Configurar e registre um roteador do Cisco IOS a um outro roteador do Cisco IOS configurado como um server de CA

Índice

Introdução

Este documento descreve como configurar um roteador de Cisco IOS® como um server do Certificate Authority (CA). Adicionalmente, ilustra como registrar um outro roteador do Cisco IOS para obter uma raiz e o certificado ID para a autenticação IPSec do server de 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 Router que executam o 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:

Convenções

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

Gerencia e exporte o par de chaves RSA para o servidor certificado

A primeira etapa é gerar o par de chaves RSA que o server de CA do Cisco IOS usa. No roteador (r1), gerencia as chaves RSA como esta saída mostra:

```
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: Você deve usar o mesmo nome para o par de chaves (chave-*etiqueta*) esse você plano para usar-se para o servidor certificado (através do comando **cripto do** *rótulo CS do* **server do pki** coberto mais tarde).

Exporte o par de chaves gerado

Exporte as chaves para o RAM não-volátil (NVRAM) ou o TFTP (baseado em sua configuração). Neste exemplo, o NVRAM é usado. Baseado em sua aplicação, você pôde querer usar um servidor TFTP separado a fim armazenar sua informação do 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)#
```

Se você usa um servidor TFTP, você pode re-importação o par de chaves gerado enquanto este

comando mostra:

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

Nota: Se você não quer a chave ser exportable de seu servidor certificado, importe-o de volta ao servidor certificado depois que foi exportado como um par de chaves NON-exportable. Esta maneira, a chave não pode ser decolada outra vez.

