CSS 11500 での期限切れ Verisign 中間証明書の修正方法

目次

概要

Verisign は、VeriSign のグローバル サーバ ID の Intermediate Root CA が 2004 年 7 月 1 日で期限切れになったことを示す通知を公開しています。 詳細は、『VeriSign Technical Support』 を参照してください。

このドキュメントは、すでに Cisco コンテンツ サービス スイッチ 11500 上に存在する証明書を、新たな Verisign グローバル サーバ ID 中間ルート CA 証明書を含む、連結された証明書で置き換える方法の説明を目的としています。

証明書インストールの詳細は、『チェーン SSL 証明書の CSS SSL モジュールへのインストール方法』を参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco コンテンツ サービス スイッチ 11500（Secure Socket Layer（SSL）モジュール搭載）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始して

います。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

設定

このドキュメントでは、次の設定を使用します。

- 既存の証明書のエクスポート
- Verisign 中間証明書の取得
- チェーン証明書ファイルのインポート
- 証明書ファイルの関連付け
- サービスの一時停止
- SSL プロキシ リストの設定
- サービスのアクティブ化
- SSL サービスおよびコンテンツ ルール

既存の証明書のエクスポート

利用可能な証明書のバックアップをすでに取得している場合は、次の手順「Verisign 中間証明書の取得」に進みます。 バックアップを取得していない場合は、Cisco コンテンツ サービス スイッチから証明書をエクスポートする必要があります。 **copy ssl ftp <ftp record> export <cert name> <quoted password>** コマンドを発行し、すでに Cisco コンテンツ サービス スイッチに存在する証明書をエクスポートします。 次に、例を示します。
`CSS11503(config)# copy ssl ftp ssl_record export servercert.pem "password" Connecting (/) Completed successfully.` **copy ssl ftp export** コマンドは、証明書を FTP サーバにコピーします。 証明書の形式は、次のようになります。
`-----BEGIN CERTIFICATE -----`
`BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5j`
`LjESMBAG`
`Binary data of your server certificate`
`BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5j`
`LjESMBAG`
`-----END CERTIFICATE-----`

Verisign 中間証明書の取得
期限切れの中間証明書を保持している場合、次のリンクから VeriSign 中間証明書を取得できます。

- 中間 CA 証明書のインストール

中間証明書をファイルに保存します（例：intermediate.pem）。 Cisco コンテンツ サービス スイッチ上でチェーン証明書を使用するには、サーバ証明書と中間証明書を連結する必要があります。 これにより、Cisco コンテンツ サービス スイッチは、最初の SSL ハンドシェイクにおいて、クライアントに完全な証明書チェーンを返すことができます。 チェーン証明書ファイルが Cisco コンテンツ サービス スイッチ用に作成されたら、証明書が正しい順に配置されていることを確認してください。 最初にサーバ証明書が配置される必要があり、サーバ証明書の署名に使用される中間証明書はその次に配置される必要があります。 Power Entry Module（PEM）の形式はあまり厳密ではありません。キーまたは証明書の間の空行は無視されます。

mychainedrsacert.pem ファイルの内容全体は次のとおりです。

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

Verisign 証明書は次のとおりです。

```
-----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-----
```

チェーン証明書ファイルのインポート

証明書ファイルを Cisco コンテンツ サービス スイッチにインポートする必要があります。 **copy ssl** コマンドを発行して、Cisco コンテンツ サービス スイッチからの証明書および秘密鍵のインポート、または Cisco コンテンツ サービス スイッチへの証明書および秘密鍵のエクスポートを実行します。 Cisco コンテンツ サービス スイッチは、インポートされたすべてのファイルを Cisco コンテンツ サービス スイッチ上の安全な場所に保存します。 このコマンドは、SuperUser モードに限り使用できます。 たとえば、mychainedrsacert.pem 証明書をリモート サーバから Cisco コンテンツ サービス スイッチにインポートするには、次のコマンドを発行します。

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

証明書ファイルの関連付け

ssl associate cert コマンドを発行して、証明書名をインポートされた証明書に関連付けます。 たとえば、証明書名 mychainedrsacert1 をインポートされた証明書ファイル mychainedrsacert.pem に関連付けるには、次のコマンドを発行します。

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

「%% Duplicate association name」というエラー メッセージを受信した場合は、別の証明書名を関連付けてください。

サービスの一時停止

SSL プロキシ リストを変更するには、SSL プロキシ リストを参照するすべての SSL サービスを一時停止する必要があります。 たとえば、プロキシ リスト **ssl_list1** を変更するには、次のサービスを一時停止する必要があります。

```
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
```

SSL プロキシ リストの設定

SSL プロキシ リストを変更するには、**ssl-proxy-list** コマンドを発行します。 SSL プロキシ リストは、SSL サービスに関連付けられている、関連する仮想 SSL サーバまたはバックエンド SSL サーバのグループです。 SSL プロキシ リストには、各仮想 SSL サーバに関するすべて

の設定情報が含まれます。 この情報には、SSL サーバの作成、証明書および対応する SSL キー ペア、仮想 IP (VIP) アドレスおよびポート、サポートされている SSL 暗号化、および他の SSL オプションが含まれます。 たとえば、SSL プロキシ リスト ssl_list1 を変更するには、次のコマンドを発行します。 CSS11500(config)# **ssl-proxy-list ssl_list1** ssl-proxy-list コンフィギュレーション モードに入ったら、最初に SSL プロキシ リストを一時停止し、次に証明書アソシエーションを指定する必要があります。 次に、例を示します。

```
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
```

サービスのアクティブ化

SSL プロキシ リストが変更およびアクティブ化されたら、SSL プロキシ リストを参照するすべてのサービスをアクティブ化する必要があります。 たとえば、プロキシ リスト **ssl_list1** を使用するには、次のサービスをアクティブ化する必要があります。

```
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
```

SSL サービスおよびコンテンツ ルール

この時点で、クライアントの HTTPS トラフィックを 192.168.3.6:443 に存在する Cisco コンテンツ サービス スイッチに送信できます。 Cisco コンテンツ サービス スイッチは HTTPS トラフィックを復号化し、HTTP に変換します。 次に、Cisco コンテンツ サービス スイッチはサービスを選択し、HTTP トラフィックを HTTP Web サーバに送信します。 次に、このドキュメントで説明した例を使用した、アクティブな Cisco コンテンツ サービス スイッチ設定を示します。

```
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
```

確認

新たな証明書がインストールされたら、ブラウザを使用してセキュアな Web サイトに接続し、アラートが表示されないことを確認します。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- CSS 11500
- CSS 11000 シリーズ コンテント サービス スイッチのハードウェア サポート (英語)
- Cisco WebNS CSS11500 ソフトウェアのダウンロード (登録ユーザ専用)
- Cisco WebNS CSS11000 ソフトウェアのダウンロード (登録ユーザ専用)
- テクニカルサポートとドキュメント - Cisco Systems