Configuration et dépannage des téléphones VPN

Contenu

Introduction

Ce document décrit comment configurer et dépanner la fonctionnalité de téléphone VPN des téléphones IP Cisco et de Cisco Unified Communications Manager.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de communications unifiées de Cisco (version CUCM)
- Appareil de sécurité adaptatif Cisco (ASA)
- Réseau privé virtuel (VPN) AnyConnect
- Téléphones IP Cisco

Components Used

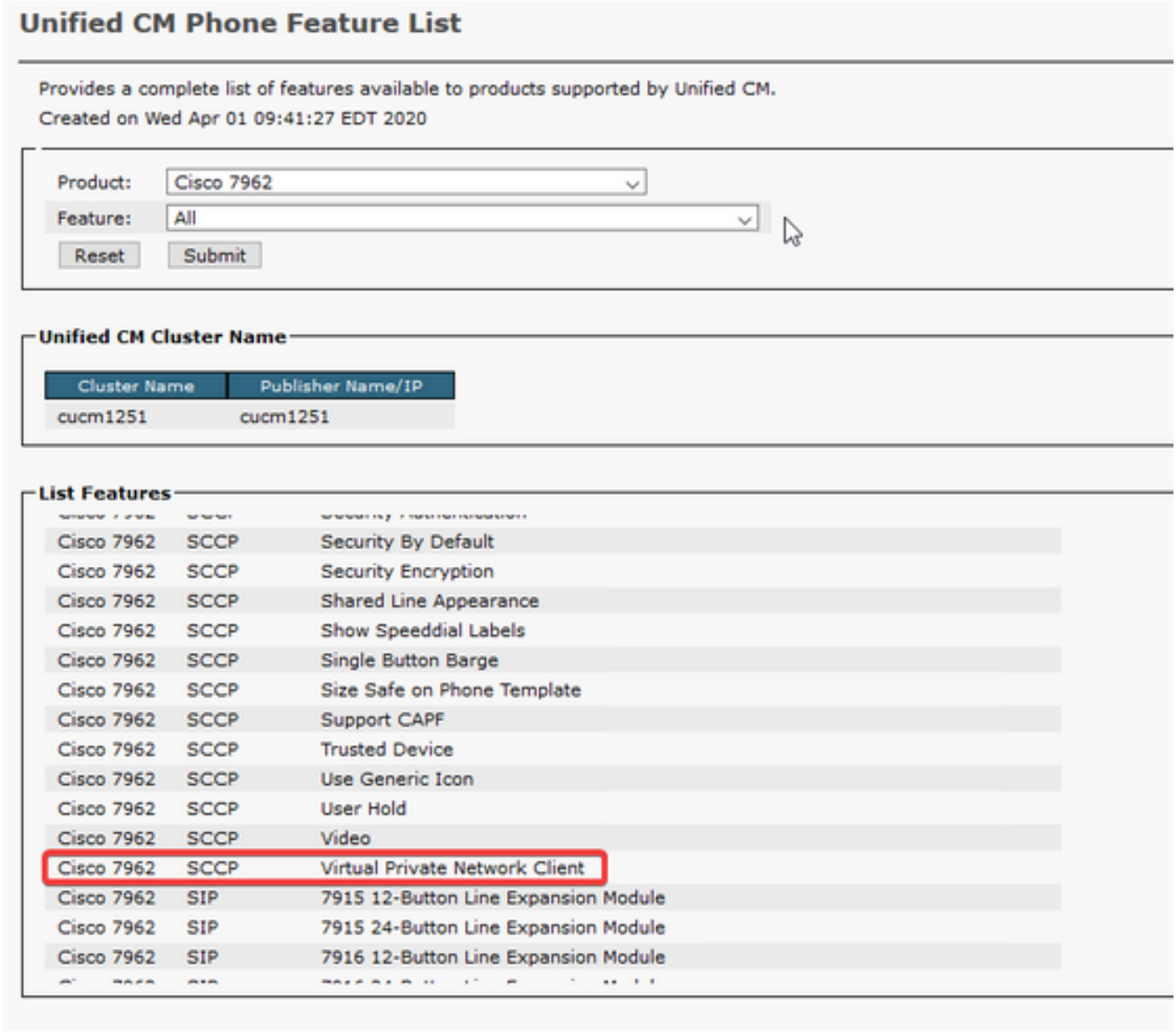
- 8861 14-0-1-0101-145
- ASAv 9.12(2)9

- CUCM 11.5.1.21900-40

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

L'environnement de test de cet article inclut un 8861, ASAv et CUCM 11.5.1, mais il existe de nombreuses variantes de ces produits que vous pouvez utiliser. Vous devez vérifier la liste des fonctionnalités du téléphone sur CUCM pour vous assurer que votre modèle de téléphone prend en charge la fonctionnalité VPN. Afin d'utiliser la liste des fonctionnalités du téléphone, accédez à votre éditeur CUCM dans votre navigateur et accédez à **Cisco Unified Reporting > Unified CM Phone Feature List**. Générez un nouveau rapport, puis sélectionnez votre modèle de téléphone dans la liste déroulante. Ensuite, vous devez rechercher la section List Features pour Virtual Private Network Client, comme l'illustre l'image :



Configuration

Les téléphones VPN nécessitent une configuration correcte sur votre ASA et CUCM. Vous pouvez commencer par l'un ou l'autre des produits, mais ce document couvre d'abord la configuration ASA.

Configuration ASA

Étape 1. Vérifiez que l'ASA est autorisé à prendre en charge AnyConnect pour les téléphones VPN. La commande **show version** sur l'ASA peut être utilisée pour vérifier que **Anyconnect pour Cisco VPN Phone** est activé, comme indiqué dans cet extrait :

```
[output omitted]
Licensed features for this platform:
Maximum VLANs : 50
Inside Hosts : Unlimited
Failover : Active/Standby
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 0
Carrier : Enabled
AnyConnect Premium Peers : 250
AnyConnect Essentials : Disabled
Other VPN Peers : 250
Total VPN Peers : 250
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 500
Botnet Traffic Filter : Enabled
Cluster : Disabled
```

Si cette fonctionnalité n'est pas activée, vous devez travailler avec l'équipe Licence pour obtenir la licence appropriée. Maintenant que vous avez confirmé que votre ASA prend en charge les téléphones VPN, vous pouvez commencer la configuration.

> **Note**: Tous les éléments soulignés de la section de configuration sont des noms configurables qui peuvent être modifiés. La plupart de ces noms sont référencés ailleurs dans la configuration. Il est donc important de mémoriser les noms que vous utilisez dans ces sections (stratégie de groupe, groupe de tunnels, etc.) car vous en aurez besoin plus tard.

