Pedindo e instalando um certificado global no CSS11500

Índice

Introdução

Se você não tem chaves PRE-existentes e Certificados para o Content Services Switch (CSS), você pode gerá-los no CSS. O CSS inclui uma série de utilitários de gerenciamento do certificado e da chave privada para simplificar o processo de gerar chaves privadas, solicitações de assinatura de certificado (CSR), e Certificados provisórios auto-assinados. Este documento descreve o processo para obter um certificado novo de um Certificate Authority (CA) e instalá-lo ao CSS.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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:

- Gerencia Rivest, Shamir, e o par de chaves de Adelman (RSA)
- Associe o arquivo do par de chaves RSA
- Gerencia o CSR
- Obtenha o certificado do intermediário de Verisign
- Importe o arquivo certificado acorrentado
- Associe o arquivo certificado
- Configurar a lista do proxy SSL
- Configurar o serviço e as regras de conteúdo do Secure Socket Layer (SSL)

Gerencia Rivest, Shamir, e o par de chaves de Adelman (RSA)

Emita o **comando ssl genrsa** gerar um RSA privado/pares de chave pública para a criptografia assimétrica. O CSS armazena o par de chaves gerado RSA como um arquivo no CSS. Por exemplo, para gerar o par de chaves myrsakey.pem RSA, datilografe o seguinte:

```
CSS11500(config) # ssl genrsa myrsakey.pem 1024 "passwd123" Please be patient this could take a
few minutes
```

Associando o arquivo do par de chaves RSA

Emita o **comando ssl associate rsakey** associar o nome do par de chaves RSA ao par de chaves gerado RSA. Por exemplo, para associar o nome chave myrsakey1 RSA ao arquivo gerado myrsakey.pem do par de chaves RSA, datilografe o seguinte:

```
CSS11500(config) # ssl associate rsakey myrsakey1 myrsakey.pem
```

Gerencia o CSR

Emita o **comando ssl gencsr rsakey** gerar um arquivo CSR para um arquivo associado do par de chaves RSA. Este CSR será enviado a CA para assinar. Por exemplo, para gerar um CSR baseado no par de chaves myrsakey1 RSA, datilografe o seguinte:

```
CSS11503(config)# ssl gencsr myrsakey1 You are about to be asked to enter information that will
be incorporated into your certificate request. What you are about to enter is what is called a
```

```
Distinguished Name or a DN. For some fields there will be a default value, If you enter '.', the
field will be left blank. Country Name (2 letter code) [US] US State or Province (full name)
[SomeState] CA Locality Name (city) [SomeCity] San Jose Organization Name (company name) [Acme
Inc]Cisco Systems, Inc. Organizational Unit Name (section) [Web Administration] Web Admin Common
Name (your domain name) [www.acme.com] www.cisco.com Email address [webadmin@acme.com]
webadmin@cisco.com
```

O comando **ssl gencsr** gerencie o CSR e outputs o à tela. A maioria de CA principais têm os aplicativos web-based que o exigem cortarar-col o pedido do certificado à tela.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBWDCCAQICAQAwgZwxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTETMBEGA1UE
BxMKQm94Ym9yb3VnaDEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESMBAG
A1UECxMJV2ViIEFkbWluMRYwFAYDVQQDEw13d3cuY2lzY28uY29tMSEwHwYJKoZI
hvcNAQkBFhJra3JvZWJlckBjaXNjby5jb20wXDANBgkqhkiG9w0BAQEFAANLADBI
AkEAqHXjtQUVXvmo6tAWPiMpe6oYhZbJUDgTxbW4VMCygzGZn2wUJTgLrifDB6N3
v+1tKFndE686BhKqfyOidml3wQIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQA94yC3
4SUJJ4UQEnO2OqRGLOZpAElc4+IV9aTWK6NmiZsM9Gt0vPhIkLx5jjhVRLlb27Ak
H6D5omXa0SPJan5x
-----END CERTIFICATE REQUEST-----
```

CA assina o CSR e retorna-lheo, tipicamente usando o endereço email fornecido dentro do CSR.

[Obtenha o certificado do intermediário de Verisign]

Obtenha o certificado de CA

Após ter submetido seu CSR a CA, toma entre um e sete dias úteis para receber um certificado assinado; os tempos variam devido a CA. Uma vez que CA assinou e entregou o certificado, pode ser adicionado ao CSS.

Se você se está aplicando para um StepUp/SGC ou um certificado acorrentado, você precisa de obter o certificado intermediário usado para assinar seu certificado. Você pode obter o certificado intermediário de Verisign do seguinte link:

- Instalando o certificado de CA intermediário

Salvar o certificado intermediário a um arquivo. Por exemplo, intermediate.pem.

Concatene o server e Certificados intermediários

A fim usar-se acorrentou Certificados no CSS, o certificado de servidor e o intermediário deve ser concatenado junto. Isto permite que o CSS retorne o certificate chain inteiro ao cliente em cima da saudação de SSL inicial. Ao criar o arquivo certificado acorrentado para o CSS, seja certo que os Certificados estão na ordem apropriada. O certificado de servidor deve ser primeiro, a seguir o certificado intermediário usado para assinar o certificado de servidor deve ser seguinte. Deve haver um único newline entre o server e os Certificados intermediários. Por exemplo, concatene o certificado de servidor servercert.pem e o intermediate.pem em um certificado acorrentado chamado mychainedrsacert.pem. Os seguintes indicadores que os índices inteiros do mychainedrsacert.pem arquivam.

