Configure y aliste a un router del Cisco IOS a otro router del Cisco IOS configurado como servidor de CA

Contenido

Introducción

Este documento describe cómo configurar a un router de Cisco IOS® como servidor del Certificate Authority (CA). Además, ilustra cómo alistar a otro router del Cisco IOS para obtener una raíz y el certificado ID para la Autenticación IPSec del servidor de CA.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dos Cisco 2600 Series Router que funcionan con el Cisco IOS Software Release 12.3(4)T3.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Genere y exporte el par clave RSA para el servidor de certificados

El primer paso es generar el par clave RSA que el servidor de CA del Cisco IOS utiliza. En el router (r1), genere las claves RSA como esta salida muestra:

```
R1(config)#crypto key generate rsa general-keys label cisco1 exportable The name for the keys
will be: cisco1 Choose the size of the key modulus in the range of 360 to 2048 for your General
Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in
the modulus [512]: % Generating 512 bit RSA keys ...[OK] R1(config)# *Jan 22 09:51:46.116: %SSH-
5-ENABLED: SSH 1.99 has been enabled
```

Nota: Usted debe utilizar el mismo nombre para el par clave (clave-*escritura de la etiqueta*) ese usted plan para utilizar para el servidor de certificados (vía el comando **crypto de la** *escritura de la etiqueta del cs del* **servidor pki** cubierto más adelante).

Exporte el par clave generado

Exporte las claves al RAM no volátil (NVRAM) o al TFTP (basado en su configuración). En este ejemplo, se utiliza el NVRAM. De acuerdo con su implementación, usted puede ser que quiera utilizar a un servidor TFTP separado para salvar su información del certificado.

```
R1(config)#crypto key export rsa cisco1 pem url nvram: 3des cisco123 % Key name: cisco1 Usage:
General Purpose Key Exporting public key... Destination filename [cisco1.pub]? Writing file to
nvram:cisco1.pub Exporting private key... Destination filename [cisco1.prv]? Writing file to
nvram:cisco1.prv R1(config)#
```

Si usted utiliza a un servidor TFTP, usted puede reimportar el par clave generado mientras que este comando muestra:

```
crypto key import rsa key-label pem [usage-keys] {terminal | url url} [exportable] passphrase
```

Nota: Si usted no quisiera que la clave fuera exportable de su servidor de certificados, impórtela de nuevo al servidor de certificados después de que se haya exportado como par clave NON-exportable. Esta manera, la clave no se puede sacar otra vez.

Verifique el par clave generado

Publique el **comando show crypto key mypubkey rsa** para verificar el par clave generado.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

```
R1#show crypto key mypubkey rsa % Key pair was generated at: 09:51:45 UTC Jan 22 2004 Key name:
cisco1 Usage: General Purpose Key Key is exportable. Key Data: 305C300D 06092A86 4886F70D
01010105 00034B00 30480241 00CC2DC8 ED26163A B3642376 FAA91C2F 93A3825B 3ABE6A55 C9DD3E83
F7B2BD56 126E0F11 50552843 7F7CA4DA 3EC3E2CE 0F42BD6F 4C585385 3C43FF1E 04330AE3 37020301 0001 %
Key pair was generated at: 09:51:54 UTC Jan 22 2004 Key name: cisco1.server Usage: Encryption
Key Key is exportable. Key Data: 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00EC5578
025D3066 72149A35 32224BC4 3E41DD68 38B08D39 93A1AA43 B353F112 1E56DA42 49741698 EBD02905
FE4EC392 7174EEBF D82B4475 2A2D7DEC 83E277F8 AEC590BE 124E00E1 C1607433 5C7BC549 D532D18C
DD0B7AE3 AECDDE9C 07AD84DD 89020301 0001
```

Habilite al servidor HTTP en el router

El servidor de CA del Cisco IOS soporta solamente las inscripciones hechas vía el protocolo simple certificate enrollment (SCEP). Por lo tanto, para hacer este posible, el router debe funcionar con al servidor HTTP incorporado del Cisco IOS. Utilice el **comando ip http server** para habilitarlo:

```
R1(config)#ip http server
```

Habilite y configure el servidor de CA en el router

Complete estos pasos:

1. Es muy importante recordar que el servidor de certificados debe utilizar el mismo nombre que el par clave usted acaba de generar manualmente.La escritura de la etiqueta hace juego la escritura de la etiqueta generada del par clave:`R1(config)#crypto pki server cisco1` Después de que usted haya habilitado a un servidor de certificados, usted puede utilizar los valores predeterminados preconfigurados o especificar los valores vía el CLI para las funciones del servidor de certificados.
2. **El comando url de la base de datos** especifica la ubicación en donde todas las entradas de la base de datos para el servidor de CA se ponen en escrito. Si este comando no se especifica, todas las entradas de la base de datos se escriben para contellear.`R1(cs-server)#database url nvram:` **Nota:** Si usted utiliza a un servidor TFTP, el URL necesita ser **tftp:// <ip_address>/directory**.
3. Configure el nivel de la base de datos:`R1(cs-server)#database level minimum` Este controles de comandos salvan a qué tipo de datos en la base de datos de la inscripción del

certificado:**Mínimo** — Bastante información se salva para continuar solamente publicando los nuevos Certificados sin el conflicto. El valor predeterminado.**Nombres** — Además de la información dada en el nivel mínimo, el número de serie y el asunto de cada certificado.**Completo** — Además de la información dada en los niveles mínimos y de los nombres, cada certificado publicado se escribe a la base de datos.**Nota:** La palabra clave **completa** presenta una gran cantidad de información. Si se publica, usted debe también especificar a un servidor TFTP externo en quien salvar los datos vía el **comando url de la base de datos**.

