Configuración e inscripción de un router Cisco IOS en otro router Cisco IOS configurado como servidor CA

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Diagrama de la red
Convenciones
Generar y exportar el par de claves RSA para el servidor de certificados
Exportar el par de claves generado
Verificar el par de claves generado
Habilitar el servidor HTTP en el router
Habilitar y configurar el servidor de la CA en el router
Configuración e inscripción del segundo router IOS (R2) en el servidor de certificados
Verificación
Troubleshoot
Información Relacionada

Introducción

Este documento describe cómo configurar un router Cisco IOS® como servidor de Autoridad de Certificación (CA). Además, ilustra cómo inscribir otro router Cisco IOS para obtener un certificado raíz e ID para la autenticación IPsec del servidor CA.

Prerequisites

Requirements

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 routers Cisco serie 2600 que ejecutan Cisco IOS Software Release 12.3(4)T3.

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.

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.

Generar y exportar el par de claves RSA para el servidor de certificados

El primer paso es generar el par de llaves RSA que utiliza el servidor de CA de Cisco IOS. En el router (R1), genere las claves RSA como muestra este resultado:

```
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: Debe utilizar el mismo nombre para el par de claves (*key-label*) que planea utilizar para el servidor de certificados (a través del **comando crypto pki server *cs-label* cubierto más adelante).**

Exportar el par de claves generado

Exporte las claves a RAM no volátil (NVRAM) o TFTP (según su configuración). En este ejemplo, se utiliza NVRAM. Según su implementación, es posible que desee utilizar un servidor TFTP independiente para almacenar la 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 utiliza un servidor TFTP, puede volver a importar el par de claves generado como muestra este comando:

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

Nota: Si no desea que la clave se pueda exportar desde el servidor de certificados, vuelva a importarla al servidor de certificados después de exportarla como un par de claves no exportables. De esta manera, la llave no puede ser despegada de nuevo.

Verificar el par de claves generado

Ejecute el comando **show crypto key mypubkey rsa** para verificar el par de claves 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
```

Habilitar el servidor HTTP en el router

El servidor de la CA de Cisco IOS solo admite las inscripciones realizadas mediante el protocolo simple de inscripción de certificados (SCEP). En consecuencia, para hacer esto posible, el router debe ejecutar el servidor HTTP integrado de Cisco IOS. Utilice el comando **ip http server** para habilitarlo:

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

Habilitar y configurar el servidor de la 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 de claves que acaba de generar manualmente.La etiqueta coincide con la etiqueta del par de claves generado:
   ```
   R1(config)#crypto pki server cisco1
   ```

   Después de haber habilitado un servidor de certificados, puede utilizar los valores predeterminados preconfigurados o especificar valores a través de CLI para la funcionalidad del servidor de certificados.
2. El comando **database url** especifica la ubicación donde se escriben todas las entradas de base de datos para el servidor de la CA. Si no se especifica este comando, todas las entradas de la base de datos se escriben en Flash.
   ```
   R1(cs-server)#database url nvram:
   ```

   Nota: Si utiliza un servidor TFTP, la URL debe ser **tftp://<ip_address>/directory**.
3. Configure el nivel de base de datos:
   ```
   R1(cs-server)#database level minimum
   ```

   Este comando controla el tipo de datos almacenados en la base de datos de inscripción de certificados:**Mínimo**: la información suficiente sólo se almacena para continuar emitiendo nuevos certificados sin conflicto. El valor predeterminado.**Nombres**: además de la información proporcionada en el nivel mínimo, el número de serie y el nombre del asunto de cada certificado.**Completo**: además de la información proporcionada en los niveles mínimo y de nombres, cada certificado emitido se escribe en la base de datos.**Nota:** La palabra clave **complete** produce una gran cantidad de información. Si se ejecuta, también debe especificar un servidor TFTP externo en el cual almacenar los datos a través del comando **database url**.
4. Configure el nombre del emisor de CA en la cadena DN especificada. En este ejemplo, se utiliza el CN (Nombre común) de cisco1.cisco.com, L (Localidad) de RTP y C (País) de US:
   ```
   R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
   ```

5. Especifique la duración, en días, de un certificado de CA o de un certificado.Los valores válidos van de *1 día a 1825 días*. La duración predeterminada del certificado de CA es de tres años y la duración predeterminada del certificado es de un año. La duración máxima del certificado es *un mes menos* que la duración del certificado de CA. Por ejemplo:
   ```
   R1(cs-server)#lifetime ca-certificate 365
   R1(cs-server)#lifetime certificate 200
   ```
6. Defina la duración, en horas, de la CRL que utiliza el servidor de certificados. El valor máximo de 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 lista de revocación de certificados (CDP) que se utilice en los certificados emitidos por el servidor de certificados.La URL debe ser una URL HTTP. 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. Ejecute el comando **no shutdown** para habilitar el servidor CA:
```
R1(cs-server)#no shutdown
```

   Nota: Ejecute este comando sólo después de haber configurado completamente su servidor de certificados.

