Comment corriger un certificat intermédiaire Verisign expiré sur CSS 11500

Contenu

Introduction

Verisign a signalé un avis qui a indiqué que la racine intermédiaire CA d'ID global de serveur de Verisign a expiré sur 1/7/2004. Le pour en savoir plus, se rapportent au Soutien technique de Verisign .

Le but de ce document est d'expliquer comment remplacer un certificat qui existe déjà sur votre commutateur 11500 de service de contenu de Cisco avec un certificat concaténé qui contient le certificat de CA intermédiaire de racine de nouvel de Verisign ID global de serveur.

Pour plus d'informations sur l'installation de certificat, référez-vous à comment installer un certificat ssl enchaîné sur le module SSL CSS.

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 :

- Commutateur 11500 de service de contenu de Cisco avec le Protocole SSL (Secure Socket Layer) - module

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 de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

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

Remarque: Pour obtenir plus d'informations sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés uniquement).

Configurations

Ce document utilise les configurations suivantes :

- Certificat existant d'exportation
- Obtenez le certificat intermédiaire de Verisign
- Fichier du certificat enchaîné d'importation
- Associez le fichier du certificat
- Interrompez les services
- Configurez la liste de proxy SSL
- Lancez les services
- Service et règles de contenu SSL

Certificat existant d'exportation

Si vous avez déjà une sauvegarde de votre certificat disponible, vous pouvez passer à l'étape suivante, « obtenez le certificat intermédiaire de Verisign ». Si vous n'avez pas une sauvegarde, vous êtes requis d'exporter votre certificat du commutateur de service de contenu de Cisco. Émettez la commande de **password> <quoted par name> de <cert d'exportation de record> de <ftp de FTP SSL de copie** d'exporter le certificat qui existe déjà sur le commutateur de service de contenu de Cisco. Exemple : `CSS11503(config)# **copy ssl ftp ssl_record export servercert.pem "password"** Connecting (/) Completed successfully.` Les commandes copy d'**exportation de FTP SSL de copie le** certificat à un ftp server. Le format du certificat semble semblable à ceci :
`-----BEGIN CERTIFICATE -----`
`BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5j`
`LjESMBAG`
`Binary data of your server certificate`
`BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5j`
`LjESMBAG`

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

Obtenez le certificat intermédiaire de Verisign

Si vous avez un certificat intermédiaire expiré, vous pouvez obtenir le certificat intermédiaire de Verisign de ce lien :

- Installer le certificat de CA intermédiaire

Sauvegardez le certificat intermédiaire à un fichier. Par exemple — intermediate.pem. Afin d'utiliser les Certificats enchaînés sur le commutateur de service de contenu de Cisco, le certificat de serveur et l'intermédiaire doivent être concaténés ensemble. Ceci permet au commutateur de service de contenu de Cisco pour renvoyer la chaîne de certificat entière au client sur la prise de contact SSL d'initiale. Quand le fichier du certificat enchaîné est créé pour le commutateur de service de contenu de Cisco, assurez-vous que les Certificats sont dans la commande appropriée. Le certificat de serveur doit être premier, puis le certificat intermédiaire est utilisé pour signer le certificat de serveur doit être prochain. Le format des modules d'entrée d'alimentation (PEM) n'est pas très strict, et les lignes vides entre les clés ou les Certificats n'importent pas. Le contenu entier du fichier mychainedrsacert.pem est affiché ici :

```
-----BEGIN CERTIFICATE -----
BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5j
LjESMBAG
Binary data of your server certificate
BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5j
LjESMBAG
-----END CERTIFICATE-----
```