4. Configure el nombre del emisor de CA a la DN-cadena especificada. En este ejemplo, el CN (Common Name) de cisco1.cisco.com, L (lugar) de RTP, y el C (país) de los E.E.U.U. se utilizan:`R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US`
5. Especifique el curso de la vida, en los días, de un certificado de CA o de un certificado.Los valores válidos se extienden a partir de *1 día a 1825 días*. El curso de la vida predeterminado del certificado de CA es tres años y el curso de la vida predeterminado del certificado es un año. La vida útil máxima del certificado es *un mes menos* que el curso de la vida del certificado de CA. Por ejemplo:`R1(cs-server)#lifetime ca-certificate 365 R1(cs-server)#lifetime certificate 200`
6. Defina el curso de la vida, en las horas, del CRL que es utilizado por el servidor de certificados. El valor máximo del curso de la vida es **336 horas** (dos semanas). El valor predeterminado es **168 horas** (una semana).`R1(cs-server)#lifetime crl 24`
7. Defina un punto de distribución de la Lista de Revocación de Certificados (CRL) (CDP) para utilizar en los Certificados que son publicados por el servidor de certificados.El URL debe ser HTTP URL. Por ejemplo, nuestro servidor tenía una dirección IP de 172.18.108.26:`R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl`
8. Publique el **comando no shutdown** para habilitar el servidor CA:`R1(cs-server)#no shutdown` **Nota:** Publique este comando solamente después que usted ha configurado totalmente a su servidor de certificados.

Configure y aliste al segundo router IOS (r2) al servidor de certificados

Siga este procedimiento.

1. Configure un nombre de host, un Domain Name, y genere las claves RSA en el r2.Utilice el **comando hostname** para configurar el nombre de host del router para ser r2:`Router(config)#hostname R2 R2(config)#` Note que el nombre de host del router cambiado inmediatamente después que usted ingresó el **comando hostname**.Utilice el **comando ip domain-name** para configurar el Domain Name en el router:`R2(config)#ip domain-name cisco.com` Utilice el **comando crypto key generate rsa** para generar el par clave del r2:`R2(config)#crypto key generate rsa The name for the keys will be: R2.cisco.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: % Generating 512 bit RSA keys ...[OK]`
2. Utilice estos comandos en el modo de configuración global para declarar a CA que su router debe utilizar (Cisco IOS CA en este ejemplo) y especificar las características para el trustpoint CA:
   `crypto ca trustpoint cisco enrollment retry count 5 enrollment retry period 3 enrollment url http://14.38.99.99:80 revocation-check none` **Nota: El comando crypto ca trustpoint**

unifica el **comando crypto ca identity** y el **comando crypto ca trusted-root** existentes, de tal modo proporcionando a las funciones combinadas bajo comando único.

3. Utilice el **Ca crypto autentican el comando cisco** (Cisco es la escritura de la etiqueta del trustpoint) para extraer el certificado raíz del servidor de CA:`R2(config)#`**`crypto ca authenticate cisco`**
4. Utilice el **Ca crypto alistan el comando cisco** (Cisco es la escritura de la etiqueta del trustpoint) para alistar y generar:`R2(config)#`**`crypto ca enroll cisco`** Después con éxito de alistar a CA del Cisco IOS el servidor, usted debe ver los Certificados publicados usando el comando show crypto ca certificates. Ésta es la salida del comando. El comando visualiza la información detallada del certificado, que corresponden con los parámetros configurados en el servidor de CA del Cisco IOS:`R2#`**`show crypto ca certificates`** `Certificate Status: Available Certificate Serial Number: 02 Certificate Usage: General Purpose Issuer:` **`cn=cisco1.cisco.com l=RTP c=US`** `Subject: Name:` **`R2.cisco.com`** `hostname=`**`R2.cisco.com`** `CRL Distribution Point:` **`http://172.18.108.26/cisco1cdp.cisco1.crl`** `Validity Date: start date: 15:41:11 UTC Jan 21 2004 end date: 15:41:11 UTC Aug 8 2004 renew date: 00:00:00 UTC Jan 1 1970 Associated Trustpoints:` **`cisco`** `CA Certificate Status: Available Certificate Serial Number: 01 Certificate Usage: Signature Issuer:` **`cn=cisco1.cisco.com l=RTP c=US`** `Subject:` **`cn=cisco1.cisco.com l=RTP c=US`** `Validity Date: start date: 15:39:00 UTC Jan 21 2004 end date: 15:39:00 UTC Jan 20 2005 Associated Trustpoints:` **`cisco`**
5. Ingrese este comando para salvar la clave a memoria flash persistente:`hostname(config)#`**`write memory`**
6. Ingrese este comando para salvar la configuración:`hostname#`**`copy run start`**

