Configurar e inscrever um roteador Cisco IOS em outro roteador Cisco IOS configurado como servidor CA

Contents

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Diagrama de Rede](#)
[Conventions](#)
[Gerar e exportar o par de chaves RSA para o servidor de certificados](#)
[Exportar o par de chaves gerado](#)
[Verificar o par de chaves gerado](#)
[Ative o servidor HTTP no roteador](#)
[Habilitar e configurar o servidor CA no roteador](#)
[Configurar e registrar o segundo roteador IOS (R2) no servidor de certificados](#)
[Verificar](#)
[Troubleshooting](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar um roteador Cisco IOS® como um servidor de Autoridade de Certificação (CA). Além disso, ele ilustra como inscrever outro roteador Cisco IOS para obter um certificado raiz e de ID para autenticação IPsec do servidor CA.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Dois Cisco 2600 Series Routers com Cisco IOS Software Release 12.3(4)T3.

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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Gerar e exportar o par de chaves RSA para o servidor de certificados

A primeira etapa é gerar o par de chaves RSA que o servidor de CA do Cisco IOS usa. No roteador (R1), gere as chaves RSA conforme mostrado nesta saída:

<#root>

```
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
```

Observação: você deve usar o mesmo nome para o par de chaves (key-label) que planeja usar para o servidor de certificado (através do comando crypto pki server cs-label abordado posteriormente).

Exportar o par de chaves gerado

Exporte as chaves para a RAM não volátil (NVRAM) ou TFTP (com base na sua configuração). Neste exemplo, a NVRAM é usada. Com base na sua implementação, talvez você queira usar um servidor TFTP separado para armazenar suas informações de certificado.

<#root>

```
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)#
```

Se você usar um servidor TFTP, poderá reimportar o par de chaves gerado, como mostra este comando:

<#root>

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

Observação: se você não quiser que a chave seja exportável do servidor de certificados, importe-a de volta para o servidor de certificados depois que ela tiver sido exportada como um par de chaves não exportável. Desta forma, a chave não pode ser tirada novamente.

Verificar o par de chaves gerado

Execute o comando show crypto key mypubkey rsa para verificar o par de chaves gerado.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

<#root>

```
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
```

Ative o servidor HTTP no roteador

O Cisco IOS CA Server suporta apenas inscrições feitas através do protocolo SCEP (Simple Certificate Enrollment Protocol). Consequentemente, para tornar isso possível, o roteador deve executar o servidor Cisco IOS HTTP integrado. Use o comando ip http server para ativá-lo:

```
<#root>

R1(config)#
ip http server
```

Habilitar e configurar o servidor CA no roteador

Conclua estes passos:

1. É muito importante lembrar que o servidor certificado deve usar o mesmo nome do par de chaves que você acabou de gerar manualmente.

O rótulo corresponde ao rótulo do par de chaves gerado:

<#root>

```
R1(config)#
```

crypto pki server cisco1

Depois de ativar um servidor certificado, você pode usar os valores padrão pré-configurados ou especificar valores via CLI para a funcionalidade do servidor certificado.

2. O comando database url especifica o local onde todas as entradas do banco de dados para o servidor de autoridade de certificação são gravadas. Se esse comando não for especificado, todas as entradas do banco de dados serão gravadas na Flash.

<#root>

```
R1(cs-server)#
```

database url nvram:

Observação: se você usar um servidor TFTP, o URL deverá ser tftp://<ip_address>/diretory.

3. Configure o nível do banco de dados:

<#root>

```
R1(cs-server)#
```

database level minimum

Este comando controla que tipo de dados é armazenado no banco de dados de registro de certificado:

- Mínimo — São armazenadas informações suficientes apenas para continuar a emitir novos certificados sem conflito. O valor padrão.
- Nomes — Além das informações fornecidas no nível mínimo, o número de série e o nome do assunto de cada certificado.
- Completo — Além das informações fornecidas nos níveis mínimo e de nomes, cada certificado emitido é gravado no banco de dados.

Observação: a palavra-chave complete produz uma grande quantidade de informações. Se for emitido, você também deverá especificar um servidor TFTP externo no qual armazenar

os dados através do comando database url.

4. Configure o nome do emissor da autoridade de certificação para a cadeia de caracteres DN especificada. Neste exemplo, o CN (Nome comum) de cisco1.cisco.com, L (Localidade) de RTP e C (País) de US são usados:

```
<#root>

R1(cs-server)#

issuer-name CN=cisco1.cisco.com L=RTP C=US
```

5. Especifique o tempo de vida, em dias, de um certificado de autoridade de certificação ou de um certificado.

   Os valores válidos variam de 1 dia a 1825 dias. O tempo de vida padrão do certificado de CA é de três anos e o padrão é de um ano. O tempo de vida máximo do certificado é um mês menor do que o tempo de vida do certificado da autoridade de certificação. Por exemplo:

```
<#root>

R1(cs-server)#

lifetime ca-certificate 365

R1(cs-server)#

lifetime certificate 200
```

6. Defina o tempo de vida, em horas, da CRL usada pelo servidor de certificado. O valor máximo do tempo de vida é 336 horas (duas semanas). O valor padrão é 168 horas (uma semana).

```
<#root>

R1(cs-server)#

lifetime crl 24
```

7. Defina um CDP (Ponto de Distribuição de Lista de Revogação de Certificados) para usar nos certificados emitidos pelo servidor de certificados.