```
-----BEGIN CERTIFICATE-----
MIICwTCCAioCAQUwDQYJKoZIhvcNAQEEBQAwgagxCzAJBgNVBAYTAlVTMRMwEQYD
 VQQIEwpDYWxpZm9ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEeMBwGA1UEChMVRXhh
 bXBsZSBTeXN0ZW1zLCBJbmMuMRIwEAYDVQQLEwlXZWIgQWRtaW4xGDAWBgNVBAMT
 D3d3dy5leGFtcGxlLmNvbTEjMCEGCSqGSIb3DQEJARYUd2ViYWRtaW5AZXhhbXBs
```

```
 ZS5jb20wHhcNMDQwMTA5MDgzMjI3WhcNMDQwMjA4MDgzMjI3WjCBqDELMAkGA1UE
 BhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMR4w
 HAYDVQQKExVFeGFtcGxlIFN5c3RlbXMsIEluYy4xEjAQBgNVBAsTCVdlYiBBZG1p
 bjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMSMwIQYJKoZIhvcNAQkBFhR3ZWJh
 ZG1pbkBleGFtcGxlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA2huF
 xhVeODHmoXJ4HulDqVQtCvX7eERyRarNI71p0ZV+q+qGYRtJdrlzUav/TbRn5dc0
 8IXjqrASAtTo2S4eWlTOJUnR2g0LH/lcPUaF8f+m+eODWoT8dCtNA5sgEnINAR2y
 HlS5j6dZNcyMY0nFOh68oRsZJJ58u0ZPJjl6eAsCAwEAATANBgkqhkiG9w0BAQQF
 AAOBgQADO/UTIIHnIq2Q0ICiqAQju9nz1vTiIYHBpBnUd8NkPhIHIOqNn9iZ5Q+a
 2zFjh+N2uEt5NxNOEZRbrTZH+HmZMsqJJfvfd62iq+636aPIcoo7X541DYotM05C
 OQjnehsjgwziKlp6UJtuiAwwaxtMIbP7lQXHGO6E9RnzQSvQGQ==
 -----END CERTIFICATE-----
-----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-----
```

Arquivo certificado acorrentado da importação

Uma vez que o CSR foi assinado por CA, está chamado agora um certificado. O arquivo certificado deve ser importado ao CSS. Emita o **comando copy ssl** facilitar a importação ou a exportação dos Certificados e das chaves privadas ou ao CSS. O CSS armazena todos os arquivos importados em um lugar seguro no CSS. Este comando está disponível somente no modo super usuário. Por exemplo, para importar o certificado mychainedrsacert.pem de um servidor remoto ao CSS, datilografe o seguinte:

```
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, datilografe o seguinte:

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

Configurar a lista do proxy SSL

Emita o **comando ssl-proxy-list** criar 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 criar a lista de proxy ssl ssl_list1, datilografe o seguinte:

```
CSS11500(config)# ssl-proxy-list ssl_list1 Create ssl-list <ssl_list1>, [y/n]: y
```

