Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Conventions](#)
[Configurez](#)
[Configurations](#)
[Vérifiez](#)
[Dépannez](#)
[Informations connexes](#)

Introduction

Si vous n'avez pas des clés préexistantes et des Certificats pour le Commutateur de services de contenu (CSS), vous pouvez les générer sur le CSS. Le CSS inclut une gamme de certificat et d'utilitaires privés de gestion des clés pour simplifier le processus de générer des clés privées, des demandes de signature de certificat (CSR), et des Certificats provisoires auto-signés. Ce document décrit le processus pour obtenir un nouveau certificat d'un Autorité de certification (CA) et l'installer sur le CSS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Pour obtenir plus d'informations sur les commandes utilisées dans ce document,

utilisez l'Outil de recherche de commande (clients enregistrés uniquement).

Configurations

Ce document utilise les configurations présentées ci-dessous.

- Générez Rivest, Shamir, et paire de clés d'Adelman (RSA)
- Associez le fichier de paire de clés RSA
- Générez le CSR
- Obtenez le certificat d'un CA
- Fichier du certificat enchaîné d'importation
- Associez le fichier du certificat
- Configurez la liste de proxy SSL
- Configurez le service et les règles de contenu de Protocole SSL (Secure Socket Layer)

Générez Rivest, Shamir, et paire de clés d'Adelman (RSA)
Émettez la commande de **genrsa SSL** de générer paire de clés privée/publique RSA pour le cryptage asymétrique. Le CSS enregistre la paire de clés RSA générée comme fichier sur le CSS. Par exemple, pour générer la paire de clés RSA myrsakey.pem, tapez ce qui suit : `CSS11500(config) # ssl genrsa myrsakey.pem 1024 ?passwd123?Please be patient this could take a few minutes`
Associer le fichier de paire de clés RSA
Émettez la commande de **rsakey d'associé SSL** d'associer le nom de paire de clés RSA à la paire de clés RSA générée. Par exemple, pour associer le nom de clé RSA myrsakey1 au fichier généré myrsakey.pem de paire de clés RSA, tapez ce qui suit : `CSS11500(config) # ssl associate rsakey myrsakey1 myrsakey.pem`
Générez le CSR
Émettez la commande de **rsakey de gencsr SSL** de générer un fichier CSR pour un fichier associé de paire de clés RSA. Ce CSR sera envoyé au CA pour la signature. Par exemple, pour générer un CSR basé sur la paire de clés RSA myrsakey1, tapez ce qui suit : `CSS11503(config)# ssl gencsr myrsakey1You are about to be asked to enter informationthat will be incorporated into your certificaterequest. What you are about to enter is what iscalled 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] USState or Province (full name) [SomeState] CALocality Name (city) [SomeCity] San JoseOrganization Name (company name) [Acme Inc]Cisco Systems, Inc.Organizational Unit Name (section) [Web Administration] Web AdminCommon Name (your domain name) [www.acme.com] www.cisco.comEmail address [webadmin@acme.com] webadmin@cisco.com`La commande de **gencsr SSL** génère le CSR et le sort à l'écran. La plupart de commandant CAs ont des applications Web qui exigent de vous de couper-coller la demande de certificat à l'écran. `CSS11503(config)#`

ssl gencsr myrsakey1 You are about to be asked to enter informationthat will be incorporated into your certificaterequest. What you are about to enter is what iscalled 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**Le CA signe le CSR et le renvoie te, typiquement utilisant l'adresse e-mail fournie dans le CSR.

Obtenez le certificat d'un CA

Après la soumission de votre CSR à un CA, il prend entre un et sept Business Day pour recevoir un certificat signé ; les temps varient en raison du CA. Une fois que le CA a signé et a fourni le certificat, il peut ajouter au CSS.

Fichier du certificat enchaîné d'importation

Une fois que le CSR a été signé par un CA, ce s'appelle maintenant un certificat. Le fichier du certificat doit être importé au CSS. Émettez la commande **SSL de copie** de faciliter l'importation ou l'exportation des Certificats et des clés privées ou derrière le CSS. Le CSS enregistre tous les fichiers importés dans un emplacement sécurisé sur le CSS. Cette commande est disponible seulement dans le mode de super utilisateur. Par exemple, pour importer le certificat mychainedrsacert.pem d'un serveur distant au CSS, tapez ce qui suit : CSS11500# **copy ssl sftp ssl_record import mychainedrsacert.pem PEM** ?passwd123?Connecting Completed successfully

Associez le fichier du certificat

Émettez la commande de **CERT d'associé SSL** d'associer un nom de certificat au certificat importé. Par exemple, pour associer le nom mychainedrsacert1 de certificat au fichier du certificat importé mychainedrsacert.pem, tapez ce qui suit : CSS11500(config)# **ssl associate cert mychainedrsacert1 mychainedrsacert.pem**

