如何修正在CSS11500的一过期的Verisign中间证书

目录

简介

Verisign张贴了表明的公告Verisign全局服务器ID半成品根CA在1/7/2004超时。欲知更多信息，参考Verisign技术支持 。

本文目的将解释如何替换在您的有一被连接的证书的Cisco内容服务交换机11500已经存在包含新的Verisign全局服务器ID中间根CA证书的证书。

关于认证安装的更多信息，参考如何安装一被串连的SSL证书到CSS SSL模块。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 有安全套接字层SSL的Cisco内容服务交换机11500 -模块

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 要查找有关本文档中所使用的命令的详细信息，请使用命令查找工具（仅限注册用户）。

配置

本文档使用以下配置：

- 出口现有的证书
- 获取Verisign中间证书
- 导入证书文件
- 关联证书文件
- 暂停服务
- 配置SSL代理列表
- 启动服务
- SSL服务和内容规则

出口现有的证书

如果已经有您可用的证书备份，您能继续前进向下一步，“获取Verisign中间证书”。如果没有一个备份，您要求导出您的从Cisco内容服务交换机的证书。发出**copy ssl ftp <ftp record> export <cert name> <quoted password>命令**导出在Cisco内容服务交换机已经存在的证书。例如：

```
CSS11503(config)# copy ssl ftp ssl_record export servercert.pem "password" Connecting (/) Completed successfully.
```

copy ssl ftp export命令复制证书对FTP服务器。证书的格式看起来类似于此：

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

获取Verisign中间证书

如果有一已到期中间证书，您能从此链路获取Verisign的中间证书：

- 安装半成品CA证书

保存中间证书到文件。例如— intermediate.pem。为了使用在Cisco内容服务交换机的被串连的证书，必须同时连接服务器证书和中间。这允许Cisco内容服务交换机返回整个证书链对客户端在初始SSL握手。当证书文件为Cisco内容服务交换机时创建，请确保证书按适当的顺序。服务器证书必须是第一，然后中间证书用于签署服务器证书一定是下的。电源入口模块(PEM)格式不严格，并且在密钥或证书之间的空线路不重要。mychainedrsacert.pem文件的整个内容显示此处：

```
-----BEGIN CERTIFICATE -----
```

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

Verisign认证显示此处：

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

导入证书文件

必须导入证书文件到Cisco内容服务交换机。发出**copy ssl命令**实现证书和专用密钥的导入或出口从或对Cisco内容服务交换机。Cisco内容服务交换机在Cisco内容服务交换机的一个安全位置存储所有导入的文件。此指令仅可用的在超级用户模式。例如，导入从远程服务器的mychainedrsacert.pem证书到Cisco内容服务交换机，请发出此命令：

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

关联证书文件

发出**ssl associate cert命令**关联验证名称到已导入证书。例如，关联验证名称mychainedrsacert1到已导入证书文件mychainedrsacert.pem，请发出此命令：

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

如果收到指示'%%'错误消息，则请选择一个不同的关联名字。

暂停服务

为了修改SSL代理列表，您必须暂停参考SSL代理列表的所有SSL服务。例如，此服务需要被暂停为了修改代理列表**ssl_list1** ：

```
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
```

配置SSL代理列表

发出**ssl-proxy-list命令**修改SSL代理列表。SSL代理列表是关联与SSL服务相关虚拟或后端SSL服务器的一组。SSL代理列表包含每台虚拟SSL服务器的所有配置信息。这包括SSL服务器创建、证书和对应SSL密钥对、Virtual IP (VIP)地址和端口、SSL密码器支持的和其他SSL选项。例如，修改ssl代理列表ssl_list1，请发出此命令：

```
CSS11500(config)# ssl-proxy-list ssl_list1
```

一旦输入到ssl代理列表配置模式，您首先需要暂停SSL代理列表，然后指定证书关联。例如：

```
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
```

启动服务

一旦修改了SSL代理列表并且激活，您需要启动参考SSL代理列表的所有服务。例如，此服务需要被启动为了使用代理列表**ssl_list1** ：

```
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服务和内容规则

这时，客户端HTTPS流量可以发送到在192.168.3.6:443的Cisco内容服务交换机。Cisco内容服务交换机解密HTTPS流量转换它到HTTP。Cisco内容服务交换机然后选择服务并且发送HTTP数据流到HTTP Web服务器。这是在本文使用被提及的示例的一活动Cisco内容服务交换机配置：

```
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
```

验证

一旦新证书安装，请使用一个浏览器连接到安全网站为了保证那里是没有被提交的警报。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- CSS 11500系列内容服务交换机硬件支持
- CSS 11000系列内容服务交换机硬件支持
- Cisco WebNS CSS11500软件下载(仅限注册用户)
- Cisco WebNS CSS 11000软件下载(仅限注册用户)
- 技术支持和文档 - Cisco Systems