Configurez le joncteur réseau de TLS de SIP sur le gestionnaire de transmissions avec un certificat signé CA.

Contenu

Introduction

Ce document décrit un processus pas à pas pour configurer le joncteur réseau de Transport Layer Security de Protocole SIP (Session Initiation Protocol) (TLS) sur le gestionnaire de transmissions avec un certificat signé d'Autorité de certification (CA).

Après avoir suivi ce document, des messages SIP entre deux batteries seront chiffrés utilisant le TLS.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de :

- Cisco Unified Communications Manager (CUCM)
- SIP

Composants utilisés

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

- Version 9.1(2) CUCM
- Version 10.5(2) CUCM
- Microsoft Windows Server 2003 comme CA

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.

Informations générales

Suivant les indications de cette image, prise de contact SSL utilisant des Certificats.

Configurez

Étape 1. Utilisez le public CA ou l'installation CA sur les Windows Server 2003

Référez-vous au lien : L'installation CA sur Windows 2003 divisent

Étape 2. Vérifiez l'adresse Internet et les configurations

Des Certificats sont basés sur des noms. Assurez-vous que les noms sont corrects avant de commencer.

```
From SSH CLI
admin:show cert own CallManager
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
```

Afin de changer l'adresse Internet, référez-vous au lien : Adresse Internet de modification sur CUCM

Étape 3. Générez et téléchargez la demande de signature de certificat (le CSR)

CUCM 9.1(2)

Afin de générer le CSR, naviguez vers l'**admin de SYSTÈME D'EXPLOITATION** > la **Gestion de Sécurité** > de **certificat** > **génèrent le CSR**

Dans la zone d'**identification de certificat,** option choisie de **CallManager de la** liste déroulante.

Afin de télécharger le CSR, naviguez **CSR** vers l'**admin de SYSTÈME D'EXPLOITATION > la Sécurité > de certificat Gestion > téléchargement**

Dans la zone d'**identification de certificat**, option choisie de **CallManager de la** liste déroulante.

CUCM 10.5(2)

Afin de générer le CSR, naviguez vers l'**admin de SYSTÈME D'EXPLOITATION > la Gestion de Sécurité > de certificat > génèrent le CSR**

1. Dans le domaine de **but de certificat, CallManager** choisi de la liste déroulante.

2. Dans le domaine de **longueur principale,** sélectionnez **1024 de la** liste déroulante.
3. Dans le domaine d'**algorithme de hachage, SHA1** choisi de la liste déroulante.

Afin de télécharger le CSR, naviguez **CSR** vers l'**admin de SYSTÈME D'EXPLOITATION > la Sécurité > de certificat Gestion > téléchargement**

Dans le domaine de **but de certificat,** option choisie de **CallManager de la** liste déroulante.

> Remarque: Le CSR de CallManager est généré avec les 1024 clés de Rivest-Shamir-Addleman de bit (RSA).

Étape 4. Signez le CSR avec l'autorité de certification de Microsoft Windows 2003

C'est des informations facultatives pour signer le CSR avec le Microsoft Windows 2003 CA.

1. Ouvrez l'autorité de certification.

2. Cliquez avec le bouton droit l'icône **CA** et naviguez vers **toutes les tâches > soumettent la nouvelle demande**

3. Sélectionnez le CSR et cliquez sur l'option **ouverte** (applicable dans chacun des deux le CSRs (CUCM 9.1(2) et CUCM 10.5(2))

4. Tout les affichage ouvert de CSRs dans le répertoire en attente de demandes. Cliquez avec le bouton droit chaque CSR et naviguez vers **toutes les tâches > question** afin de délivrer les Certificats. (Applicable dans chacun des deux le CSRs (CUCM 9.1(2) et CUCM 10.5(2))

5. Afin de télécharger le certificat, choisissez le répertoire **émis de Certificats**.

Cliquez avec le bouton droit le certificat et cliquez sur l'option **ouverte**.

6. Les détails de certificat sont affichés. Afin de télécharger le certificat, sélectionner les **détails** tabulent et cliquent sur la **copie de** bouton **pour classer…**

7. Dans la fenêtre d'**assistant d'exportation de certificat**, cliquez sur le **Base-64 a encodé X.509(.CER) la** case d'option.