Étape 2. Créez un pool d'adresses IP pour les clients VPN. Ceci est similaire à un pool DHCP en ce sens que lorsqu'un téléphone IP se connecte à l'ASA, il reçoit une adresse IP de ce pool. Le pool peut être créé avec cette commande sur l'ASA :

ip local pool vpn-phone-pool 10.1.1-10.10.1.254 masque 255.255.255.0

En outre, si vous préférez un réseau ou un masque de sous-réseau différent, il est également possible de le modifier. Une fois le pool créé, vous devez configurer une stratégie de groupe (un ensemble de paramètres pour la connexion entre l'ASA et les téléphones IP) :

politique de groupe vpn-politique de téléphone-interne

attributs group-policy vpn-phone-policy

split-tunnel-policy tunnelall

vpn-tunnel-protocol ssl-client

Étape 3. Vous devez activer AnyConnect s'il n'est pas déjà activé. Pour ce faire, vous devez connaître le nom de l'interface externe. Généralement, cette interface est nommée **outside** (comme illustré dans l'extrait), mais elle est configurable, assurez-vous donc de disposer de l'interface appropriée. Exécutez **show ip** pour afficher la liste des interfaces :

```
sckiewer-ASAv# show ip
System IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
Current IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
```

Dans cet environnement, l'interface externe est nommée **outside**, de sorte que ces commandes activent AnyConnect sur cette interface.

webvpn
activer externe
anyconnect enable

Étape 4. Configurez un nouveau groupe de tunnels afin d'appliquer la stratégie de groupe créée précédemment à tous les clients qui se connectent sur une URL spécifique. Notez la référence aux noms du pool d'adresses IP et de la stratégie de groupe que vous avez créés précédemment aux 3e et 4e lignes de l'extrait. Si vous avez modifié les noms du pool d'adresses IP ou de la stratégie de groupe, remplacez les valeurs incorrectes par vos noms modifiés :

tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attribute
address-pool vpn-phone-pool
default-group-policy vpn-phone-policy
tunnel-group vpn-phone-group webvpn-attribute
certificat d'authentification
group-url https://asav.sckiewer.lab/phone enable

Vous pouvez utiliser une adresse IP plutôt qu'un nom pour l'**url de groupe**. Cela se fait généralement si les téléphones n'ont pas accès à un serveur DNS qui peut résoudre le nom de domaine complet (FQDN) de l'ASA. Vous pouvez également voir que cet exemple utilise une authentification basée sur un certificat. Vous avez également la possibilité d'utiliser l'authentification nom d'utilisateur/mot de passe, mais il y a d'autres exigences sur l'ASA qui ne sont pas couvertes par ce document.

Dans cet exemple, le serveur DNS a l'enregistrement A, **asav.sckiewer.lab - 172.16.1.250** et vous pouvez voir dans la sortie **show ip** que 172.16.1.250 est configuré sur l'interface nommée **externe**. La configuration serait donc :

crypto ca trustpoint asa-identity-cert

inscription automatique

subject-name CN=asav.sckiewer.lab

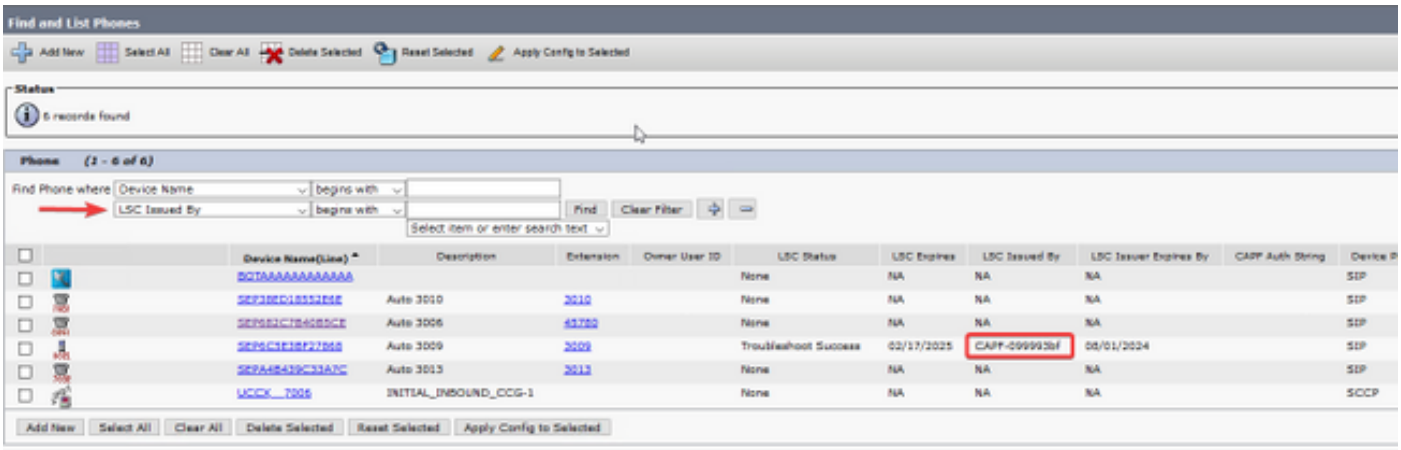
crypto ca enroll asa-identity-cert

ssl trust-point asa-identity-cert outside

A noter :

1. Un nouveau point de confiance a été créé appelé asa-identity-cert et un nom de sujet lui a été appliqué. Cela entraîne l'utilisation du nom de sujet spécifié par le certificat généré à partir de ce point de confiance
2. Ensuite, la commande 'crypto ca enroll asa-identity-cert' permet à l'ASA de générer un certificat auto-signé et de l'enregistrer sur ce point de confiance
3. Enfin, l'ASA présente le certificat du point de confiance à tout périphérique qui se connecte à l'interface externe

Étape 5. Créez les points de confiance nécessaires pour permettre à l'ASA de faire confiance au certificat du téléphone IP. Tout d'abord, vous devez déterminer si vos téléphones IP utilisent le certificat installé par le fabricant (MIC) ou le certificat d'importance locale (LSC). Par défaut, tous les téléphones utilisent leur MIC pour des connexions sécurisées, sauf si un LSC est installé sur eux. Dans CUCM 11.5.1 et versions ultérieures, vous pouvez lancer une recherche à l'adresse **Unified CM Administration > Device > Phone** pour voir si les LSC sont installés alors que les versions plus anciennes de CUCM nécessitent que vous vérifiiez physiquement les paramètres de sécurité sur chaque téléphone. Dans CUCM 11.5.1, notez que vous devez ajouter un filtre (ou modifier le filtre par défaut) à **LSC Émis par**. Les périphériques avec **NA** dans la colonne **LSC Émis par** utilisent le MIC car ils n'ont pas de LSC installé.

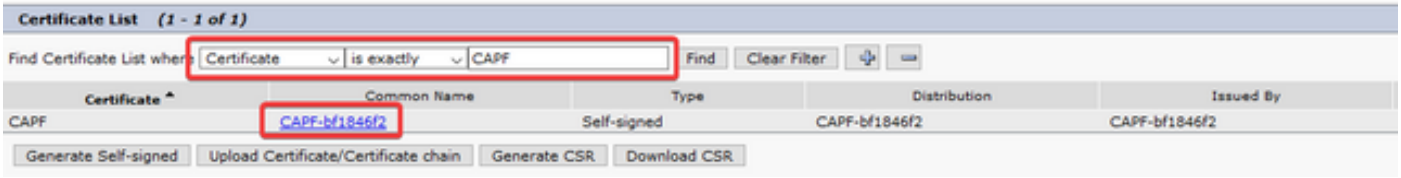


Si votre téléphone ressemble à celui mis en surbrillance dans l'image, vous devez télécharger le certificat CAPF de CUCM Publisher sur l'ASA afin que l'ASA puisse valider le certificat du téléphone pour la connexion sécurisée. Si vous souhaitez utiliser des périphériques sans LSC installé, vous devez télécharger les certificats de fabrication Cisco sur l'ASA. Ces certificats sont disponibles sur le serveur de publication CUCM à l'adresse **Cisco Unified OS Administration > Security > Certificate Management** :

> **Note**: Vous pouvez voir que certains de ces certificats se trouvent dans plusieurs magasins d'approbation (CallManager-trust et CAPF-trust). Peu importe de quel magasin de confiance vous téléchargez les certificats tant que vous vous assurez de sélectionner ceux avec ces noms exacts.