Le certificat Verisign est affiché ici :

```
-----BEGIN CERTIFICATE-----
MIIDgzCCAuygAwIBAgIQJUuKhThCzONY+MXdriJupDANBgkqhkiG9w0B
AQUFADBf
MQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xNzA1
BgNVBAsT
LkNsYXNzIDMgUHVibGljIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdHkw
HhcNOTcwNDE3MDAwMDAwWhcNMTExMDI0MjM1OTU5WjCBujEfMB0GA1UE
ChMWVmVy
aVNpZ24gVHJ1c3QgTmV0d29yazEXMBUGA1UECxMOVmVyaVNpZ24sIElu
Yy4xMzAx
BgNVBAsTKlZlcmlTaWduIEludGVybmF0aW9uYWwgU2VydmVyIENBIC0g
Q2xhc3Mg
MzFJMEcGA1UECxNAd3d3LnZlcmlzaWduLmNvbS9DUFMgSW5jb3JwLmJ5
IFJlZi4g
TElBQklMSVRZIExURC4oYyk5NyBWZXJpU2lnbjCBnzANBgkqhkiG9w0B
AQEFAAOB
jQAwgYkCgYEA2IKA6NYZAn0fhRg5JaJlK+G/1AXTvOY2O6rwTGxbtueq
PHNFVbLx
veqXQu2aNAoV1Klc9UAl3dkHwTKydWzEyruj/lYncUOqY/UwPpMo5frx
CTvzt01O
OfdcSVq4wR3Tsor+cDCVQsv+K1GLWjw6+SJPkLICp1OcTzTnqwSye28C
AwEAAaOB
4zCB4DAPBgNVHRMECDAGAQH/AgEAMEQGA1UdIAQ9MDswOQYLYIZIAYb4
RQEHAQEw
```

```
KjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL0NQ
UzA0BgNV
HSUELTArBggrBgEFBQcDAQYIKwYBBQUHAwIGCWCGSAGG+EIEAQYKYIZI
AYb4RQEI
ATALBgNVHQ8EBAMCAQYwEQYJYIZIAYb4QgEBBAQDAgEGMDEGA1UdHwQq
MCgwJqAk
oCKGIGh0dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTMuY3JsMA0GCSqG
SIb3DQEB
BQUAA4GBAAgB7ORolANC8XPxI6I63unx2sZUxCM+hurPajozq+qcBBQH
NgYL+Yhv
1RPuKSvD5HKNRO3RrCAJLeH24RkFOLA9D59/+J4C3IYChmFOJl9en5Ie
DCSk9dBw
E88mw0M9SR2egi5SX7w+xmYpAY5Okiy8RnUDgqxz6dl+C2fvVFIa
-----END CERTIFICATE-----
```

Fichier du certificat enchaîné d'importation

Le fichier du certificat doit être importé au commutateur de service de contenu de Cisco. Émettez la commande **SSL de copie** de faciliter l'importation ou l'exportation des Certificats et des clés privées ou derrière le commutateur de service de contenu de Cisco. Le commutateur de service de contenu de Cisco enregistre tous les fichiers importés dans un emplacement sécurisé sur le commutateur de service de contenu de Cisco. Cette commande est disponible seulement dans le mode de super utilisateur. Par exemple, pour importer le certificat mychainedrsacert.pem d'un serveur distant au commutateur de service de contenu de Cisco, émettez cette commande :

```
CSS11500# copy ssl sftp ssl_record import
mychainedrsacert.pem PEM "passwd123" Connecting
Completed successfully
```

Associez le fichier du certificat

Émettez la commande de **CERT d'associé SSL** d'associer un nom de certificat au certificat importé. Par exemple, pour associer le nom mychainedrsacert1 de certificat au fichier du certificat importé mychainedrsacert.pem, émettez cette commande :

```
CSS11500(config)#ssl associate cert mychainedrsacert1
mychainedrsacert.pem
```

Si vous recevez un message d'erreur qui indique « le nom d'association en double de %% », alors choisissez un nom d'association différent.

Interrompez les services

Afin de modifier une liste de proxy SSL, vous devez interrompre tous les services SSL qui mettent en référence la liste de proxy SSL. Par exemple, ce service doit être interrompu afin de modifier la liste **ssl_list1 de** proxy :

```
service ssl_serv1
     type ssl-accel
     slot 2
     keepalive type none
     add ssl-proxy-list ssl_list1
     active

CSS11500(config)# service ssl_serv1 CSS11500(config-
```

```
service[ssl_serv1])# suspend
```