8. Nommez le fichier exactement. Cet exemple utilise le format de **CUCM1052.cer**.

Pour CUCM 9.1(2), suivez la même procédure.

Étape 5. Obtenez le certificat racine du CA

Ouvrez la fenêtre d'**autorité de certification**.

Afin de télécharger le racine-CA

1. Cliquez avec le bouton droit l'icône CA et cliquez sur l'option de **Properties**.

2. En général ONGLET, **certificat de vue de** clic.

3. Dans la fenêtre de **certificat**, cliquez sur l'ONGLET de détails.

4. **Copie de** clic **à classer…**

Étape 6. Certificat racine du téléchargement CA comme confiance de CallManager

Afin de télécharger le certificat racine CA, procédure de connexion à l'**admin de SYSTÈME D'EXPLOITATION > à la Gestion de Sécurité > de certificat > au certificat de téléchargement/à chaîne de certificat**

> Remarque: Exécutez ces étapes sur chacun des deux le CUCMs (CUCM 9.1(2) et CUCM 10.5(2))

Étape 7. Certificat CSR de CallManager de signe du téléchargement CA comme certificat de CallManager.

Afin de télécharger le CSR de CallManager de signe CA, procédure de connexion à l'**admin de SYSTÈME D'EXPLOITATION > à la Sécurité > à la Gestion de certificat > au certificat de téléchargement/à chaîne de certificat**

> Remarque: Exécutez ces étapes sur chacun des deux le CUCMs (CUCM 9.1(2) et CUCM 10.5(2))

Étape 8. Créez les profils de Sécurité de joncteur réseau de SIP

CUCM 9.1(2)

Afin de créer le profil de Sécurité de joncteur réseau de SIP, naviguez **profil de Sécurité** vers le **système > la Sécurité > de SIP joncteur réseau**.

Copiez exister profil non sécurisé de joncteur réseau de SIP et donnez-lui un nouveau nom. Dans l'exemple, le profil non sécurisé de joncteur réseau de SIP a été renommé avec le TLS sécurisé de profil de joncteur réseau de SIP.

Dans l'utilisation du **nom du sujet X.509 le** nom commun (NC) du CUCM 10.5(2) (certificat signé CA) suivant les indications de cette image.

CUCM 10.5(2)

Naviguez **profil de Sécurité** vers le **système > la Sécurité > de SIP joncteur réseau.**

Copiez exister profil non sécurisé de joncteur réseau de SIP et donnez-lui un nouveau nom. Dans l'exemple, le profil non sécurisé de joncteur réseau de SIP a été renommé avec le TLS sécurisé de profil de joncteur réseau de SIP.

Dans l'utilisation du nom du sujet X.509 la NC du CUCM 9.1(2) (certificat signé CA) comme mis en valeur :

Les les deux les profils de Sécurité de joncteur réseau de SIP placent un port d'entrée de 5061, dans lesquels chaque batterie écoute sur le port TCP 5061 les nouveaux appels d'arrivée de TLS de SIP.

Étape 9. Créez les joncteurs réseau de SIP

Après que les profils de Sécurité soient créés, créez les joncteurs réseau de SIP et apportez les modifications pour le paramètre de configuration ci-dessous sur le joncteur réseau de SIP.

CUCM 9.1(2)

1. Sur la fenêtre de configuration de joncteur réseau de SIP, vérifiez le paramètre de configuration SRTP permis la case à cocher.

Ceci sécurise le Protocole RTP (Real-Time Transport Protocol) à utiliser pour les appels au-dessus de ce joncteur réseau. Cette case doit seulement être cochée quand vous utilisez le TLS de SIP parce que les clés pour le protocole de transport en temps réel Secure (SRTP) sont permutées dans le corps du message SIP. La signalisation de SIP doit être sécurisée par TLS, autrement n'importe qui avec la signalisation non-sécurisée de SIP pourrait déchiffrer le flot correspondant SRTP au-dessus du joncteur réseau.

2. Sur la section Informations de SIP de la fenêtre de configuration de joncteur réseau de SIP, profil de Sécurité ajoutez l'adresse de destination, la destination port, et de SIP joncteur réseau.

CUCM 10.5(2)

1. Sur la fenêtre de configuration de joncteur réseau de SIP, vérifiez le paramètre de configuration SRTP permis la case à cocher.