- Cisco_Root_CA_2048 < racine MIC SHA-1

- Cisco_Manufacturing_CA < MIC SHA-1 intermédiaire
- Cisco_Root_CA_M2 < MIC SHA-256 Racine
- Cisco_Manufacturing_CA_SHA2 < MIC SHA-256 intermédiaire
- CAPF à partir de CUCM Publisher < LSC



En ce qui concerne la carte MIC, les modèles de téléphones plus anciens tels que les séries 79xx et 99xx utilisent la chaîne de certificats SHA-1, tandis que les modèles de téléphones plus récents tels que la série 88xx utilisent la chaîne de certificats SHA-256. La chaîne de certificats que vos téléphones utilisent doit être téléchargée vers l'ASA.

Une fois que vous avez les certificats requis, vous pouvez créer le ou les points de confiance avec :

crypto ca trustpoint cert1

terminal d'inscription

crypto ca authenticate cert1

La première commande crée un point de confiance nommé **cert1**, et la commande **crypto ca authenticate** vous permet de coller le certificat codé base64 dans l'interface de ligne de commande. Vous pouvez exécuter ces commandes autant de fois que nécessaire pour obtenir les points de confiance appropriés sur l'ASA, mais assurez-vous d'utiliser un nouveau nom de point de confiance pour chaque certificat.

Étape 6. Procurez-vous une copie du certificat d'identité ASA en exécutant cette commande :

crypto ca export asa-identity-cert identity-certificate

Ceci exporte le certificat d'identité du point de confiance nommé asa-identity-cert. Veillez à ajuster le nom de manière à ce qu'il corresponde au point de confiance que vous avez créé à l'étape 4.

Voici la configuration complète des travaux pratiques pour l'ASA :

```
ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 mask 255.255.255.0

group-policy vpn-phone-policy internal
group-policy vpn-phone-policy attributes
     split-tunnel-policy tunnelall
     vpn-tunnel-protocol ssl-client

webvpn
     enable outside
     anyconnect enable

tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attributes
     address-pool vpn-phone-pool
     default-group-policy vpn-phone-policy
```

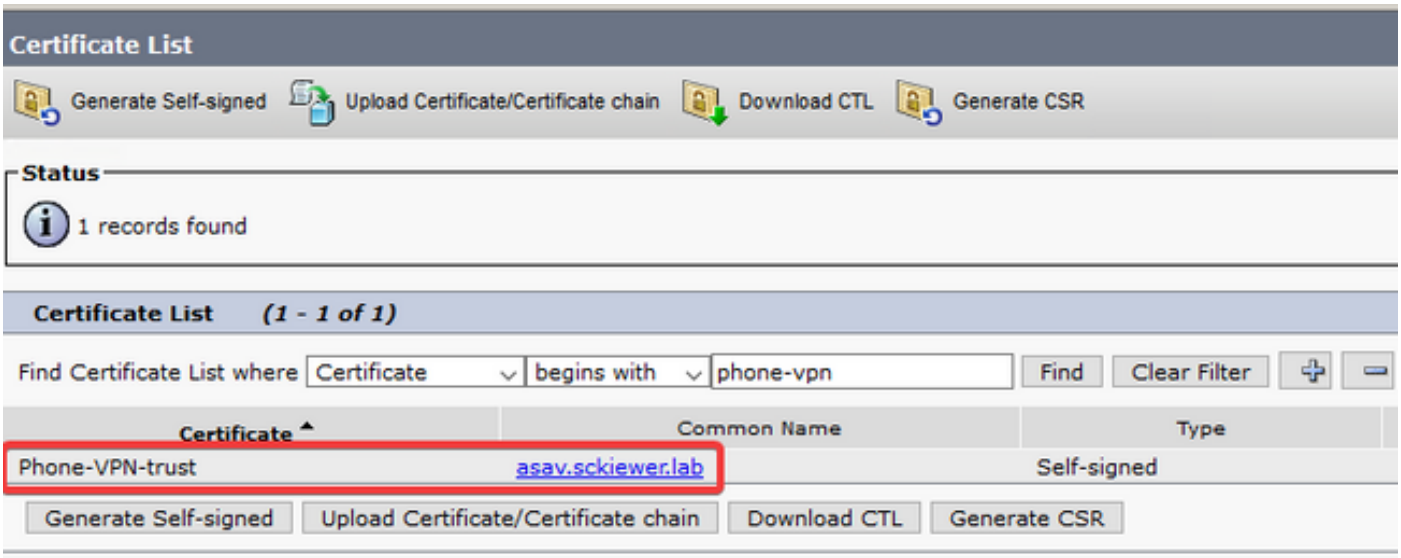
```
tunnel-group vpn-phone-group webvpn-attributes
     authentication certificate
     group-url https://asav.sckiewer.lab/phone enable

ssl trust-point asa-identity-cert outside
```

Àce stade, la configuration ASA est terminée et vous pouvez poursuivre la configuration de CUCM. Vous devez disposer d'une copie du certificat ASA que vous venez de collecter et de l'URL qui a été configurée dans la section tunnel-group.

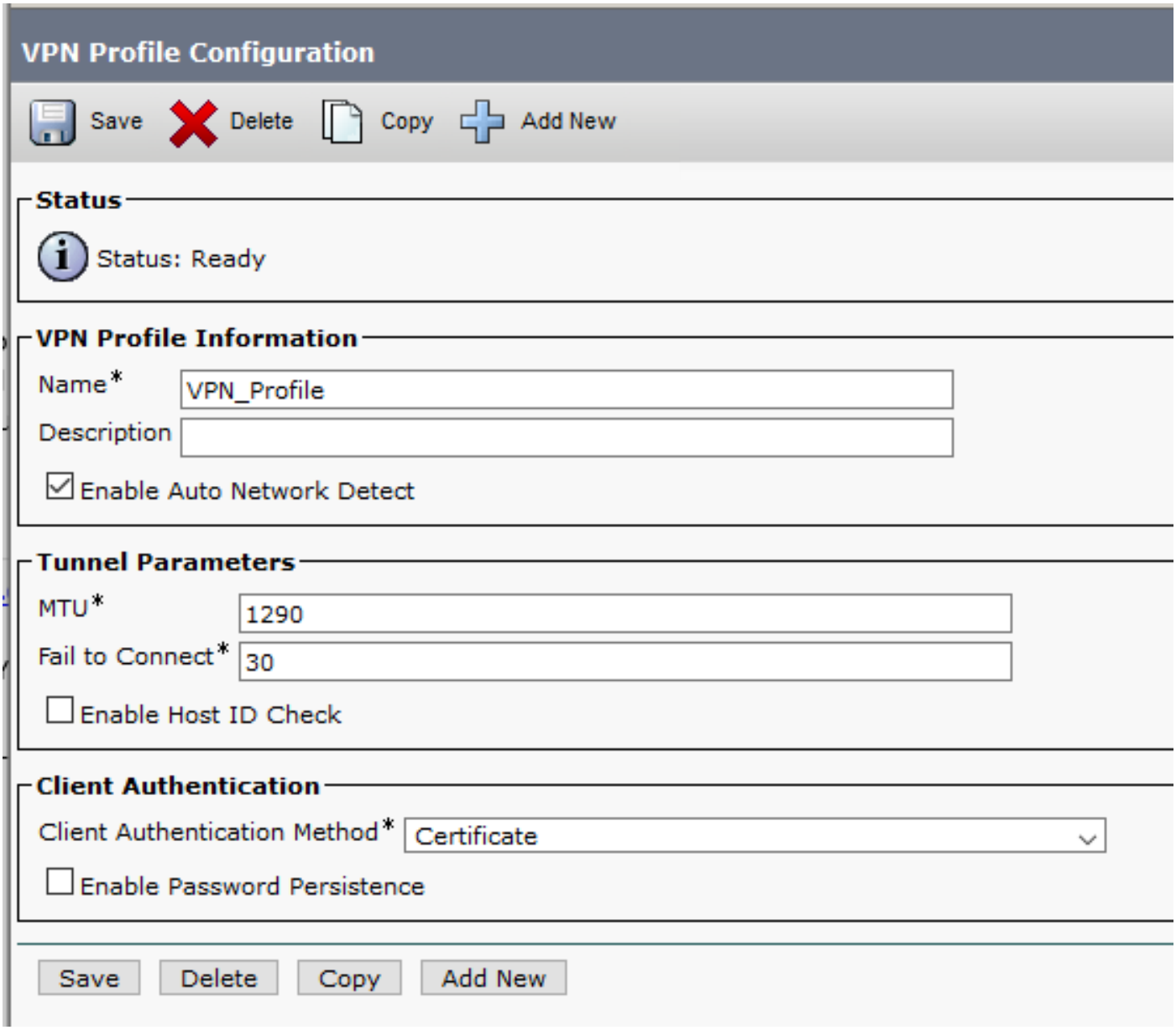
Configuration CUCM

Étape 1. Sur CUCM, accédez à **Cisco Unified OS Administration > Security > Certificate Management** et téléchargez le certificat ASA en tant que **phone-vpn-trust**.

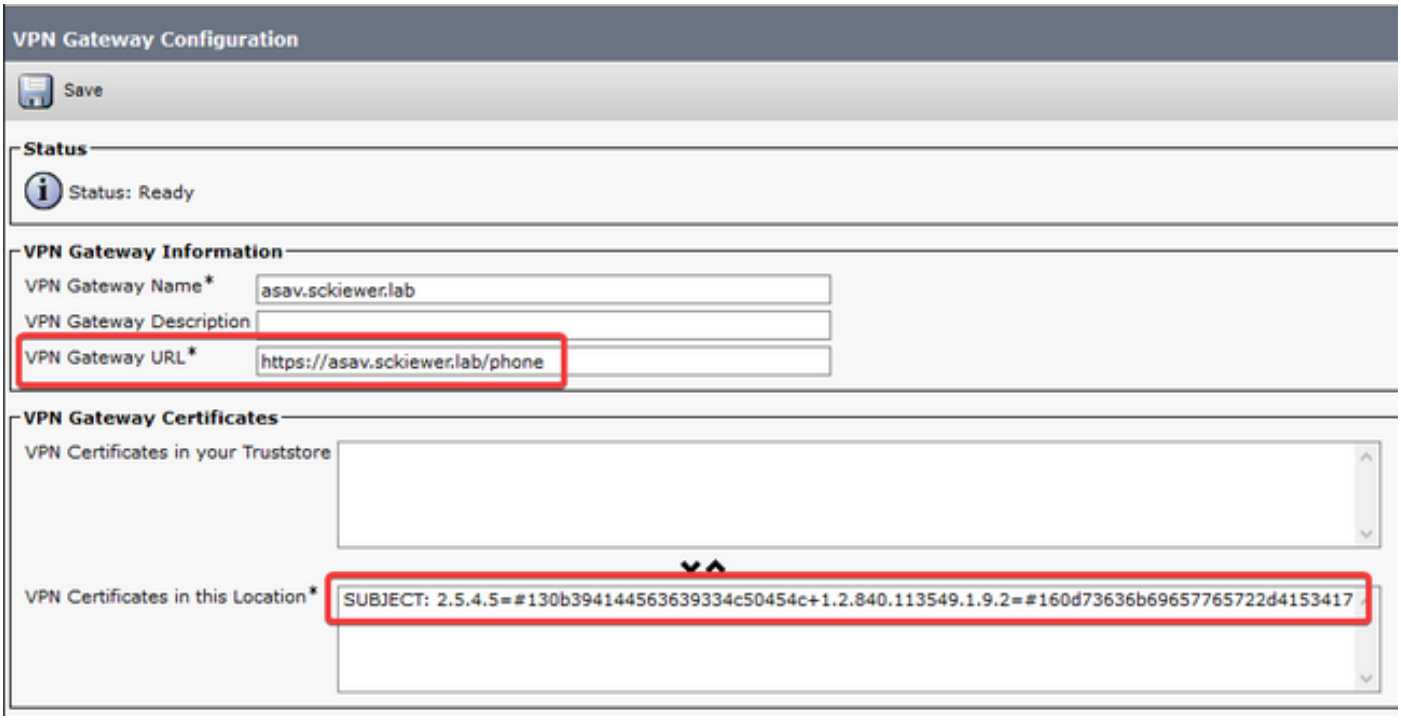


Étape 2. Une fois cette opération effectuée, accédez à **Cisco Unified CM Administration > Advanced Features > VPN > VPN Profile** et créez un nouveau profil. Il n'y a pas de bien ou de mal dans cette section, il est juste important de comprendre le but de chaque paramètre.

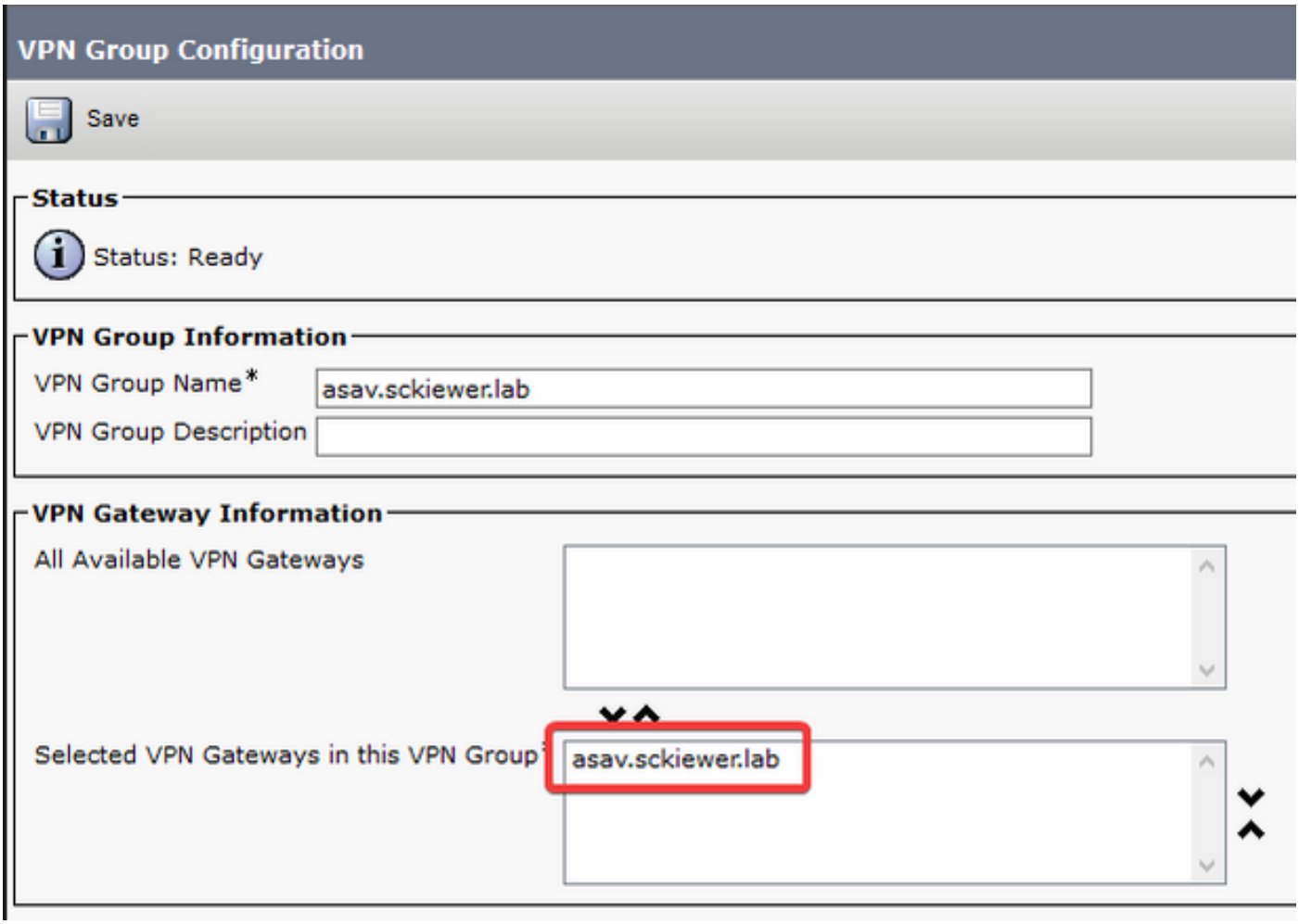
1. **Activer la détection automatique du réseau** : lorsque cette option est activée, le téléphone envoie une requête ping à son serveur TFTP lorsqu'il est sous tension. S'il reçoit une réponse à cette requête ping, il n'active pas VPN. Si le téléphone ne reçoit pas de réponse à cette requête ping, il active le VPN. Lorsque ce paramètre est activé, VPN ne peut pas être activé manuellement.
2. **Vérification de l'ID d'hôte** : lorsque cette option est activée, le téléphone inspecte l'URL VPN à partir de son fichier de configuration (https://asav.sckiewer.lab/phone est utilisé dans ce document) et s'assure que le nom d'hôte ou le nom de domaine complet correspond au nom commun (CN) ou à une entrée SAN dans le certificat présenté par l'ASA.
3. **Authentication Method** - contrôle le type de méthode d'authentification utilisée pour la connexion à l'ASA. Dans l'exemple de configuration de ce document, l'authentification basée sur les certificats est utilisée.
4. **Persistance du mot de passe** : si cette option est activée, le mot de passe du client est stocké dans le téléphone jusqu'à ce qu'une tentative de connexion échouée se produise, que le client efface manuellement le mot de passe ou que le téléphone se réinitialise.



