Como fixar um certificado intermediário expirado de Verisign no CSS11500

Índice

Introdução

Verisign afixou uma observação que indicasse que a CA de raiz intermediária do ID de servidor global VeriSign expirou em 1/7/2004. Para mais informação, refira o Suporte técnico de Verisign .

A finalidade deste documento é explicar como substituir um certificado que já exista em seu Cisco Content Service Switch 11500 com um certificado concatenado que contenha o certificado novo da CA de raiz intermediária do ID de servidor global VeriSign.

Para obter mais informações sobre da instalação certificada, refira como instalar um certificado acorrentado SSL ao módulo de CSS SSL.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Content Service Switch 11500 com Secure Socket Layer (SSL) - módulo

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto

potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Para encontrar informações adicionais sobre os comandos usados neste documento, use a Command Lookup Tool (somente clientes registrados).

Configurações

Este documento utiliza as seguintes configurações:

- Certificado existente da exportação
- Obtenha o certificado do intermediário de Verisign
- Importe o arquivo certificado acorrentado
- Associe o arquivo certificado
- Suspenda serviços
- Configurar a lista do proxy SSL
- Ative serviços
- Serviço e regras de conteúdo SSL

Certificado existente da exportação

Se você já tem um backup de seu certificado disponível, você pode transportar-se sobre à próxima etapa, “obtém o certificado intermediário de Verisign”. Se você não tem um backup, você está exigido exportar seu certificado do Cisco Content Service Switch. Emita o **comando copy ssl ftp <ftp record> export <cert name> <quoted password>** exportar o certificado que já existe no Cisco Content Service Switch. Por exemplo:
`CSS11503(config)# copy ssl ftp ssl_record export servercert.pem "password" Connecting (/) Completed successfully.` **O comando copy ssl ftp export** copia o certificado a um servidor FTP. O formato do certificado olha similar a este:
`-----BEGIN CERTIFICATE -----`
`BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5j`
`LjESMBAG`
`Binary data of your server certificate`
`BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5j`
`LjESMBAG`
`-----END CERTIFICATE-----`

Obtenha o certificado do intermediário de Verisign
Se você tem um certificado intermediário expirado, você

pode obter o certificado intermediário de Verisign deste link:

- Instalando o certificado de CA intermediário

Salvar o certificado intermediário a um arquivo. Por exemplo — intermediate.pem. A fim usar os Certificados acorrentados no Cisco Content Service Switch, o certificado de servidor e o intermediário devem ser concatenados junto. Isto permite que o Cisco Content Service Switch retorne o certificate chain inteiro ao cliente em cima da saudação de SSL inicial. Quando o arquivo certificado acorrentado é criado para o Cisco Content Service Switch, certifique-se que os Certificados estão na ordem apropriada. O certificado de servidor deve ser primeiro, a seguir o certificado intermediário é usado para assinar o certificado de servidor deve ser seguinte. O formato dos módulos de entrada de alimentação (PEM) não é muito restrito, e as linhas vazias entre chaves ou Certificados não importam. Os índices inteiros do arquivo mychainedrsacert.pem são mostrados aqui:

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

O certificado Verisign é mostrado aqui:

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

Arquivo certificado acorrentado da importação

O arquivo certificado deve ser importado ao Cisco Content Service Switch. Emita o **comando copy ssl** facilitar a importação ou a exportação dos Certificados e das chaves privadas ou ao Cisco Content Service Switch. O Cisco Content Service Switch armazena todos os arquivos importados em um lugar seguro no Cisco Content Service Switch. Este comando está disponível somente no modo super usuário. Por exemplo, para importar o certificado mychainedrsacert.pem de um servidor remoto ao Cisco Content Service Switch, emita este comando:

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

Associe o arquivo certificado

Emita o **comando ssl associate cert** associar um nome do certificado ao certificado importado. Por exemplo, para associar o nome mychainedrsacert1 do certificado ao arquivo certificado importado mychainedrsacert.pem, emita este comando:

`CSS11500(config)#ssl associate cert mychainedrsacert1 mychainedrsacert.pem` Se você recebe um Mensagem de Erro que indique de "`o nome de associação duplicado %%`", a seguir escolha um nome de associação diferente.

Suspenda serviços

A fim alterar uma lista do proxy SSL, você deve suspender todos os serviços SSL que proveem a lista do proxy SSL. Por exemplo, este serviço precisa de ser suspendido a fim alterar a lista **ssl_list1 do** 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
```

Configurar a lista do proxy SSL

Emita o **comando ssl-proxy-list** alterar uma lista do proxy SSL. Uma lista do proxy SSL é um grupo de servidores SSL virtuais ou backend relacionados que são associados com um serviço SSL. A lista do proxy SSL

contém toda a informação de configuração para cada servidor SSL virtual. Isto inclui a criação de servidor SSL, o par de chaves SSL dos Certificados e da correspondência, o endereço e a porta do IP virtual (VIP), as cifras SSL apoiadas, e as outras opções de SSL. Por exemplo, para alterar a lista de proxy ssl ssl_list1, emita este comando: `CSS11500(config)# **ssl-proxy-list ssl_list1**` Uma vez que você incorpora na lista de proxy ssl o modo de configuração, você primeiramente precisa de suspender a lista do proxy SSL, a seguir especifica a associação do certificado. Por exemplo:

```
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
```

Ative serviços

Uma vez que a lista do proxy SSL foi alterada e ativada, você precisa de ativar todos os serviços que proveem a lista do proxy SSL. Por exemplo, este serviço precisa de ser ativado a fim usar a lista **ssl_list1 do** 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
```

Serviço e regras de conteúdo SSL

Neste momento, o tráfego do cliente HTTPS pode ser enviado ao Cisco Content Service Switch em 192.168.3.6:443. O Cisco Content Service Switch decifra o tráfego HTTPS para convertê-lo ao HTTP. O Cisco Content Service Switch então escolhe um serviço e envia o tráfego de HTTP a um servidor de Web HTTP. Esta é uma configuração ativa do Cisco Content Service Switch que use os exemplos mencionados neste documento:

```
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
```

Verificar

Uma vez que o certificado novo é instalado, use um navegador para conectar ao site seguro a fim assegurar-se de que não haja nenhum alerta apresentado.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Suporte a hardware dos CSS 11500 Series Content Services Switch
- Suporte a hardware dos CSS 11000 Series Content Services Switch
- Download do software de Cisco WebNS CSS11500 (clientes registrados somente)
- Download do software de Cisco WebNS CSS11000 (clientes registrados somente)
- Suporte Técnico e Documentação - Cisco Systems