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **muestre los Certificados Ca crypto** — Certificados de las visualizaciones.
- **mypubkey rsa del show crypto key** — Visualiza el par clave.
```
!% Key pair was generated at:
09:28:16 EST Jan 30 2004
  !Key name: ese-ios-ca
  ! Usage: General Purpose Key
  ! Key is exportable.
  ! Key Data:
  !  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AF2198
  !  C56F1A8F 5AC501FF ADFB1489 1F503F91 CA3C3FA3 9FB2C150 FFCBF815 2AA73060
  !  E79AF510 E292C171 C6804B45 0CAAD4AF 5834AB85 B204208B 3960D20D 9B51AF7B
  !  ACF12D3D F5BC6EAE 77186AE9 1471F5A4 443CE5B5 1336EC33 5FEB3398 002C15EE
  !  9F8FD331 83490D8A 983FBBE1 9E72A130 121A3B97 A3ACD147 C37DA3D6 77020301 0001
  !% Key pair was generated at: 09:28:17 EST Jan 30 2004
  !Key name: ese-ios-ca.server
  ! Usage: Encryption Key
  ! Key is exportable.
  ! Key Data:
  !  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 0096456A 01AEC6A5
  !  0049CCA7 B41B675E 5317328D DF879CAE DB96A739 26F2A03E 09638A7A 99DFF8E9
  !  18F7635D 6FB6EE27 EF93B3DE 336C148A 6A7A91CB 6A5F7E1B E0084174 2C22B3E2
  !  3ABF260F 5C4498ED 20E76948 9BC2A360 1C799F8C 1B518DD8 D9020301 0001
```
- **info crl crypto del servidor pki ESE-IOS-Ca** — Visualiza el Listas de revocación de certificados (CRL).
```
! Certificate Revocation List:
  !    Issuer: cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
  !    This Update: 09:58:27 EST Jan 30 2004
```

```
!    Next Update: 09:58:27 EST Jan 31 2004
!    Number of CRL entries: 0
!    CRL size: 300 bytes
```

- **peticiones crypto de la información del servidor pki ESE-IOS-Ca** — Peticiones pendientes de la inscripción de las visualizaciones.
```
! Enrollment Request Database:
! ReqID  State      Fingerprint                      SubjectName
! --------------------------------------------------------------
```
- **muestre al servidor pki crypto** — Visualiza al estado del servidor actual del Public Key Infrastructure (PKI).
```
! Certificate Server status: enabled, configured
!    Granting mode is: manual
!    Last certificate issued serial number: 0x1
!    CA certificate expiration timer: 10:58:20 EDT Jun 21 2005
!    CRL NextUpdate timer: 09:58:26 EST Jan 31 2004
!    Current storage dir: nvram:
!    Database Level: Names - subject name data written as .cnm
```
- **concesión crypto de la** *escritura de la etiqueta del cs del* **servidor pki {toda |** *la transacción - identificación***}** — concede todos o las peticiones específicas SCEP.
- **rechazo crypto de la** *escritura de la etiqueta del cs del* **servidor pki {todo |** *la transacción - identificación***}** — rechaza todos o las peticiones específicas SCEP.
- **la contraseña crypto de la escritura de la etiqueta del cs del servidor pki genera el [minutes]** — Genera un contraseña que se puede utilizar una sola vez (OTP) para una petición SCEP (minutos - longitud del tiempo (en los minutos) que la contraseña sea válida. El intervalo válido es a partir 1 a 1440 minutos. El valor por defecto es 60 minutos.**Nota:** Solamente un OTP es en un momento válido. Si se genera un segundo OTP, el OTP anterior es no más válido.
- *la escritura de la etiqueta del cs* **crypto del servidor pki revoca el** *número de serie del certificado* — Revoca un certificado basado en su número de serie.
- **petición crypto** *pkcs10* **{***URL de la escritura de la etiqueta del cs del* **servidor pki URL | [pem] de la** *terminal***}** — agrega manualmente la petición del base64 o de la inscripción del certificado PEM PKCS10 a la base de datos de la petición.
- **info crl crypto de la** *escritura de la etiqueta del cs del* **servidor pki** — Visualiza la información con respecto al estatus del CRL actual.
- **petición crypto de la información de la** *escritura de la etiqueta del cs del* **servidor pki** — Visualiza todas las peticiones excepcionales de la inscripción del certificado.

Vea el verificar la sección generada del par clave de este documento para la información de verificación adicional.

Troubleshooting

Refiera al Troubleshooting de IP Security - Entendiendo y con los comandos debug para la información de Troubleshooting.

Nota: En muchas situaciones, usted puede solucionar los problemas cuando usted borra y redefine el servidor de CA.

Información Relacionada

- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems