Cómo reparar un certificado intermedio expirado de Verisign en el CSS11500

Contenido

Introducción

Verisign fijó un aviso que indicó que intermedia del ID del Servidor global de VeriSign raíz CA expirado en 1/7/2004. Para más información, refiera al Soporte técnico de Verisign .

El propósito de este documento es explicar cómo substituir un certificado que exista ya en su switch de servicio de contenido de Cisco 11500 con un certificado concatenado que contenga el nuevo intermedia del ID del Servidor global de VeriSign certificado raíz CA.

Para más información sobre la instalación del certificado, refiérase a cómo instalar un certificado encadenado SSL al módulo CSS SSL.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Switch de servicio de contenido de Cisco 11500 con el Secure Socket Layer (SSL) - módulo

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para encontrar la información adicional en los comandos usados en este documento, use la Command Lookup Tool (clientes registrados solamente).

Configuraciones

En este documento, se utilizan estas configuraciones:

- Certificado existente de la exportación
- Obtenga el certificado del intermedio de Verisign
- Importe el archivo de certificado encadenado
- Asocie el archivo de certificado
- Suspenda los servicios
- Configure la lista del proxy SSL
- Active los servicios
- Servicio y reglas de contenido SSL

Certificado existente de la exportación

Si usted tiene ya un respaldo de su certificado disponible, usted puede trasladarse encendido al siguiente paso, “obtiene el certificado intermedio de Verisign”. Si usted no tiene un respaldo, le requieren exportar su certificado del switch de servicio de contenido de Cisco. Publique el **comando copy ssl ftp <ftp record> export <cert name> <quoted password>** de exportar el certificado que existe ya en el switch de servicio de contenido de Cisco. Por ejemplo:
`CSS11503(config)# copy ssl ftp ssl_record export servercert.pem "password" Connecting (/) Completed successfully.` **El comando copy ssl ftp export** copia el certificado a un servidor FTP. El formato del certificado parece similar a esto:
`-----BEGIN CERTIFICATE -----`
`BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5j`
`LjESMBAG`
`Binary data of your server certificate`
`BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5j`
`LjESMBAG`
`-----END CERTIFICATE-----`

Obtenga el certificado del intermedio de Verisign

Si usted tiene un certificado intermedio expirado, usted puede obtener el certificado intermedio de Verisign de este link:

- Instalar el certificado de CA intermedio

Salve el certificado intermedio a un archivo. Por ejemplo — intermediate.pem. Para utilizar los Certificados encadenados en el switch de servicio de contenido de Cisco, el certificado de servidor y el intermedio se deben concatenar juntos. Esto permite que el switch de servicio de contenido de Cisco vuelva la Cadena de certificados entera al cliente sobre el contacto SSL inicial. Cuando el archivo de certificado encadenado se crea para el switch de servicio de contenido de Cisco, aseegurese los Certificados están en la orden apropiada. El certificado de servidor debe ser primer, después el certificado intermedio se utiliza para firmar el certificado de servidor debe ser siguiente. El formato de los módulos de entrada de energía (PEM) no es muy estricto, y las líneas vacías entre las claves o los Certificados no importan. El contenido entero del archivo del mychainedrsacert.pem se muestra aquí:

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

El certificado de Verisign se muestra aquí:

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

Archivo de certificado encadenado de la importación

El archivo de certificado se debe importar al switch de servicio de contenido de Cisco. Publique el **comando copy ssl** de facilitar la importación o la exportación de los Certificados y de las claves privadas o al switch de servicio de contenido de Cisco. El switch de servicio de contenido de Cisco salva todos los archivos importados en una ubicación segura en el switch de servicio de contenido de Cisco. Este comando está disponible solamente en el modo de superusuario. Por ejemplo, para importar el certificado del mychainedrsacert.pem de un servidor remoto al switch de servicio de contenido de Cisco, publique este comando:

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

Asocie el archivo de certificado

Publique el **comando ssl associate cert** de asociar un nombre del certificado al certificado importado. Por ejemplo, para asociar el nombre mychainedrsacert1 del certificado al mychainedrsacert.pem importado del archivo de certificado, publique este comando:

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

Si usted recibe un mensaje de error que indique el `"nombre de asociación duplicado del %%"`, después elija un diverso nombre de asociación.

Suspenda los servicios

Para modificar una lista del proxy SSL, usted debe suspender todos los servicios SSL que se refieran a la lista del proxy SSL. Por ejemplo, este servicio necesita ser suspendido para modificar la lista **ssl_list1 del** 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
```

Configure la lista del proxy SSL

Publique el **comando ssl-proxy-list** de modificar una lista del proxy SSL. Una lista del proxy SSL es un grupo de

servidores SSL virtuales o backend relacionados que se asocien a un servicio SSL. La lista del proxy SSL contiene toda la información de la configuración para cada servidor SSL virtual. Esto incluye el par clave SSL de la creación de servidor SSL, de los Certificados y de la correspondencia, IP virtual el direccionamiento (VIP) y puerto, las cifras SSL soportadas, y otras opciones de SSL. Por ejemplo, para modificar la lista SSL del proxy ssl_list1, publique este comando: `CSS11500(config)# **ssl-proxy-list ssl_list1**` Una vez que usted ingresa en la lista SSL del proxy al modo de configuración, usted primero necesita suspender la lista del proxy SSL, después especifica la asociación del certificado. Por ejemplo:

```
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
```

Active los servicios

Una vez que se ha modificado y se ha activado la lista del proxy SSL, usted necesita activar todos los servicios que se refieran a la lista del proxy SSL. Por ejemplo, este servicio necesita ser activado para utilizar la lista **ssl_list1 del** 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
```

Servicio y reglas de contenido SSL

En este momento, el tráfico del cliente HTTPS se puede enviar al switch de servicio de contenido de Cisco en 192.168.3.6:443. El switch de servicio de contenido de Cisco desencripta el tráfico HTTPS para convertirlo al HTTP. El switch de servicio de contenido de Cisco después elige un servicio y envía el tráfico HTTP a un servidor Web HTTP. Ésta es una configuración activa del switch de servicio de contenido de Cisco que utiliza los ejemplos mencionados en este 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
```

Verificación

Una vez que el nuevo certificado está instalado, utilice a un navegador para conectar con el sitio web seguro para asegurarse que no hay alertas presentadas.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Soporte del hardware de los CSS 11500 Series Content Services Switch
- Soporte del hardware de los CSS 11000 Series Content Services Switch
- Descarga del software de Cisco WebNS CSS11500 (clientes registrados solamente)
- Descarga del software de Cisco WebNS CSS11000 (clientes registrados solamente)
- Soporte Técnico y Documentación - Cisco Systems