

请求和安装服务器证书在CSS11500上

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

如果没有已存在的密钥和证书内容服务交换机(CSS)的，您在CSS能生成他们。CSS包括一系列的证书和专用密钥管理工具简化生成专用密钥、Certificate Signing Requests (CSR)和自己签署的临时证书进程。本文描述获取新证书从Certificate Authority (CA)和安装的它进程对CSS。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意：要查找有关本文档中所使用的命令的详细信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

配置

本文档使用如下所示的配置。

- 生成Rivest、沙米尔和Adelman (RSA)密钥对
- 关联RSA密钥对文件
- 生成 CSR
- 从CA获取证书
- 导入证书文件
- 关联证书文件
- 配置SSL代理列表
- 配置安全套接字层SSL服务和内容规则

生成Rivest、沙米尔和Adelman (RSA)密钥对

发出**ssl genrsa**命令生成RSA非对称加密的私有/公共密钥对。CSS存储生成的RSA密钥对作为在CSS的一个文件。例如，生成RSA密钥对myrsakey.pem，请键入以下：

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

关联RSA密钥对文件

发出**ssl associate rsakey**命令关联RSA密钥对名称到生成的RSA密钥对。例如，关联RSA密钥名称myrsakey1到生成的RSA密钥对文件myrsakey.pem，请键入以下：

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

生成 CSR

发出**ssl gencsr rsakey**命令生成一个相关的RSA密钥对文件的一个CSR文件。此CSR将发送对签字的CA。例如，生成根据RSA密钥对myrsakey1的CSR，请键入以下：

```
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** **ssl gencsr**命令生成CSR并且输出它到屏幕。多数主要CA有要求您剪贴证书请求到屏幕的基于Web的应用。

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBWDCAQICAQAwgZwxZzAJBgNVBAYTA1VMTQswCQYDVQQLIEwJNQTET
MBEGA1UE
BxMKQm94Ym9yY3VnaDEcMBoGA1UEChMTQ2l2Y28gU3lzdGVtcywgSW5j
LjESMBAG
A1UECxMJV2ViIEFkbluMRYwFAYDVQQDEw13d3cuY2l2Y28uY29tMSEw
HwYJKoZI
hvCNAQkBFhJra3JvZWJlckBjaXNjby5jb20wXDANBgkqhkiG9w0BAQEF
```

```
AANLADBI
AkEAqHXjtQUVXvmo6tAWPiMpe6oYhZbJUDgTxbW4VMCygZGzn2wUJTgL
rifDB6N3
v+1tKFndE686BhKqfyOidml3wQIDAQABoAAwDQYJKoZIhvcNAQEEBQAD
QQA94yC3
4SUJJ4UQEnO2OqRGL0ZpAE1c4+IV9aTWK6NmiZsM9Gt0vPhIkLx5jjhV
RLlb27Ak
H6D5omXa0SPJan5x
-----END CERTIFICATE REQUEST-----
```

CA签署CSR并且返回它给您，典型地使用在CSR内提供的电子邮件地址。

从CA获取证书

在提交您的CSR以后对CA，它采取在一个和七个工作日之间接收签名证书;时代变化由于CA。一旦CA签署了并且传送证书，可以被添加到CSS。

导入证书文件

一旦CSR由CA签了字，它当前呼叫证书。必须导入证书文件到CSS。发出**copy ssl**命令实现证书和专用密钥导入或出口从或对CSS。CSS在CSS的一个安全位置存储所有导入的文件。此指令仅可用的在超级用户模式。例如，导入从远程服务器的mychainedrsacert.pem证书到CSS，请键入以下：

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

关联证书文件

发出**ssl associate cert**命令关联验证名称到已导入证书。例如，关联验证名称mychainedrsacert1到已导入证书文件mychainedrsacert.pem，请键入以下：

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

配置SSL代理列表

发出**ssl-proxy-list**命令建立SSL代理列表。SSL代理列表是关联与SSL服务相关虚拟或后端SSL服务器的一组。SSL代理列表包含每台虚拟SSL服务器的所有配置信息。这包括SSL服务器创建、证书和对应SSL密钥对、Virtual IP (VIP)地址和端口、SSL密码器支持的和和其他SSL选项。例如，创建ssl代理列表ssl_list1，请键入以下：

```
CSS11500(config)# ssl-proxy-list ssl_list1 Create ssl-
list <ssl_list1>, [y/n]: y 一旦建立SSL代理列表，
CLI送进您到ssl代理列表配置模式。配置您的SSL服务器
如下所示。
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
```

配置安全套接字层SSL服务和内容规则

一旦SSL代理列表激活，服务和内容规则需要配置允许CSS发送SSL流量到SSL模块。此表提供要求的步骤的概

述创建一个虚拟SSL服务器的一SSL服务，包括添加SSL代理列表到服务和创建SSL内容规则。**创建SSL服务**

```
CSS11500(config)# service ssl_serv1 Create 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 创建SSL内容规则
```

```
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 创建明文内容规则
```

```
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
```

这时，客户端HTTPS流量可以发送到在192.168.3.6:443的CSS。CSS解密HTTPS流量，转换它对HTTP。CSS然后选择服务并且发送HTTP数据流到HTTP Web服务器。使用以上示例，下列是一个工作的CSS配置：

```
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
```

[验证](#)

当前没有可用于此配置的验证过程。

[故障排除](#)

目前没有针对此配置的故障排除信息。

[相关信息](#)

- [CSS 11500系列内容服务交换机硬件支持](#)
- [CSS 11000系列内容服务交换机硬件支持](#)
- [Cisco WebNS CSS11500软件下载\(仅限注册用户\)](#)
- [Cisco WebNS CSS 11000软件下载\(仅限注册用户\)](#)
- [技术支持和文档 - Cisco Systems](#)