Ceci permet SRTP à utiliser pour des appels au-dessus de ce joncteur réseau. Cette case doit seulement être cochée en utilisant le TLS de SIP, parce que les clés pour SRTP sont permutées dans le corps du message SIP. La signalisation de SIP doit être sécurisée par le TLS parce que n'importe qui avec une signalisation non-sécurisée de SIP pourrait déchiffrer le flot sécurisé correspondant de RTP au-dessus du joncteur réseau.

2. Sur la section Informations de SIP de la fenêtre de configuration de joncteur réseau de SIP, ajoutez l'adresse IP de destination, la destination port, et le profil de Sécurité

Étape 10. Créez les modèles d'artère

La méthode la plus simple est de créer un modèle d'artère sur chaque batterie, indiquant directement le joncteur réseau de SIP. Des groupes et les listes de routage d'artère ont pu également être utilisés.

Les points CUCM 9.1(2) pour conduire le modèle 9898 par l'intermédiaire du TLS SIROTENT le joncteur réseau au CUCM 10.5(2)

Les points CUCM 10.5(2) pour conduire le modèle 1018 par l'intermédiaire du TLS SIROTENT le joncteur réseau au CUCM 9.1(2)

Vérifiez

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

Dépannez

L'appel de TLS de SIP peut être mis au point avec ces étapes.

Collectez la capture de paquet sur CUCM

Afin de vérifier la Connectivité entre le CUCM 9.1(2) et le CUCM 10.5(2), prendre une capture de paquet sur les serveurs et la montre CUCM pour le TLS de SIP trafiquez.

Le trafic de TLS de SIP est transmis sur le port TCP 5061, vu comme sip-tls.

Dans l'exemple suivant il y a une session ILC de SSH établie au CUCM 9.1(2)

1. Capture de paquet CLI sur l'écran

Ce CLI imprime la sortie sur l'écran pour le trafic de TLS de SIP.

```
admin:utils network capture host ip 10.106.95.200
Executing command with options:
interface=eth0
ip=10.106.95.200
19:04:13.410944 IP CUCMA.42387 > 10.106.95.200.sip-tls: P 790302485:790303631(1146) ack
3661485150 win 182 <nop,nop,timestamp 2864697196 5629758>
19:04:13.450507 IP 10.106.95.200.sip-tls > CUCMA.42387: . ack 1146 win 249 <nop,nop,timestamp
6072188 2864697196>
19:04:13.465388 IP 10.106.95.200.sip-tls > CUCMA.42387: P 1:427(426) ack 1146 win 249
<nop,nop,timestamp 6072201 2864697196>
```

2. Captures CLI à classer

Ce CLI fait la capture de paquet basée sur l'hôte et crée un fichier nommé des paquets.

```
admin:utils network capture eth0 file packets count 100000 size all host ip 10.106.95.200
```

Redémarrez le joncteur réseau de SIP sur CUCM 9.1(2) et faites l'appel à partir de l'extension 1018 (CUCM 9.1(2)) à l'extension 9898 (CUCM 10.5(2))

Afin de télécharger le fichier du CLI, exécutez cette commande :

```
admin:file get activelog platform/cli/packets.cap
```

La capture est faite dans le format standard .cap. Cet exemple emploie Wireshark pour ouvrir le fichier packets.cap mais n'importe quel outil d'affichage de capture de paquet peut être utilisé.

1. Le Protocole TCP (Transmission Control Protocol) synchronisent (synchronisation) pour établir la transmission de TCP entre le CUCM 9.1(2)(Client) et le CUCM 10.5(2)(Server).
2. Le CUCM 9.1(2) envoie le client bonjour pour commencer la session de TLS.
3. Le CUCM 10.5(2) envoie le serveur bonjour, le certificat de serveur, et la demande de certificat de commencer le processus d'échange de certificat.
4. Le certificat que le client CUCM 9.1(2) envoie pour se terminer l'échange de certificat.
5. Les données des applications qui sont signalisation chiffrée de SIP, prouvent que la session

de TLS a été établie.

Promouvez le contrôle si les Certificats corrects sont permutés. Après serveur bonjour, le serveur CUCM 10.5(2) envoie son certificat au client CUCM 9.1(2).