Configuración e inscripción del segundo router IOS (R2) en el servidor de certificados

Siga este procedimiento.

1. Configure un nombre de host, un nombre de dominio y genere las claves RSA en R2.Utilice el comando **hostname** para configurar el nombre de host del router para que sea R2:
```
Router(config)#hostname R2
R2(config)#
```
   Observe que el nombre de host del router cambió inmediatamente después de ingresar el comando **hostname**.Utilice el comando **ip domain-name** para configurar el nombre de dominio en el router:
```
R2(config)#ip domain-name cisco.com
```

   Utilice el comando **crypto key generate rsa** para generar el par de claves 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 la CA que su router debe utilizar (Cisco IOS CA en este ejemplo) y especificar las características para la CA del punto de confianza:

```
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 trustroot**, proporcionando así funcionalidad combinada bajo un único comando.
3. Utilice el comando **crypto ca authenticate cisco** (cisco es la etiqueta del punto de confianza) para recuperar el certificado raíz del servidor de la CA:
```
R2(config)#crypto ca authenticate cisco
```

4. Utilice el comando **crypto ca enroll cisco** (cisco es la etiqueta del punto de confianza) para inscribirse y generar:
```
R2(config)#crypto ca enroll cisco
```

Después de inscribirse correctamente en el servidor de CA de Cisco IOS, debe ver los certificados emitidos mediante el comando **show crypto ca certificates**. Ésta es la salida del comando. El comando muestra la información detallada del certificado, que corresponde con los parámetros configurados en el servidor de la CA de 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 guardar la clave en la memoria Flash persistente:
```
hostname(config)#write memory
```

6. Ingrese este comando para guardar 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.

- **show crypto ca certificates**—Muestra certificados.
- **show crypto key mypubkey rsa**—Muestra el par de claves.
```
!% 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
```

- **crypto pki server ese-ios-ca info crl**: muestra la lista 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
```

- **crypto pki server ese-ios-ca info requests**—Muestra las solicitudes de inscripción pendientes.

```
! Enrollment Request Database:
  ! ReqID  State      Fingerprint                      SubjectName
  ! --------------------------------------------------------------
```

- **show crypto pki server**: muestra el estado actual del servidor de infraestructura de clave pública (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
```

- **crypto pki server *cs-label* Grant { all | *tranaction-id* }** : concede todas las solicitudes SCEP o las solicitudes específicas.
- **crypto pki server *cs-label* reject { all | *tranaction-id* }** : rechaza todas las solicitudes SCEP o las solicitudes específicas.
- **crypto pki server cs-label password genera [*minutos*]** —Genera una contraseña de una sola vez (OTP) para una solicitud SCEP (minutos - tiempo (en minutos) de que la contraseña es válida. El intervalo válido es de 1 a 1440 minutos. El valor predeterminado es 60 minutos.**Nota:** Sólo un OTP es válido a la vez. Si se genera un segundo OTP, el OTP anterior ya no es válido.
- **crypto pki server *cs-label* revoke *certificate-serial-number*** —Devuelve un certificado basado en su número de serie.
- **crypto pki server *cs-label* request *pkcs10* {url *url* | *terminal*} [pem]**: agrega manualmente la solicitud de inscripción de certificados de base64 o PEM PKCS10 a la base de datos de solicitudes.
- **crypto pki server *cs-label* info crl*: muestra información relacionada con el estado de la CRL actual.***
- **crypto pki server *cs-label* info request** —Muestra todas las solicitudes de inscripción de certificados pendientes.

Consulte la sección Verificar el Par de Llaves Generadas de este documento para obtener información de verificación adicional.

Troubleshoot

Refiérase a Troubleshooting de Seguridad IP - Comprensión y Uso de los Comandos debug para obtener información de troubleshooting.

Nota: En muchas situaciones, puede resolver los problemas al eliminar y redefinir el servidor de la CA.

Información Relacionada

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