Исправление промежуточного сертификата Verisign с истекшим сроком действия на CSS 11500

Содержание

Введение

VeriSign зарегистрировал предупреждение, которое указало, что Узел CA промежуточного глобального идентификатора сервера VeriSign истек 07.01.2004. Для получения дополнительной информации обратитесь к Технической поддержке VeriSign.

Цель этого документа состоит в том, чтобы объяснить, как заменить сертификат, который уже существует на вашем коммутаторе Cisco Content Service 11500 со связанным сертификатом, который содержит новый Корневой сертификат CA промежуточного глобального идентификатора сервера VeriSign.

Для получения дополнительной информации об установке сертификатов обратитесь к тому, Как Установить Цепочечный сертификат SSL к Модулю CSS SSL.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Коммутатор Cisco Content Service 11500 с протоколом SSL - модуль

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Дополнительные сведения о командах, использованных в данном документе, см. в разделе Средство поиска команд (только для зарегистрированных клиентов).

Конфигурации

Эти конфигурации используются в данном документе:

- Существующий сертификат экспорта
- Получите промежуточный сертификат Verisign
- Импортируйте цепочечный файл сертификата
- Привяжите файл сертификата
- Suspend Services
- Настройте список SSL прокси
- Activate Services
- Сервис SSL и правила содержимого

Существующий сертификат экспорта

Если у вас уже есть резервная копия вашего доступного сертификата, можно перейти к следующему шагу, "Получите Промежуточный Сертификат Verisign". Если у вас нет резервной копии, вы обязаны экспортировать свой сертификат от коммутатора Cisco Content Service. Выполните **команду copy ssl ftp <ftp record> export <cert name> <quoted password>** для экспортирования сертификата, который уже существует на коммутаторе Cisco Content Service. Пример: `CSS11503(config)# copy ssl ftp ssl_record export servercert.pem "password" Connecting (/) Completed successfully.` **Команда copy ssl ftp export** копирует сертификат к серверу FTP. Формат сертификата выглядит подобным этому:
`-----BEGIN CERTIFICATE -----`
`BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5j`
`LjESMBAG`
`Binary data of your server certificate`

```
BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5j
LjESMBAG
-----END CERTIFICATE-----
```

Получите промежуточный сертификат Verisign

Если у вас есть промежуточный сертификат с истекшим сроком, можно получить Промежуточный Сертификат VeriSign из этой ссылки:

- Установка промежуточного сертификата CA

Сохраните промежуточный сертификат в файл. Например — intermediate.pem. Для использования цепочечных сертификатов на коммутаторе Cisco Content Service серверный сертификат и промежуточное звено должны быть связаны вместе. Это позволяет коммутатору Cisco Content Service возвращать всю цепочку сертификатов к клиенту на начальное подтверждение связи SSL. Когда цепочечный файл сертификата создан для коммутатора Cisco Content Service, удостоверьтесь, что сертификаты находятся в надлежащем заказе. Серверный сертификат должен быть первым, тогда промежуточный сертификат используется для подписания, серверный сертификат должен быть следующим. Формат модулей ввода питания (PEM) не очень строг, и пустые линии между ключами, или сертификаты не имеют значения. Все содержание файла mychainedrsacert.pem показывают здесь:

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

Сертификат Verisign показывают здесь:

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

Импортируйте цепочечный файл сертификата

Файл сертификата должен быть импортирован в коммутатор Cisco Content Service. Выполните **команду copy ssl** для упрощения импорта или экспорта сертификатов и секретных ключей от или до коммутатора Cisco Content Service. Коммутатор Cisco Content Service хранит все импортированные файлы в безопасном месте на коммутаторе Cisco Content Service. Эта команда доступна только в Режиме суперпользователя. Например, для импорта сертификата mychainedrsacert.pem от удаленного сервера до коммутатора Cisco Content Service выполните эту команду:

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

Привяжите файл сертификата

Выполните **команду ssl associate cert** для соединения названия сертификата к импортированному сертификату. Например, для соединения названия mychainedrsacert1 сертификата к импортированному mychainedrsacert.pem файла сертификата выполните эту команду:

`CSS11500(config)#`**`ssl associate cert mychainedrsacert1 mychainedrsacert.pem`** Если вы получаете сообщение об ошибках, которое указывает `'%% Duplicate association name'`, то выберите другое имя сопоставления.

Suspend Services

Для изменения Списка SSL прокси необходимо приостановить все сервисы SSL та ссылка Список SSL прокси. Например, этот сервис должен быть приостановлен для изменения прокси-листа **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
```

Настройте список SSL прокси

Выполните **команду ssl-proxy-list** для изменения Списка SSL прокси. Список SSL прокси является группой действительных связанных или SSL - серверы бэкэнда, которые привязаны к сервису SSL. Список SSL прокси содержит все сведения о конфигурации для каждого виртуального сервера SSL. Это включает создание сервера SSL, сертификаты и соответствующую пару ключей SSL, Виртуальную IP (VIP) адрес и порт, шифры SSL, поддерживаемые, и другие параметры SSL. Например, для изменения ssl-proxy-list ssl_list1 выполните эту команду: `CSS11500(config)# ssl-proxy-list ssl_list1` Как только вы вводите в режим конфигурации ssl-proxy-list, сначала необходимо приостановить Список SSL прокси, затем задать ассоциацию сертификата. Пример:

```
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
```

Activate Services

Как только Список SSL прокси модифицировался и активировался, необходимо активировать все сервисы та ссылка Список SSL прокси. Например, этот сервис должен быть активирован для использования прокси-листа **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
```

Сервис SSL и правила содержимого

На этом этапе клиентский Трафик HTTPS может быть передан коммутатору Cisco Content Service в 192.168.3.6:443. Коммутатор Cisco Content Service дешифрует Трафик HTTPS для преобразования его в HTTP. Коммутатор Cisco Content Service тогда выбирает сервис и передает трафик HTTP к Web-серверу HTTP. Это - активная конфигурация коммутатора Cisco Content Service, которая использует примеры, упомянутые в этом документе:

```
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
```

Проверка

Как только новый сертификат установлен, используйте браузер для соединения с безопасным веб-сайтом, чтобы гарантировать, что нет никаких представленных предупреждений.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Аппаратная поддержка коммутаторов контент-сервисов CSS 11500
- Аппаратная поддержка коммутаторов контент-сервисов CSS 11000
- Загрузка программного обеспечения WEBNS CSS11500 Cisco только для зарегистрированных пользователей)
- Загрузка программного обеспечения WEBNS CSS11000 Cisco (только зарегистрированные клиенты)
- Cisco Systems – техническая поддержка и документация