Étape 3. Ensuite, accédez à **Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway**. Vous devez vous assurer que l'URL de votre passerelle VPN correspond à la configuration ASA et que vous déplacez le certificat de la zone supérieure vers la zone inférieure, comme l'indique l'image :

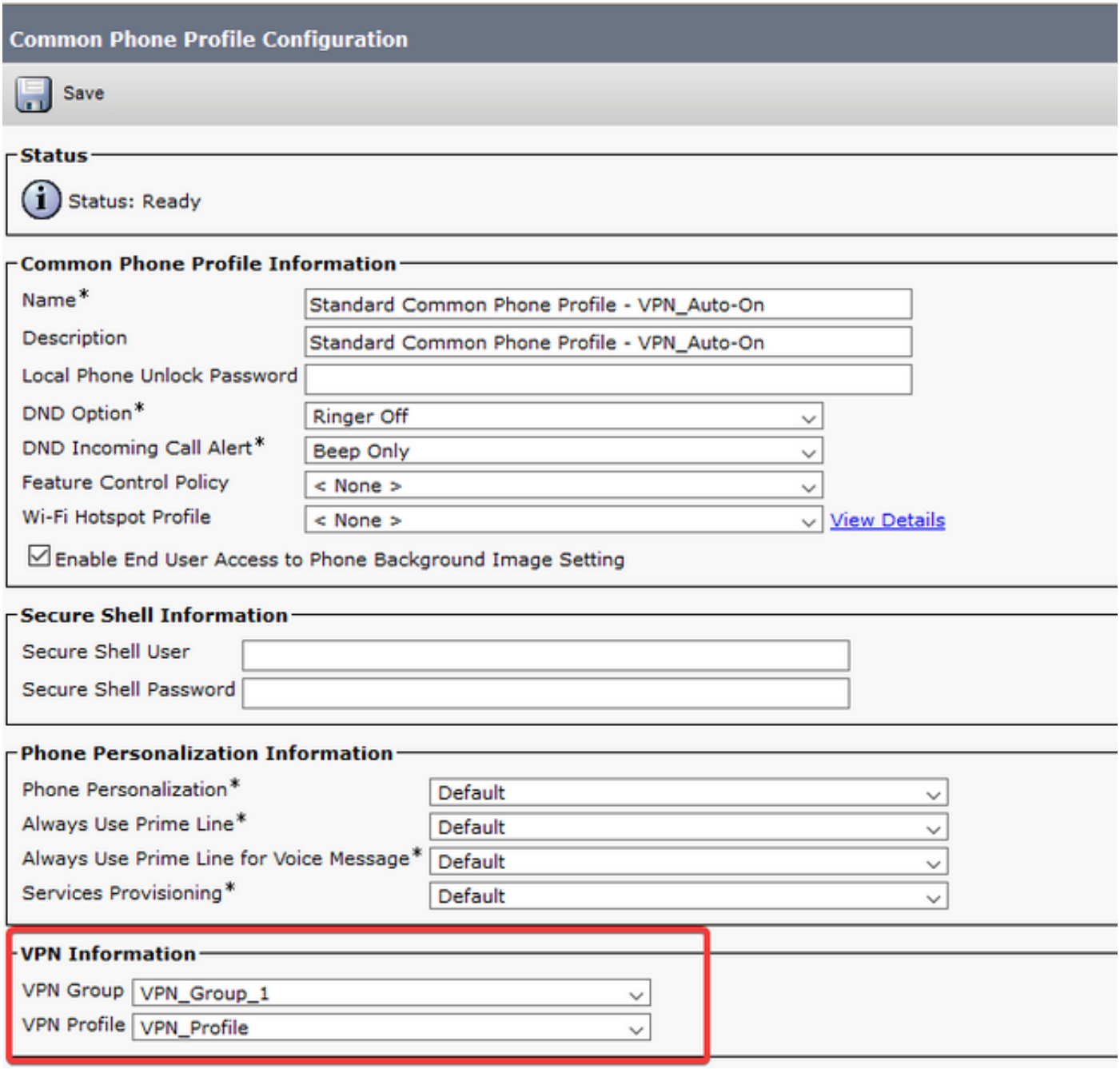


Étape 4. Une fois enregistré, vous devez accéder à **Cisco Unified CM Administration > Advanced Features > VPN > VPN Group** et déplacer la passerelle que vous avez créée vers la zone Selected VPN Gateways in this VPN Group :



Étape 5. Maintenant que les paramètres VPN ont été configurés, vous devez accéder à **Cisco Unified CM Administration > Device > Device Settings > Common Phone Profile**. Ici, vous devez copier le profil utilisé par votre téléphone VPN souhaité, le renommer et sélectionner votre groupe