Verifique o par de chaves gerado

Emita o **comando show crypto key mypubkey rsa** a fim verificar o par de chaves gerado.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do 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
```

Permita o Server do HTTP no roteador

O server de CA do Cisco IOS apoia somente os registros feitos através do protocolo simple certificate enrollment (SCEP). Consequentemente, a fim fazer este possível, o roteador deve executar o Server do HTTP incorporado do Cisco IOS. Use o **comando ip http server** a fim permiti-lo:

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

Permita e configurar o server de CA no roteador

Conclua estes passos:

1. Émuito importante recordar que o servidor certificado deve usar o mesmo nome que o par de chaves você apenas gerou manualmente.A etiqueta combina a etiqueta gerada do par de chaves:`R1(config)#crypto pki server cisco1` Depois que você permitiu um servidor certificado, você pode usar os valores padrão preconfigured ou especificar valores através do CLI para a funcionalidade do servidor certificado.
2. **O comando url do base de dados** especifica o lugar onde todas as entradas no base de dados para o server de CA são escritas para fora. Se este comando não é especificado, todas as entradas no base de dados estão escritas para piscar.`R1(cs-server)#database url nvram:` **Nota:** Se você usa um servidor TFTP, a URL precisa de ser **tftp://<ip_address>/directory**.
3. Configurar o nível do base de dados:`R1(cs-server)#database level minimum` Este controles de comando que tipo de dados é armazenado no base de dados do certificado de registro:**Mínimo** — Bastante informação é armazenada para continuar somente a emitir Certificados novos sem conflito. O valor padrão.**Nomes** — Além do que a informação dada

no nível mínimo, no número de série e no nome do sujeito de cada certificado.**Termine** — Além do que a informação dada nos níveis mínimos e dos nomes, cada certificado emitido é redigido ao base de dados.**Nota:** A palavra-chave **completa** produz uma grande quantidade de informação. Se é emitida, você deve igualmente especificar um servidor TFTP externo em que para armazenar os dados através do **comando url do base de dados**.

4. Configurar o nome de emissor de CA à DN-corda especificada. Neste exemplo, o CN (Common Name) de cisco1.cisco.com, L (localidade) do RTP, e o C (país) dos E.U. são usados:`R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US`
5. Especifique a vida, nos dias, de um certificado de CA ou de um certificado.Os valores válidos variam de *1 dia a 1825 dias*. A vida do certificado de CA do padrão é três anos e a vida do certificado do padrão é um ano. A duração máxima de certificado é *um mês menos* do que a vida do certificado de CA. Por exemplo:`R1(cs-server)#lifetime ca-certificate 365`
`R1(cs-server)#lifetime certificate 200`
6. Defina a vida, nas horas, do CRL que é usado pelo servidor certificado. O valor máximo da vida é **336 horas** (duas semanas). O valor padrão é **168 horas** (uma semana).`R1(cs-server)#lifetime crl 24`
7. Defina um ponto de distribuição da Lista de revogação de certificado (CDP) para usar-se nos Certificados que são emitidos pelo servidor certificado.A URL deve ser um URL DO HTTP. Por exemplo, nosso server teve um endereço IP de Um ou Mais Servidores Cisco ICM NT de 172.18.108.26:`R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl`
8. Emita o **comando no shutdown** a fim permitir o server de CA:`R1(cs-server)#no shutdown`
Nota: Emita este comando somente depois que você configurou completamente seu servidor certificado.

Configurar e registre o segundo IOS Router (R2) ao servidor certificado

Siga este procedimento.

1. Configurar um hostname, um Domain Name, e gerencia as chaves RSA no R2.Use o **comando hostname** a fim configurar o hostname do roteador para ser R2:`Router(config)#hostname R2 R2(config)#` Observe que o hostname do roteador mudado imediatamente depois que você inscreveu o **comando hostname**.Use o **comando ip domain-name** a fim configurar o Domain Name no roteador:`R2(config)#ip domain-name cisco.com` Use o **comando crypto key generate rsa** a fim gerar o par de chaves 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. Use estes comandos no modo de configuração global a fim declarar a CA que seu roteador deve usar (Cisco IOS CA neste exemplo) e especificar características para o ponto confiável 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: O comando crypto ca trustpoint** unifica o **comando crypto ca identity** e o **comando crypto ca trusted-root** existentes, fornecendo desse modo a funcionalidade combinada sob um comando único.
3. Use o **Ca cripto autenticam o comando cisco** (Cisco é a etiqueta do ponto confiável) a fim recuperar o certificado de raiz do server de CA:`R2(config)#crypto ca authenticate cisco`
4. Use o **Ca cripto registram o comando cisco** (Cisco é a etiqueta do ponto confiável) a fim

registrar-se e gerar:`R2(config)#crypto ca enroll cisco` Após com sucesso ter registrado a CA do Cisco IOS o server, você deve ver os Certificados emitidos usando o comando show crypto ca certificates. Esta é a saída do comando. O comando indica a informação detalhada do certificado, que correspondem com os parâmetros configurados no server de CA do 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. Incorpore este comando a fim salvar a chave à memória Flash persistente:`hostname(config)#write memory`
6. Incorpore este comando a fim salvar a configuração:`hostname#copy run start`

Verificar

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

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

- **mostre Certificados Ca criptos** — Indica Certificados.
- **rsa do mypubkey do show crypto key** — Indica 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
```
- **crl cripto da informação do server ESE-IO-Ca do pki** — Indica o Certificate Revocation List (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
```
- **pedidos criptos da informação do server ESE-IO-Ca do pki** — Pedidos pendentes do registro dos indicadores.
```
! Enrollment Request Database:
  ! ReqID  State      Fingerprint                      SubjectName
  ! --------------------------------------------------------------
```

- **mostre o server cripto do pki** — Indica o estado do servidor atual do 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
```
- **concessão cripto do** *rótulo CS do* **server do pki {tudo |** *a transação - identificação***}** — concede tudo ou pedidos específicos SCEP.
- **rejeição cripto do** *rótulo CS do* **server do pki {tudo |** *a transação - identificação***}** — rejeita tudo ou pedidos específicos SCEP.
- **a senha cripto do rótulo CS do server do pki gerencie o [minutes]** — gerencie uma senha de uma vez (OTP) para um pedido SCEP (minutos - o intervalo de tempo (nos minutos) que a senha é válida. O intervalo válido é 1 a 1440 minutos. O padrão é 60 minutos.**Nota:** Somente um OTP é válido em um momento. Se um segundo OTP é gerado, o OTP precedente é já não válido.
- *o rótulo CS* **cripto do server do pki revoga o** *número de série do certificado* — Revoga um certificado baseado em seu número de série.
- **pedido cripto** *pkcs10 do rótulo CS do* **server do pki {URL** *URL* **| [pem] do** *terminal***}** — adiciona manualmente o pedido base64 ou de certificado de registro PEM PKCS10 ao base de dados do pedido.
- **crl cripto da informação do** *rótulo CS do* **server do pki** — Indica a informação em relação ao estado do CRL atual.
- **pedido cripto da informação do** *rótulo CS do* **server do pki** — Indica todos os pedidos proeminentes do certificado de registro.

Veja a verificação a seção gerada do par de chaves deste documento para a informação de verificação adicional.

Troubleshooting

Refira o Troubleshooting de Segurança IP - Compreendendo e usando comandos debug para a informação de Troubleshooting.

Nota: Em muitas situações, você pode resolver os problemas quando você suprime e redefine do server de CA.

Informações Relacionadas

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