Configurez la liste de proxy SSL

Émettez la commande de SSL-proxy-**liste** de créer une liste de proxy SSL. Une liste de proxy SSL est un groupe de serveurs virtuels ou principaux relatifs SSL qui sont associés avec un service SSL. La liste de proxy SSL contient toutes les informations de configuration pour chaque serveur virtuel SSL. Ceci inclut la création de serveur SSL, paire de clés SSL de Certificats et de correspondance, adresse virtuelle et port IP (VIP), chiffrements SSL pris en charge, et d'autres options SSL. Par exemple, pour créer la SSL-proxy-liste ssl_list1,

tapez ce qui suit : `CSS11500(config)# ssl-proxy-list ssl_list1Create ssl-list <ssl_list1>, [y/n]: y` Une fois que vous créez une liste de proxy SSL, le CLI vous présente dans le mode de configuration de SSL-proxy-liste. Configurez votre serveur SSL comme affiché ci-dessous.

```
CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20 vip address 192.168.3.6CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20 rsacert mychainedrsacert1CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20 rsakey myrsakey1CSS11500(ssl-proxy-list[ssl_list1])# ssl-server 20 cipher rsa-export-with-rc4-40-md5 192.168.11.2 80 5CSS11500(ssl-proxy-list[ssl_list1])# active
```

Configurez le service et les règles de contenu de Protocole SSL (Secure Socket Layer)

Une fois que la liste de proxy SSL est lancée, un besoin de service et de règle de contenu d'être configuré pour permettre au CSS pour envoyer le trafic SSL au module SSL. Cette table fournit un aperçu de l'étape nécessaire pour créer un service SSL pour un serveur virtuel SSL, y compris ajouter la liste de proxy SSL au service et créer une règle de contenu SSL. **Créez un service SSL**

```
CSS11500(config)# service ssl_serv1Create service <ssl_serv1>,    [y/n]: yCSS11500(config-service[ssl_serv1])# type ssl-accelCSS11500(config-service[ssl_serv1])# slot 2CSS11500(config-service[ssl_serv1])# keepalive type noneCSS11500(config-service[ssl_serv1])# add ssl-proxy-list ssl_list1CSS11500(config-service[ssl_serv1])# active
```

Créez une règle de contenu SSL

```
CSS11500(config)# owner ssl_ownerCreate owner <ssl_owner>, [y/n]: yCSS11500(config-owner[ssl_owner])# content ssl_rule1Create content <ssl_rule1>, [y/n]: yCSS11500(config-owner-content[ssl-rule1]# vip address 192.168.3.6CSS11500(config-owner-content[ssl-rule1]# port 443 CSS11500(config-owner-content[ssl_rule1])# add service ssl_serv1 CSS11500(config-owner-content[ssl_rule1])# active
```

Créez une règle de contenu des textes clairs

```
CSS11500(config-owner[ssl_owner])# content decrypted_www Create content <decrypted_www>, [y/n]: yCSS11500(config-owner-content[decrypted_www]# vip address 192.168.11.2CSS11500(config-owner-content[decrypted_www]# port 80CSS11500(config-owner-content[decrypted_www])# add service linux_httpCSS11500(config-owner-content[decrypted_www])# add service win2k_httpCSS11500(config-owner-content[decrypted_www])# active
```

En ce moment, le trafic du client HTTPS peut être envoyé au CSS à 192.168.3.6:443. Le CSS déchiffre le trafic HTTPS, le convertissant en HTTP. Le CSS alors choisit un service et envoie le trafic http à un serveur Web de HTTP. Ce qui suit est une configuration fonctionnante CSS utilisant les exemples ci-dessus :

```
CSS11501# show runconfigure!**************************
GLOBAL ***************************ssl associate rsakey
myrsakey1 myrsakey.pemssl associate cert mychainedrsacert1
mychainedrsacert.pemip route 0.0.0.0 0.0.0.0 192.168.3.1
1ftp-record conf 192.168.11.101 admin des-password
4f2bxansrcehjgka /tftpboot!************************
INTERFACE ************************interface 1/1bridge vlan
10description "Client Side"interface 1/2bridge vlan
```

```
20description "Server Side"!*************************
CIRCUIT ************************circuit VLAN10description
"Client Segment"ip address 192.168.3.254 255.255.255.0circuit
VLAN20description "Server Segment"ip address 192.168.11.1
255.255.255.0!********************** SSL PROXY LIST
**********************ssl-proxy-list ssl_list1ssl-server
20ssl-server 20 vip address 192.168.3.6ssl-server 20 rsakey
myrsakey1ssl-server 20 rsacert mycertcert1ssl-server 20
cipher rsa-with-rc4-128-md5 192.168.11.2
80active!************************** SERVICE
**************************service linux-httpip address
192.168.11.101port 80activeservice win2k-httpip address
192.168.11.102port 80activeservice ssl_serv1type ssl-
accelslot 2keepalive type noneadd ssl-proxy-list
ssl_list1active!************************** OWNER
**************************owner ssl_ownercontent
ssl_rule1vip address 192.168.3.6protocol tcpport 443add
service ssl_serv1activecontent decrypted_wwwvip address
192.168.11.2add service linux-httpadd service win2k-
httpprotocol tcpport 80active
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Support matériel pour les commutateurs de services de contenu de la gamme CSS 11500
- Support matériel de Commutateurs de services satisfaits de gamme 11000 CSS
- Téléchargement logiciel de Cisco WebNS CSS11500 (enregistrés seulement
- Téléchargement logiciel de Cisco WebNS CSS11000 (enregistrés seulement
- Support et documentation techniques - Cisco Systems