How to Fix an Expired Verisign Intermediate Certificate on the CSS 11500

Document ID: 47780

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Configure
Configurations
Verify
Troubleshoot
Related Information

Introduction

VeriSign posted a notice which indicated that the VeriSign Global Server ID Intermediate Root CA expired on 1/7/2004. For more information, refer to VeriSign Technical Support .

The purpose of this document is to explain how to replace a certificate that already exists on your Cisco Content Service Switch 11500 with a concatenated certificate that contains the new VeriSign Global Server ID Intermediate Root CA certificate.

For more information on certificate installation, refer to How to Install a Chained SSL Certificate to the CSS SSL Module.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Content Service Switch 11500 with Secure Socket Layer (SSL)−module

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: In order to find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Configurations

This document uses these configurations:

- Export Existing Certificate
- Obtain the Verisign Intermediate Certificate
- Import Chained Certificate File
- Associate the Certificate File
- Suspend Services
- Configure the SSL Proxy List
- Activate Services
- SSL Service and Content Rules

Export Existing Certificate

If you already have a backup of your available certificate, you can move on to the next step, "Obtain the Verisign Intermediate Certificate". If you do not have a backup, you are required to export your certificate from the Cisco Content Service Switch. Issue the **copy ssl ftp <ftp record> export <cert name> <quoted password>** command to export the certificate that already exists on the Cisco Content Service Switch. For example:

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

Connecting (/)
Completed successfully.
```

The **copy ssl ftp export** command copies the certificate to an FTP server. The format of the certificate looks similar to this:

```
-----BEGIN CERTIFICATE -----
BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESMBAG
Binary data of your server certificate
BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESMBAG
-----END CERTIFICATE-----
```

Obtain the Verisign Intermediate Certificate

If you have an expired intermediate certificate, you can obtain VeriSign's Intermediate Certificate from this link:

- Installing the Intermediate CA Certificate

Save the intermediate certificate to a file. For example intermediate.pem. In order to use the chained certificates on the Cisco Content Service Switch, the server certificate and intermediate must be concatenated together. This allows the Cisco Content Service Switch to return the entire certificate chain to the client upon the initial SSL handshake. When the chained certificate file is created for the Cisco Content Service Switch, make sure the certificates are in

the proper order. The server certificate must be first, then the intermediate certificate is used to sign the server certificate must be next. The power entry modules (PEM) format is not very strict, and the empty lines between keys or certificates do not matter. The entire contents of the mychainedrsacert.pem file are shown here:

```
-----BEGIN CERTIFICATE -----
BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESMBAG
Binary data of your server certificate
BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESMBAG
-----END CERTIFICATE-----
```

The Verisign Certificate is shown here:

```
-----BEGIN CERTIFICATE-----
MIIDgzCCAuygAwIBAgIQJUuKhThCzONY+MXdriJupDANBgkqhkiG9w0BAQUFADBf
MQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xNzA1BgNVBAsT
LkNsYXNzIDMgUHVibGljIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkw
HhcNOTcwNDE3MDAwMDAwWhcNMTExMDI0MjM1OTU5WjCBujEfMB0GA1UEChMWVmVy
aVNpZ24gVHJ1c3QgTmV0d29yazEXMBUGA1UECxMOVmVyaVNpZ24sIEluYy4xMzAx
BgNVBAsTKlZlcmlTaWduIEludGVybmF0aW9uYWwgU2VydmVyIENBIC0gQ2xhc3Mg
MzFJMEcGA1UECxNAd3d3LnZlcmlzaWduLmNvbS9DUFMgSW5jb3JwLmJ5IFJlZi4g
TElBQklMSVRZIExURC4oYyk5NyBWZXJpU2lnbjCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEA2IKA6NYZAn0fhRg5JaJlK+G/1AXTvOY2O6rwTGxbtueqPHNFVbLx
veqXQu2aNAoV1Klc9UAl3dkHwTKydWzEyruj/lYncUOqY/UwPpMo5frxCTvzt01O
OfdcSVq4wR3Tsor+cDCVQsv+K1GLWjw6+SJPkLICp1OcTzTnqwSye28CAwEAAaOB
4zCB4DAPBgNVHRMECDAGAQH/AgEAMEQGA1UdIAQ9MDswOQYLYIZIAYb4RQEHAQEw
KjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL0NQUzA0BgNV
HSUELTArBggrBgEFBQcDAQYIKwYBBQUHAwIGCWCGSAGG+EIEAQYKYIZIAYb4RQEI
ATALBgNVHQ8EBAMCAQYwEQYJYIZIAYb4QgEBBAQDAgEGMDEGA1UdHwQqMCgwJqAk
oCKGIGh0dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTMuY3JsMA0GCSqGSIb3DQEB
BQUAA4GBAAgB7ORolANC8XPxI6I63unx2sZUxCM+hurPajozq+qcBBQHNgYL+Yhv
1RPuKSvD5HKNRO3RrCAJLeH24RkFOLA9D59/+J4C3IYChmFOJl9en5IeDCSk9dBw
E88mw0M9SR2egi5SX7w+xmYpAY5Okiy8RnUDgqxz6dl+C2fvVFIa
-----END CERTIFICATE-----
```

Import Chained Certificate File

The Certificate file must be imported to the Cisco Content Service Switch. Issue the **copy ssl** command to facilitate the import or export of the certificates and private keys from or to the Cisco Content Service Switch. The Cisco Content Service Switch stores all imported files in a secure location on the Cisco Content Service Switch. This command is available only in SuperUser mode. For example, to import the mychainedrsacert.pem certificate from a remote server to the Cisco Content Service Switch, issue this command:

```
CSS11500# copy ssl sftp ssl_record import mychainedrsacert.pem PEM  passwd123

Connecting
Completed successfully
```

Associate the Certificate File

Issue the **ssl associate cert** command to associate a certificate name to the imported certificate. For example, to associate the certificate name mychainedrsacert1 to the imported certificate file mychainedrsacert.pem, issue this command:

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

If you receive an error message which indicates `'%% Duplicate association name'`, then choose a different association name.

Suspend Services

In order to modify an SSL proxy list, you must suspend all SSL services that reference the SSL proxy list. For example, this service needs to be suspended in order to modify the proxy list **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
```

Configure the SSL Proxy List

Issue the **ssl-proxy-list** command to modify an SSL proxy list. An SSL proxy list is a group of related virtual or backend SSL servers that are associated with an SSL service. The SSL proxy list contains all the configuration information for each virtual SSL Server. This includes the SSL server creation, certificates and corresponding SSL key pair, Virtual IP (VIP) address and port, SSL ciphers supported, and other SSL options. For example, to modify the ssl-proxy-list ssl_list1, issue this command:

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

Once you enter into the ssl-proxy-list configuration mode, you first need to suspend the SSL proxy list, then specify the certificate association. For example:

```
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

Once the SSL proxy list has been modified and activated, you need to activate all services that reference the SSL proxy list. For example, this service needs to be activated in order to use the proxy list **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 Service and Content Rules

At this point, the client HTTPS traffic can be sent to the Cisco Content Service Switch at 192.168.3.6:443. The Cisco Content Service Switch decrypts the HTTPS traffic to convert it to HTTP. The Cisco Content Service Switch then chooses a service and sends the HTTP traffic to an HTTP Web server. This is an active Cisco Content Service Switch configuration which uses the examples mentioned in this document:

```
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
```

Verify

Once the new certificate is installed, use a browser to connect to the secure Web site in order to ensure there are no alerts presented.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **CSS 11500 Series Content Services Switches Hardware Support**
- **CSS 11000 Series Content Services Switches Hardware Support**
- **Cisco WebNS CSS11500 Software Download (registered customers only)**
- **Cisco WebNS CSS11000 Software Download (registered customers only)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jan 19, 2006 Document ID: 47780