Uma vez que você cria uma lista do proxy SSL, o CLI inscreve-o no modo de configuração da lista de proxy ssl. Configurar seu servidor SSL como mostrado abaixo.

```
CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20 CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20 vip address 192.168.3.6 CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20 rsacert mychainedrsacert1 CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20 rsakey myrsakey1 CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20 cipher rsa-export-with-rc4-40-md5 192.168.11.2 80 5 CSS11500(ssl-proxy-list[ssl_list1])# active
```

Configurar o serviço e as regras de conteúdo do Secure Socket Layer (SSL)

Uma vez que a lista do proxy SSL é ativada, uma necessidade do serviço e da regra de conteúdo de ser configurado para permitir que o CSS envie o tráfego SSL ao módulo SSL. Esta tabela fornece uma vista geral das etapas exigidas para criar um serviço SSL para um servidor SSL virtual, incluindo adicionando a lista do proxy SSL ao serviço e criando uma regra de conteúdo SSL.

Crie um serviço SSL

```
CSS11500(config)# service ssl_serv1Create service <ssl_serv1>, [y/n]: y CSS11500(config-service[ssl_serv1])# type ssl-accel CSS11500(config-service[ssl_serv1])# slot 2 CSS11500(config-service[ssl_serv1])# keepalive type none CSS11500(config-service[ssl_serv1])# add ssl-proxy-list ssl_list1 CSS11500(config-service[ssl_serv1])# active
```

Crie uma regra de conteúdo SSL

```
CSS11500(config)# owner ssl_owner Create owner <ssl_owner>, [y/n]: y CSS11500(config-owner[ssl_owner])# content ssl_rule1 Create content <ssl_rule1>, [y/n]: y CSS11500(config-owner-content[ssl-rule1]# vip address 192.168.3.6 CSS11500(config-owner-content[ssl-rule1]# port 443 CSS11500(config-owner-content[ssl_rule1])# add service ssl_serv1 CSS11500(config-owner-content[ssl_rule1])# active
```

Crie uma regra de conteúdo do texto claro

```
CSS11500(config-owner[ssl_owner])# content decrypted_www Create content <decrypted_www>, [y/n]: y CSS11500(config-owner-content[decrypted_www]# vip address 192.168.11.2 CSS11500(config-owner-content[decrypted_www]# port 80 CSS11500(config-owner-content[decrypted_www])# add service linux_http CSS11500(config-owner-content[decrypted_www])# add service win2k_http CSS11500(config-owner-content[decrypted_www])# active
```

Neste momento, o tráfego do cliente HTTPS pode ser enviado ao CSS em 192.168.3.6:443. O CSS decifra o tráfego HTTPS, convertendo o ao HTTP. O CSS então escolhe um serviço e envia o tráfego de HTTP a um servidor de Web HTTP. O seguinte é uma configuração de CSS de trabalho usando os exemplos acima:

```
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 conf 192.168.11.101 admin des-password 4f2bxansrcehjgka /tftpboot !************************ INTERFACE ************************ interface 1/1 bridge vlan 10 description "Client Side" interface 1/2
```

```
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 mycertcert1 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

Use esta seção para confirmar se a sua configuração funciona corretamente.

Use os **comandos show ssl file e show ssl associate** verificar a configuração.

Verifique que todos os arquivos têm um tamanho maior de 0.

Você pode remover todo o certificado ou chave usando o **comando clear ssl file**.

Troubleshooting

Use esta seção para resolver problemas de configuração.

Se a negociação de SSL falha, use o **comando show ssl statistics** ver a informação util sobre a negociação de SSL falhada.

Por exemplo, verifique estes campos:

```
0 Unknown issuer certificates
0 Failed signatures decryptions
0 Invalid issuer keys
0 Not yet valid certificates
0 Expired Client certificates
0 Revoked certificates
0 CRLs not obtained from host
0 CRLs with bad HTTP return codes
0 CRLs not loaded because of low memory
0 CRLs obtained but failed to load
0 CRLs with invalid signatures
0 CRLs successfully loaded
0 Successful server authentications
0 Server authentications failed
0 Expired Server certificates
```

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