Configurez la liste de proxy SSL

Émettez la commande de SSL-proxy-**liste** de modifier une liste de proxy SSL. Une liste de proxy SSL est un groupe de serveurs virtuels ou principaux relatifs SSL qui sont associés avec un service SSL. La liste de proxy SSL contient toutes les informations de configuration pour chaque serveur virtuel SSL. Ceci inclut la création de serveur SSL, paire de clés SSL de Certificats et de correspondance, adresse virtuelle et port IP (VIP), chiffrements SSL pris en charge, et d'autres options SSL. Par exemple, pour modifier la SSL-proxy-liste ssl_list1, émettez cette commande : `CSS11500(config)# **ssl-proxy-list ssl_list1**` Une fois que vous entamez le mode de configuration de SSL-proxy-liste, vous le premier besoin d'interrompre la liste de proxy SSL, puis spécifiez l'association de certificat. Exemple :

```
CSS11500(ssl-proxy-list[ssl_list1])# suspend
CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20
rsacert mychainedrsacert1 CSS11500(ssl-proxy-
list[ssl_list1])# active
```

Lancez les services

Une fois que la liste de proxy SSL a été modifiée et lancée, vous devez lancer tous les services qui mettent en référence la liste de proxy SSL. Par exemple, ce service doit être lancé afin d'utiliser la liste **ssl_list1 de** proxy :

```
service ssl_serv1
     type ssl-accel
     slot 2
     keepalive type none
     add ssl-proxy-list ssl_list1

CSS11500(config)# service ssl_serv1 CSS11500(config-
service[ssl_serv1])# active
```

Service et règles de contenu SSL

En ce moment, le trafic du client HTTPS peut être envoyé au commutateur de service de contenu de Cisco à 192.168.3.6:443. Le commutateur de service de contenu de Cisco déchiffre le trafic HTTPS pour le convertir en HTTP. Le commutateur de service de contenu de Cisco alors choisit un service et envoie le trafic http à un serveur Web de HTTP. C'est une configuration active de commutateur de service de contenu de Cisco qui utilise les exemples mentionnés dans ce document :

```
CSS11501# show run configure
!************************** GLOBAL
************************** ssl associate rsakey
myrsakey1 myrsakey.pem ssl associate cert
mychainedrsacert1 mychainedrsacert.pem ip route 0.0.0.0
0.0.0.0 192.168.3.1 1 ftp-record ssl_record
192.168.11.101 admin des-password 4f2bxansrcehjgka
/tftpboot !************************ INTERFACE
************************ interface 1/1 bridge vlan 10
description "Client Side" interface ½ bridge vlan 20
```

```
description "Server Side" !************************
CIRCUIT ************************* circuit VLAN10
description "Client Segment" ip address 192.168.3.254
255.255.255.0 circuit VLAN20 description "Server
Segment" ip address 192.168.11.1 255.255.255.0
!********************** SSL PROXY LIST
********************** ssl-proxy-list ssl_list1 ssl-
server 20 ssl-server 20 vip address 192.168.3.6 ssl-
server 20 rsakey myrsakey1 ssl-server 20 rsacert
mychainedrsacert1 ssl-server 20 cipher rsa-with-rc4-128-
md5 192.168.11.2 80 active !*************************
SERVICE ************************* service linux-http ip
address 192.168.11.101 port 80 active service win2k-http
ip address 192.168.11.102 port 80 active service
ssl_serv1 type ssl-accel slot 2 keepalive type none add
ssl-proxy-list ssl_list1 active
!************************** OWNER
************************** owner ssl_owner content
ssl_rule1 vip address 192.168.3.6 protocol tcp port 443
add service ssl_serv1 active content decrypted_www vip
address 192.168.11.2 add service linux-http add service
win2k-http protocol tcp port 80 active
```

Vérifiez

Une fois le nouveau certificat est installé, utilise un navigateur pour se connecter au serveur Web sécurisé afin de s'assurer qu'il n'y a aucune alerte présentée.

Dépannez

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

Informations connexes

- Support matériel pour les commutateurs de services de contenu de la gamme CSS 11500
- Support matériel de Commutateurs de services satisfaits de gamme 11000 CSS
- Téléchargement logiciel de Cisco WebNS CSS11500 (clients enregistrés seulement)
- Téléchargement logiciel de Cisco WebNS CSS11000 (clients enregistrés seulement)
- Support et documentation techniques - Cisco Systems