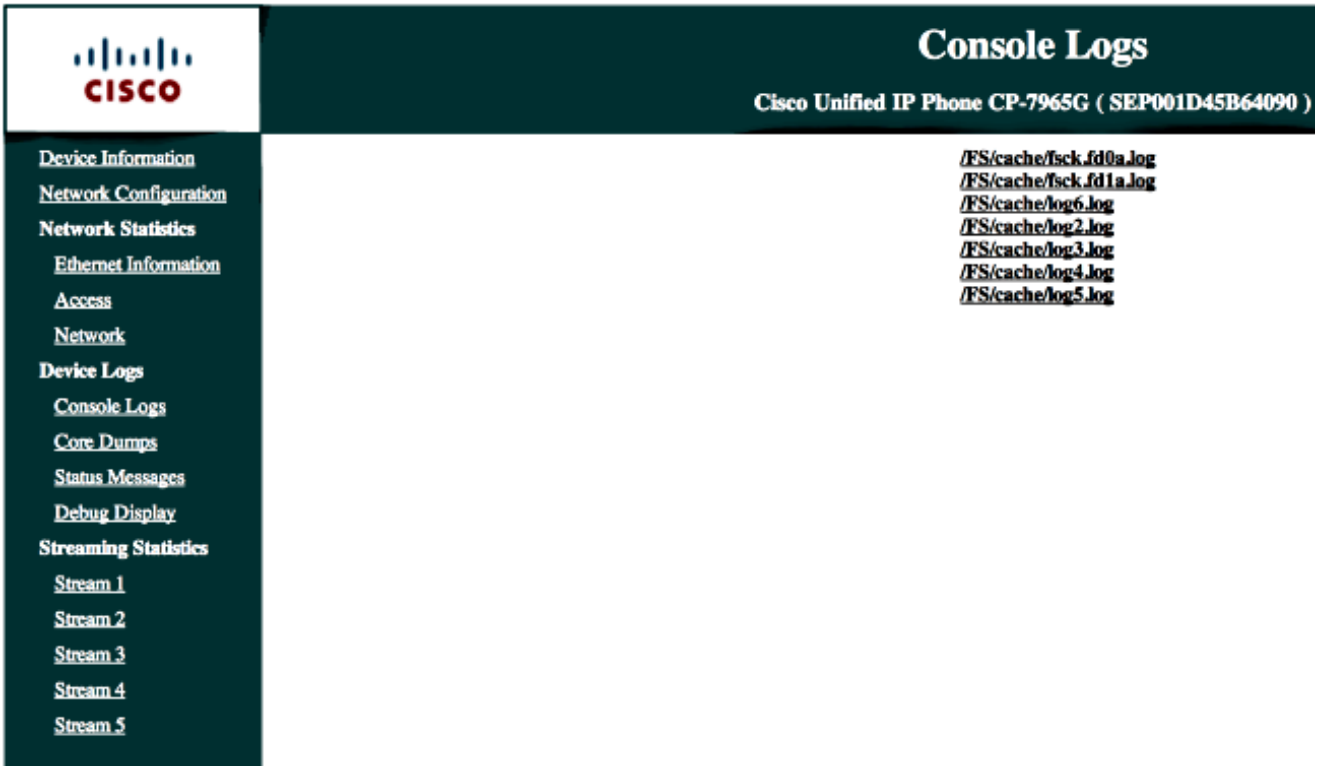
Debugs sur le serveur de VPN SSL

```
Router#show debug

WebVPN Subsystem:
WebVPN (verbose) debugging is on
WebVPN HTTP debugging is on
WebVPN AAA debugging is on
WebVPN tunnel debugging is on
WebVPN Tunnel Events debugging is on
WebVPN Tunnel Errors debugging is on
Webvpn Tunnel Packets debugging is on


PKI:
Crypto PKI Msg debugging is on
Crypto PKI Trans debugging is on
Crypto PKI Validation Path debugging is on
```

Debugs du téléphone

1. Naviguez vers le **Device > Phone de** CUCM.
2. Sur la page de configuration de périphérique, placez l'accès au Web à **activer**.
3. Cliquez sur la **sauvegarde**, et puis cliquez sur Apply le **config**.

4. D'un navigateur, écrivez l'adresse IP du téléphone, et choisissez les **messages de console du** menu du côté gauche.



5. Téléchargez tous les fichiers de **/FS/cache/log *.log**. Les fichiers journal de console contiennent des informations sur pourquoi le téléphone ne se connecte pas au VPN.

Bogues relatives

ID de bogue Cisco CSCty46387, IOS SSLVPN : Amélioration pour faire être un contexte un par

défaut
ID de bogue Cisco CSCty46436, IOS SSLVPN : Amélioration au comportement de validation de certificat client