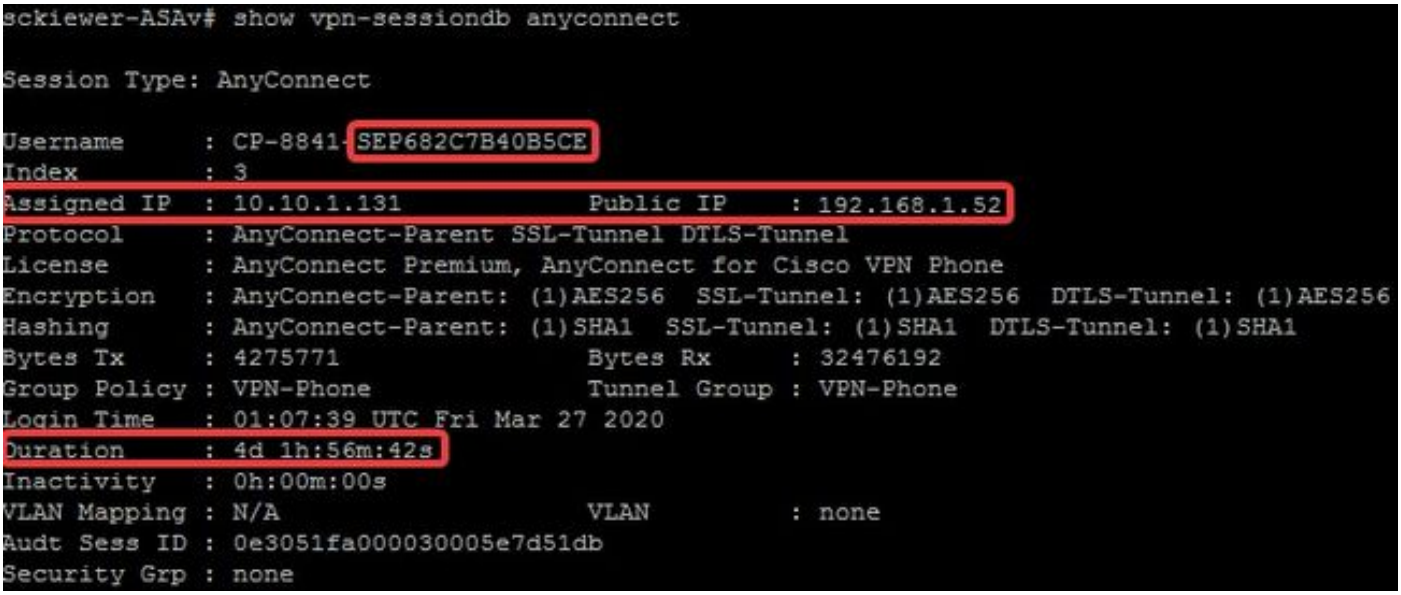
VPN et votre profil VPN, puis enregistrer le nouveau profil :



Étape 6. Enfin, vous devez appliquer ce nouveau profil à votre téléphone, puis réinitialiser le téléphone lorsqu'il se trouve sur le réseau interne. Cela permet au téléphone de recevoir toute cette nouvelle configuration, comme le hachage de certificat ASA et l'URL VPN.

> **Note**: Avant de tester le téléphone, vous devez vous assurer que le serveur TFTP alternatif est configuré sur les téléphones. Comme l'ASA ne fournit pas d'option 150 aux téléphones, l'IP TFTP doit être configuré manuellement sur les téléphones.

Étape 7. Testez le téléphone VPN et vérifiez qu'il peut se connecter correctement à l'ASA et enregistrez-vous. Vous pouvez vérifier que le tunnel est actif sur l'ASA avec, **show vpn-sessiondb anyconnect** :



Dépannage

Données à collecter

Afin de dépanner un problème de téléphone VPN, ces données sont recommandées :

- Débogage de l'ASA: logging buffered debuglogging debug-tracedebug crypto ca transactions 255debug crypto ca messages 255debug crypto ca 255debug webvpn 255debug webvpn anyconnect 255
- Journaux de console téléphonique (ou PRT si le téléphone le prend en charge - plus d'informations ici)

Une fois que vous avez reproduit le problème avec les débogages activés, vous pouvez afficher la sortie avec cette commande car la sortie de débogage contient toujours 711001 :

show log | i 711001

Problèmes courants

> **Note**: Aux fins de cette section, les extraits de journal proviennent d'un téléphone 8861, car il s'agit d'une des séries de téléphones les plus courantes déployées en tant que téléphone VPN. N'oubliez pas que d'autres modèles peuvent écrire différents messages dans les journaux.

Mettre à jour le certificat d'identité auto-signé ASA

Avant l'expiration du certificat d'identité ASA, un nouveau certificat doit être généré et envoyé aux téléphones. Pour ce faire sans impact sur les téléphones VPN, utilisez ce processus :

Étape 1. Créez un nouveau point de confiance pour le nouveau certificat d'identité :

crypto ca trustpoint asa-identity-cert-2

inscription automatique

subject-name CN=asav.sckiewer.lab

crypto ca enroll asa-identity-cert-2

Étape 2. À ce stade, vous auriez un nouveau certificat d'identité pour l'ASA, mais il n'est encore utilisé sur aucune interface. Vous devez exporter ce nouveau certificat et le télécharger vers CUCM :

crypto ca export asa-identity-cert-2 identity-certificate

Étape 3. Une fois que vous avez le nouveau certificat d'identité, téléchargez-le sur l'un de vos noeuds CUCM en tant que téléphone-VPN-trust à l'adresse **Cisco Unified OS Administration > Security > Certificate Management > Upload**.

> **Note**: Le certificat d'approbation du VPN du téléphone actuel ne serait présent que sur le noeud CUCM auquel il a été initialement chargé (il n'est pas automatiquement propagé vers d'autres noeuds comme certains certificats). Si votre version CUCM est affectée par CSCuo58506, vous devez télécharger le nouveau certificat ASA sur un autre noeud.

Étape 4. Une fois le nouveau certificat téléchargé vers l'un des noeuds du cluster, accédez à **Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway** sur le serveur de publication CUCM

Étape 5. Sélectionnez la passerelle appropriée.

Étape 6. Sélectionnez le certificat dans la zone supérieure (celui que vous venez de télécharger) et cliquez sur la flèche vers le bas pour le déplacer vers le bas (ceci permet à TFTP d'ajouter ce certificat dans les fichiers de configuration de votre téléphone VPN) et sélectionnez Enregistrer.

Étape 7. Une fois cela fait, réinitialisez tous les téléphones VPN. À ce stade du processus, l'ASA présente toujours l'ancien certificat, de sorte que les téléphones peuvent se connecter, cependant, ils acquièrent un nouveau fichier de configuration qui contient à la fois le nouveau certificat et l'ancien certificat.

Étape 8. Vous pouvez maintenant appliquer le nouveau certificat à l'ASA. Pour ce faire, vous avez besoin du nom du nouveau point de confiance et du nom de l'interface externe, puis exécutez cette commande avec ces informations :

ssl trust-point asa-identity-cert-2 outside

> **Note**: Vous pouvez accéder à l'URL webvpn dans votre navigateur pour vérifier que l'ASA présente le nouveau certificat. Comme cette adresse doit être accessible au public pour que des téléphones externes puissent l'atteindre, votre PC peut également l'atteindre. Vous pouvez ensuite vérifier le certificat que l'ASA présente à votre navigateur et confirmer qu'il s'agit du nouveau certificat.

Étape 9. Une fois que l'ASA est configuré pour utiliser le nouveau certificat, réinitialisez un téléphone de test et vérifiez qu'il est en mesure de se connecter à l'ASA et de s'enregistrer. Si le téléphone s'enregistre correctement, vous pouvez réinitialiser tous les téléphones et vérifier qu'ils

sont en mesure de se connecter à l'ASA et de s'enregistrer. Il s'agit du processus recommandé car les téléphones connectés à l'ASA restent connectés après la modification du certificat. Si vous testez d'abord votre mise à jour de certificat sur un téléphone, vous réduisez le risque de problème de configuration affectant un grand nombre de téléphones. Si le premier téléphone VPN ne parvient pas à se connecter à l'ASA, vous pouvez collecter des journaux à partir du téléphone et/ou de l'ASA pour le dépanner pendant que les autres téléphones restent connectés.

Étape 10. Une fois que vous avez vérifié que les téléphones sont en mesure de se connecter et de s'enregistrer avec le nouveau certificat, l'ancien certificat peut être supprimé de CUCM.

ASA sélectionne le chiffon de courbe elliptique (EC)

Les ASA prennent en charge la cryptographie Elliptic Curve (EC) à partir de la version 9.4(x), il est donc courant de voir des téléphones VPN précédemment actifs échouer après une mise à niveau ASA vers la version 9.4(x) ou supérieure. Cela se produit parce que l'ASA sélectionne maintenant un chiffrement EC lors de la connexion TLS avec des modèles de téléphone plus récents. En règle générale, il existe un certificat RSA associé à l'interface à laquelle le téléphone se connecte, car la version ASA précédente ne prenait pas en charge EC. À ce stade, étant donné que l'ASA a sélectionné un chiffrement EC, il ne peut pas utiliser de certificat RSA pour la connexion, il génère et envoie au téléphone un certificat auto-signé temporaire qu'il crée avec l'algorithme EC plutôt qu'avec RSA. Comme ce certificat temporaire n'est pas reconnu par le téléphone, la connexion échoue. Vous pouvez vérifier ceci dans les journaux de téléphone 88xx est assez simple.

```
2101 NOT Mar 30 12:23:21.331861 (393:393) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
2102 NOT Mar 30 12:23:21.331871 (393:393) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
```

Les journaux téléphoniques montrent que l'ASA a sélectionné un chiffrement EC pour cette connexion, car la ligne 'nouveau chiffrement' contient des chiffrement EC, ce qui provoque l'échec de la connexion.

Dans un scénario où AES a été sélectionné, vous verriez ceci :

```
2691 NOT Mar 30 12:18:19.016923 (907:907) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
2690 NOT Mar 30 12:18:19.016943 (907:907) VPNC: -protocol_handler: new cipher -> AES256-
SHA:AES128-SHA
```

Vous trouverez plus d'informations à ce sujet ici, CSCuu02848.

La solution serait de désactiver les chiffrements EC sur l'ASA pour la version TLS que votre téléphone utilise. Pour plus d'informations sur la version TLS prise en charge par chaque modèle de téléphone, cliquez ici :

Table 6 lists the TLS versions supported by the Cisco IP phones.

Table 6. TLS version support

	Phone Models			
Version	7900	6900, 8900, 9900	7811, 7821, 7841, 7861	8811, 8821, 8841, 8845, 8851, 8861, 8865
TLS 1.0	Yes	Yes	Yes	Yes
TLS 1.2	No	No	Yes	Yes
Disable TLS 1.0 and TLS 1.1 with https for web access*	No	No	Yes	Yes
Selectively Disable TLS cipher suites used by TLS connection or handshake**	No	No	Yes	Yes

* With 12.1 firmware
** With 12.5 firmware

https://www.cisco.com/c/dam/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-c11-739097.pdf

Une fois que vous savez quelles versions TLS sont pertinentes dans votre environnement, vous pouvez exécuter ces commandes sur l'ASA pour désactiver les chiffrement EC pour ces versions :

```
ssl cipher tlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"
ssl cipher dtlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"
```

Gardez à l'esprit que les téléphones IP utilisent par défaut DTLS (Datagram Transport Layer Security), vous devez donc exécuter l'instruction de chiffrement pour DTLS et la version TLS appropriée pour vos téléphones. En outre, il est important de comprendre que ces modifications sont des modifications globales sur l'ASA, de sorte qu'elles empêchent les algorithmes de chiffrement EC d'être négociés par tout autre client AnyConnect qui utilise ces versions TLS.

Échec de la connexion DTLS

Dans certains cas, les téléphones VPN ne peuvent pas établir de connexion à l'ASA avec DTLS. Si le téléphone tente d'utiliser DTLS mais qu'il échoue, le téléphone continue à essayer DTLS encore et encore, sans succès, car il sait que DTLS est activé. Vous verriez ceci dans les journaux du téléphone 88xx :

```
3249 ERR Mar 29 15:22:38.949354 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert: fatal:illegal parameter
3250 NOT Mar 29 15:22:38.951428 (385:385) VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status: 0x0 error: 0x0
3251 ERR Mar 29 15:22:38.951462 (385:385) VPNC: -alert_err: DTLS write alert: code 47, illegal parameter
3252 ERR Mar 29 15:22:38.951489 (385:385) VPNC: -create_dtls_connection: SSL_connect ret -1, error 1
```

```
3253 ERR Mar 29 15:22:38.951506 (385:385) VPNC: -DTLS: SSL_connect: SSL_ERROR_SSL (error 1)
3254 ERR Mar 29 15:22:38.951552 (385:385) VPNC: -DTLS: SSL_connect: error:140920C5:SSL
routines:ssl3_get_server_hello:old session cipher not returned
3255 ERR Mar 29 15:22:38.951570 (385:385) VPNC: -create_dtls_connection: DTLS setup failure,
cleanup
3256 WRN Mar 29 15:22:38.951591 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert:
warning:close notify
3257 ERR Mar 29 15:22:38.951661 (385:385) VPNC: -do_dtls_connect: create_dtls_connection failed
3258 ERR Mar 29 15:22:38.951722 (385:385) VPNC: -protocol_handler: connect: do_dtls_connect
failed
3259 WRN Mar 29 15:22:38.951739 (385:385) VPNC: -protocol_handler: connect : err: SSL success
DTLS fail
```

Cela peut être dû au même problème mentionné dans la section Cipher de courbe elliptique (EC) ASA Selecting, vous devez donc vous assurer que les chiffrement EC sont désactivés pour DTLS. En outre, vous pouvez désactiver DTLS, ce qui force les téléphones VPN à utiliser TLS à la place. Cela ne serait pas idéal car cela signifierait que tout le trafic utiliserait TCP plutôt que UDP, ce qui ajouterait une certaine surcharge. Cependant, dans certains scénarios, il s'agit d'un bon test, car il confirme au moins que la plupart de la configuration est correcte et que le problème est spécifique à DTLS. Si vous voulez tester cela, il est préférable de le faire au niveau de la stratégie de groupe, car les administrateurs utilisent généralement une stratégie de groupe unique pour les téléphones VPN, ce qui nous permet de tester une modification sans affecter les autres clients.

attributs group-policy vpn-phone-policy
webvpn
anyconnect ssl dtls none

Un autre problème de configuration courant qui peut empêcher une connexion DTLS réussie est si le téléphone ne peut pas établir la connexion TLS et DTLS avec le même chiffrement. Exemple d'extrait de journal :

```
%%%%% TLS Ciphers Offered
3905 NOT Apr 01 20:14:22.741838 (362:362) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA

%%%%% DTLS Ciphers Offered
4455 NOT Apr 01 20:14:23.405417 (362:362) VPNC: -process_connect: x-dtls-ciphersuite: AES128-SHA
4487 NOT Apr 01 20:14:23.523994 (362:362) VPNC: -create_dtls_connection: cipher list: AES128-SHA

%%%%% DTLS connection failure
4496 WRN Apr 01 20:14:53.547046 (362:474) VPNC: -vpnc_control: conn timer expired at:1585772093,
to abort connect
4497 NOT Apr 01 20:14:53.547104 (362:474) VPNC: -abort_connect: in dtls setup phase
```

Vous pouvez voir les chiffrements TLS offerts dans la première ligne à partir de l'extrait. L'option la plus sécurisée prise en charge par les deux côtés est sélectionnée (les journaux n'affichent pas la sélection, cependant, vous pouvez déduire qu'elle est au moins AES-256 de l'extrait de journal). Vous pouvez également voir que le seul chiffrement DTLS proposé est AES128. Comme le chiffrement TLS sélectionné n'est pas disponible pour DTLS, la connexion échoue. La solution dans ce scénario serait de s'assurer que la configuration ASA permet d'utiliser les mêmes algorithmes de chiffrement pour TLS et DTLS.

Le téléphone ne peut pas se connecter à ASA après la mise à jour du certificat

Il est très important de télécharger un nouveau certificat d'identité ASA en tant que phone-vpn-trust sur CUCM afin que les téléphones puissent acquérir le hachage de ce nouveau certificat. Si

ce processus n'est pas suivi, après la mise à jour et la prochaine fois qu'un téléphone VPN tente de se connecter à l'ASA, le téléphone reçoit un certificat auquel il n'a pas confiance, de sorte que la connexion échoue. Cela peut se produire quelques jours ou semaines après la mise à jour du certificat ASA, car les téléphones ne sont pas déconnectés lorsque le certificat change. Tant que l'ASA continue à recevoir des messages de veille du téléphone, le tunnel VPN reste actif. Par conséquent, si vous avez confirmé que le certificat ASA a été mis à jour, mais que le nouveau certificat n'a pas été mis sur CUCM en premier, vous avez deux options :

1. Si l'ancien certificat d'identité ASA est toujours valide, rétablir l'ASA à l'ancien certificat, puis suivre le processus fourni dans ce document pour mettre à jour le certificat. Vous pouvez ignorer la section de génération de certificats si vous avez déjà généré un nouveau certificat.
2. Si l'ancien certificat d'identité ASA a expiré, vous devez télécharger le nouveau certificat ASA sur CUCM et ramener les téléphones sur le réseau interne pour recevoir le fichier de configuration mis à jour avec le nouveau hachage de certificat.

Le téléphone ne peut pas résoudre l'URL ASA via DNS

Dans certains scénarios, l'administrateur configure l'URL VPN avec un nom d'hôte plutôt qu'une adresse IP. Lorsque cela est fait, le téléphone doit disposer d'un serveur DNS pour pouvoir résoudre le nom en adresse IP. Dans l'extrait, vous pouvez voir que le téléphone tente de résoudre le nom avec ses deux serveurs DNS, 192.168.1.1 et 192.168.1.2, mais ne reçoit pas de réponse. Au bout de 30 secondes, le téléphone imprime une erreur 'DnsLookupErr:'

```
3816 NOT Mar 3 15:38:03.819168 VPNC: -do_login: URL -> https://asav.sckiewer.lab/phone
...
3828 INF Mar 3 15:38:03.834915 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3829 INF Mar 3 15:38:03.835004 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3830 INF Mar 3 15:38:03.835030 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3831 INF Mar 3 15:38:17.845305 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3832 INF Mar 3 15:38:17.845352 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3833 INF Mar 3 15:38:17.845373 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3834 INF Mar 3 15:38:31.854834 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3835 INF Mar 3 15:38:31.854893 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3836 INF Mar 3 15:38:31.855213 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3837 ERR Mar 3 15:38:32.864376 VPNC: -parse_url: gethostbyname failed <asav.sckiewer.lab>
3838 NOT Mar 3 15:38:32.864435 VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status:
0x0 error: 0x0
3839 ERR Mar 3 15:38:32.864464 VPNC: -do_login: parse URL failed ->
https://asav.sckiewer.lab/phone
3840 NOT Mar 3 15:38:32.864482 VPNC: -vpn_stop: de-activating vpn
3841 NOT Mar 3 15:38:32.864496 VPNC: -vpn_set_auto: auto -> auto
3842 NOT Mar 3 15:38:32.864509 VPNC: -vpn_set_active: activated -> de-activated
3843 NOT Mar 3 15:38:32.864523 VPNC: -set_login_state: LOGIN: 1 (TRYING) --> 3 (FAILED)
3844 NOT Mar 3 15:38:32.864538 VPNC: -set_login_state: VPNC : 1 (LoggingIn) --> 3 (LoginFailed)
3845 NOT Mar 3 15:38:32.864561 VPNC: -vpnc_send_notify: notify type: 1 [LoginFailed]
3846 NOT Mar 3 15:38:32.864580 VPNC: -vpnc_send_notify: notify code: 32 [DnsLookupErr]
3847 NOT Mar 3 15:38:32.864611 VPNC: -vpnc_send_notify: notify desc: [url hostname lookup err]
```

Ceci indique généralement l'une des valeurs suivantes :

1. Le téléphone possède un serveur DNS non valide
2. Le téléphone n'a pas reçu de serveur DNS via DHCP ou n'a pas été configuré manuellement

Pour résoudre ce problème, deux options sont possibles :

1. Vérifiez la configuration du téléphone pour vous assurer qu'il reçoit un serveur DNS du

serveur DHCP lorsqu'il est externe et/ou vérifiez que le serveur DNS du téléphone peut résoudre le nom utilisé dans la configuration ASA
2. Modifier l'URL dans la configuration ASA et CUCM en une adresse IP afin que DNS ne soit pas requis

Le téléphone n'active pas VPN

Comme mentionné précédemment dans ce document, la détection automatique du réseau entraîne le téléphone à envoyer une requête ping au serveur TFTP et à rechercher une réponse. Si le téléphone se trouve sur le réseau interne, alors le serveur TFTP est accessible sans VPN, donc quand le téléphone reçoit des réponses aux requêtes ping, il n'active pas VPN. Lorsque le téléphone n'est PAS sur le réseau interne, les requêtes ping échouent, de sorte que le téléphone active ensuite le VPN et se connecte à l'ASA. Gardez à l'esprit que le réseau domestique d'un client ne sera probablement pas configuré pour fournir au téléphone une option 150 via DHCP, et l'ASA ne peut pas non plus fournir une option 150, de sorte que 'Autre TFTP' est une condition requise pour les téléphones VPN.

Dans les journaux, vous devez vérifier quelques éléments :

1. Le téléphone envoie-t-il une requête ping à l'adresse IP du serveur TFTP CUCM ?
2. Le téléphone reçoit-il une réponse aux requêtes ping ?
3. Le téléphone active-t-il le VPN après ne pas recevoir de réponse aux requêtes ping ?

Il est important d'afficher ces éléments dans cet ordre. Dans un scénario où le téléphone envoie une requête ping à une adresse IP incorrecte et reçoit une réponse, il serait inutile d'activer les débogages sur l'ASA car le téléphone n'active pas VPN. Validez ces 3 éléments dans cet ordre afin d'éviter une analyse de journal inutile. Vous le verrez dans les journaux du téléphone 88xx si la requête ping échoue et si le VPN est activé par la suite :

```
5645 NOT Mar 27 11:32:34.630109 (574:769) JAVA-vpnAutoDetect: ping time out
5647 DEB Mar 27 11:32:34.630776 (710:863) JAVA-configmgr MQThread|cip.vpn.VpnStateHandler:? -
VpnStateHandler: handleVPN_ENABLED_STATE()
```

Enregistrement du téléphone mais impossible d'afficher l'historique des appels

Vérifiez que le mode TFTP alternatif est activé sur le téléphone et que l'adresse IP TFTP correcte est configurée. Un autre TFTP est requis pour les téléphones VPN car l'ASA ne peut pas fournir une option 150.

Informations connexes

- Support et documentation techniques - Cisco Systems