   A URL deve ser uma URL HTTP. Por exemplo, nosso servidor tinha um endereço IP

172.18.108.26:

```
<#root>
R1(cs-server)#
cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
```

8. Execute o comando no shutdown para habilitar o servidor CA:

```
<#root>
R1(cs-server)#
no shutdown
```

Observação: emita este comando somente depois de ter configurado completamente o servidor de certificado.

Configurar e registrar o segundo roteador IOS (R2) no servidor de certificados

Siga este procedimento.

1. Configure um nome de host, um nome de domínio e gere as chaves RSA em R2.

   Use o comando hostname para configurar o nome de host do roteador para ser R2:

```
<#root>
Router(config)#
hostname R2
R2(config)#
```

   Observe que o nome de host do roteador mudou imediatamente depois que você inseriu o comando hostname.

   Use o comando ip domain-name para configurar o nome de domínio no roteador:

```
<#root>
R2(config)#
```

```
ip domain-name cisco.com
```

Use o comando crypto key generate rsa para gerar o par de chaves R2:

<#root>

```
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. Use estes comandos no modo de configuração global para declarar à CA que o roteador deve usar (CA do Cisco IOS neste exemplo) e especificar características para a CA do ponto de confiança:

<#root>

```
crypto ca trustpoint cisco


enrollment retry count 5


enrollment retry period 3



enrollment url http://14.38.99.99:80



revocation-check none
```

Observação: o comando crypto ca trustpoint unifica os comandos crypto ca identity e crypto ca trusted-root existentes, fornecendo assim a funcionalidade combinada sob um único comando.

3. Use o comando crypto ca authenticate cisco (cisco é o rótulo do ponto confiável) para recuperar o certificado raiz do servidor de CA:

<#root>

R2(config)#

crypto ca authenticate cisco

4. Use o comando crypto ca enroll cisco (cisco é o rótulo do ponto confiável) para registrar e gerar:

<#root>

R2(config)#

crypto ca enroll cisco

Depois de se inscrever com êxito no servidor de CA do Cisco IOS, você deve ver os certificados emitidos usando o comando show crypto ca certificates. Esta é a saída do comando. O comando exibe as informações detalhadas do certificado, que correspondem aos parâmetros configurados no servidor Cisco IOS CA:

<#root>

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. Insira este comando para salvar a chave na memória Flash persistente:

```
<#root>

hostname(config)#

write memory
```

6. Insira este comando para salvar a configuração:

```
<#root>

hostname#

copy run start
```

Verificar

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

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- show crypto ca certificates — Exibe os certificados.
- show crypto key mypubkey rsa — Exibe o par de chaves.

```
!% 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 — Exibe a lista de revogação de certificado (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 — exibe solicitações de inscrição pendentes.

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

- show crypto pki server — Exibe o estado atual do servidor da infraestrutura de chave 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 as solicitações SCEP ou solicitações específicas.
- crypto pki server cs-label reject { all | tranaction-id } — Rejeita todas as solicitações SCEP ou as específicas.
- crypto pki server cs-label password generate [minutes]—Gera uma senha única (OTP) para uma solicitação SCEP (minutos - duração do tempo (em minutos) em que a senha é válida. O intervalo válido é de 1 a 1440 minutos. O padrão é 60 minutos.

  Observação: apenas um OTP é válido por vez. Se um segundo OTP for gerado, o OTP anterior não será mais válido.
- crypto pki server cs-label revoke certificate-serial-number — Revoga um certificado com base em seu número de série.
- crypto pki server cs-label request pkcs10 {url url | terminal} [pem] — Adiciona manualmente a solicitação de registro de certificado de base64 ou PEM PKCS10 ao banco de dados de solicitações.
- crypto pki server cs-label info crl — Exibe informações sobre o status da CRL atual.
- crypto pki server cs-label info request — Exibe todas as solicitações pendentes de registro de certificado.

Consulte a seção Verificação do Par de Chaves Gerado deste documento para obter informações de verificação adicionais.

Troubleshooting

Consulte Troubleshooting de Segurança IP - Entendendo e Utilizando Comandos debug para obter informações sobre Troubleshooting.

Observação: em muitas situações, você pode resolver os problemas ao excluir e redefinir o servidor CA.

Informações Relacionadas

- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.