Le numéro de série et les informations soumises que le serveur CUCM 10.5(2) a, est présenté au numéro de série du client CUCM 9.1(2).The, sujet, émetteur, et des dates de validité toutes sont comparées aux informations à la page de Gestion de certificat d'admin de SYSTÈME D'EXPLOITATION.

Le serveur que CUCM 10.5(2) présente son propre certificat pour la vérification, maintenant il vérifie le certificat du client CUCM 9.1(2). La vérification se produit dans les deux directions.

S'il y a une non-concordance entre les Certificats dans la capture de paquet et les Certificats dans la page Web d'admin de SYSTÈME D'EXPLOITATION, alors les Certificats corrects ne sont pas téléchargés.

Les Certificats corrects doivent être téléchargés sur la page de CERT d'admin de SYSTÈME D'EXPLOITATION.

Collectez les suivis CUCM

Les suivis CUCM peuvent également être utiles de déterminer quels messages sont permutés entre le CUCM 9.1(2) et les serveurs CUCM 10.5(2) et si la session SSL est correctement établie.

Dans l'exemple, les suivis du CUCM 9.1(2) ont été collectés.

Écoulement d'appel :

Ext. 1018 > CUCM 9.1(2) > JONCTEUR RÉSEAU de TLS de SIP > CUCM 10.5(2) > ext. 9898

Analyse de chiffre ++

```
04530161.009 |19:59:21.185 |AppInfo |Digit analysis: match(pi="2", fqcn="1018",
cn="1018",plv="5", pss="", TodFilteredPss="", dd="9898",dac="0")
04530161.010 |19:59:21.185 |AppInfo |Digit analysis: analysis results
04530161.011 |19:59:21.185 |AppInfo ||PretransformCallingPartyNumber=1018
|CallingPartyNumber=1018
|DialingPartition=
|DialingPattern=9898
|FullyQualifiedCalledPartyNumber=9898
```

Le TLS de SIP ++ est utilisé sur le port 5061 pour cet appel.

```
04530191.034 |19:59:21.189 |AppInfo |//SIP/SIPHandler/ccbId=0/scbId=0/SIP_PROCESS_ENQUEUE:
createConnMsg tls_security=3
04530204.002 |19:59:21.224 |AppInfo
|//SIP/Stack/Transport/0x0/sipConnectionManagerProcessConnCreated: gConnTab=0xb444c150,
addr=10.106.95.200, port=5061, connid=12, transport=TLS Over TCP
04530208.001 |19:59:21.224 |AppInfo |SIPTcp - wait_SdlSPISignal: Outgoing SIP TCP message to
10.106.95.200 on port 5061 index 12
[131,NET]
INVITE sip:9898@10.106.95.200:5061 SIP/2.0
Via: SIP/2.0/TLS 10.106.95.203:5061;branch=z9hG4bK144f49a43a
From: <sip:1018@10.106.95.203>;tag=34~4bd244e4-0988-4929-9df2-2824063695f5-19024196
To: <sip:9898@10.106.95.200>
Call-ID: 94fffc00-57415541-7-cb5f6a0a@10.106.95.203
User-Agent: Cisco-CUCM9.1
```

Le message SIPCertificateInd de la couche de distribution de signal ++ (SDL) fournit des détails au sujet de NC de sujet et d'informations de connexion.

```
04530218.000 |19:59:21.323 |SdlSig   |SIPCertificateInd                    |wait
                  |SIPHandler(1,100,72,1)           |SIPTcp(1,100,64,1)
|1,100,17,11.3^*^*                       |[T:N-H:0,N:1,L:0,V:0,Z:0,D:0] connIdx= 12 --
remoteIP=10.106.95.200 --remotePort = 5061 --X509SubjectName
/C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --SubjectAltname =
04530219.000 |19:59:21.324 |SdlSig   |SIPCertificateInd
|restart0                       |SIPD(1,100,74,16)
|SIPHandler(1,100,72,1)           |1,100,17,11.3^*^*                       |[R:N-
H:0,N:0,L:0,V:0,Z:0,D:0] connIdx= 12 --remoteIP=10.106.95.200 --remotePort = 5061 --
X509SubjectName /C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --
SubjectAltname =
```