Índice

Introdução

Este documento fornece uma configuração de exemplo para o LAN dinâmico a LAN VPN entre o Roteadores do ® do Cisco IOS que usa Certificados digitais ao utilizar a característica do Certificate Authority (CA) IO. Este documento demonstra como configurar o servidor IOS CA e um roteador Cisco IOS para obter um certificado de identidade através do registro automático.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco 2851 Router que executa o Software Cisco IOS versão 12.4(6)T
- Cisco 871 Router que executa o Cisco IOS Software Release 12.3(14)YT1

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.

Convenções

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

Configurar

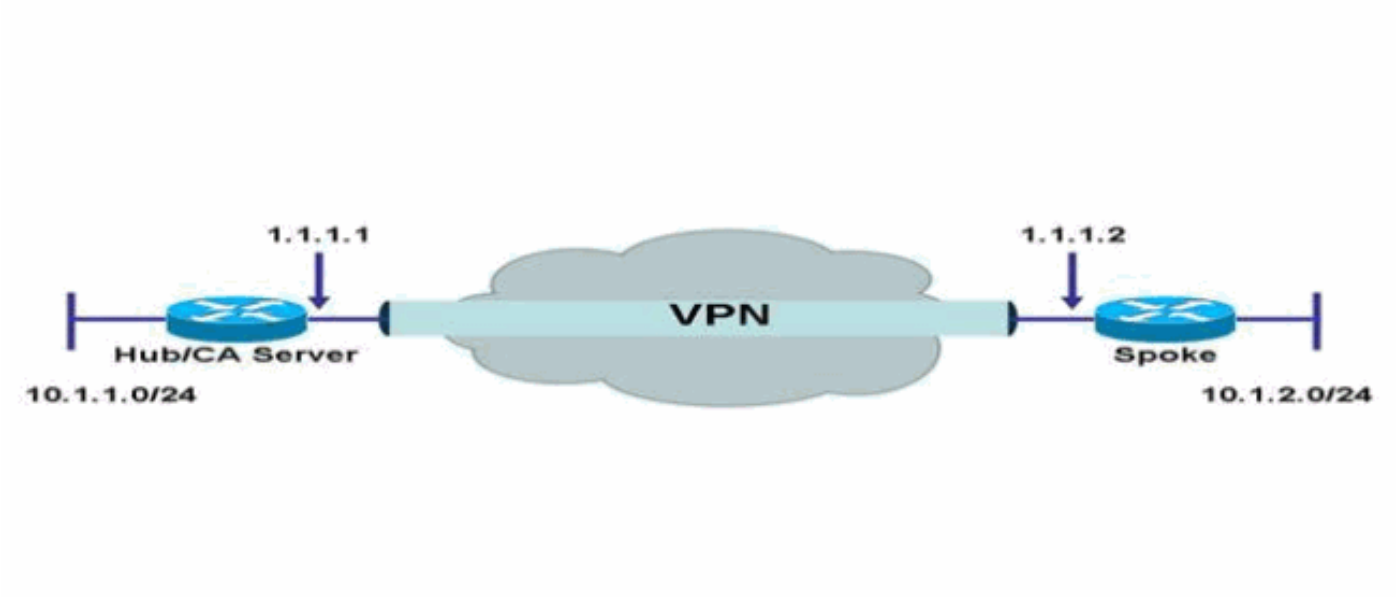
Nesta seção, você encontrará informações para configurar os recursos descritos neste

documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- Configurar o server IO CA no roteador
- Autentique e registre a IO CA um server
- Configuração do hub
- Configuração de raio

Configurar o server IO CA no roteador

Termine estas etapas a fim configurar o server IO CA no roteador:

1. Emita o **comando server cripto do pki** a fim incorporar os parâmetros para a configuração do servidor IO CA.Neste caso, a etiqueta que é dada à configuração do servidor IO CA é **Cisco**. A etiqueta pode ser qualquer coisa que você gostaria.`HubIOSCA(config)#crypto pki server cisco`
2. Emita o subcommand do **nome de emissor** a fim definir a informação do certificado.Neste caso, o Common Name (CN), localidade (L), o estado (ST), e o código de país (c) são definidos como mostrado aqui:`HubIOSCA(cs-server)#issuer-name CN=iosca.cisco.com L=RTP ST=NC C=US`
3. Emita o comando da **concessão**.Neste caso, o servidor de IOS concede automaticamente um certificado ao cliente.`HubIOSCA(cs-server)#grant auto`
4. Emita o **comando no shut** a fim permitir o server IO CA.`HubIOSCA(cs-server)#no shut`Depois que você incorpora este comando, você está alertado entrar em uma frase de passagem para proteger a chave privada.Algumas configurações de servidor não podem ser mudadas após

a geração do certificado de CA. Entre em uma frase de passagem para proteger a chave privada ou para incorporar o **retorno à** saída.`HubIOSCA(cs-server)#`**`no shut`**

Autentique e registre a IO CA um server

O servidor certificado igualmente tem um ponto confiável automaticamente gerado do mesmo nome. O ponto confiável armazena o certificado do servidor certificado. Depois que o roteador detecta que um ponto confiável está sendo usado para armazenar o certificado do servidor certificado, o ponto confiável trava de modo que não possa ser alterado.

1. Antes que você configure o servidor certificado, você pode emitir o comando **cripto do ponto confiável do pki** a fim criar e estabelecer manualmente este ponto confiável.Isto permite que você especifique um par de chaves da alternativa RSA (que usa o comando do **rsakeypair**).**Nota:** O ponto confiável automaticamente gerado e o certificado de servidor certificado não estão disponíveis para a identidade do dispositivo do servidor certificado. Consequentemente, todo o comando line interface(cli), tal como o comando do seguro-**ponto confiável do HTTP de IP**, que é usado para especificar o ponto confiável de CA para obter Certificados e autenticar o certificado de conexão do cliente deve apontar a um ponto confiável adicional configurado no dispositivo do servidor certificado.Se o server é um server do certificado de raiz, usa os pares de chaves RSA e diversos outros atributos para gerar um certificado auto-assinado. O certificado de CA associado manda estes fechar Ramais do uso:Assinatura digitalSinal do certificadoSinal do Certificate Revocation List (CRL)Neste caso, o roteador de HubIOSCA é registrado com um certificado usando um ponto confiável diferente a fim poder estabelecer um túnel VPN com o roteador do spoke. Defina um ponto confiável, como mostrado aqui (o iosca é o nome dado a este ponto confiável novo):`HubIOSCA(config)#`**`crypto pki trustpoint iosca`**
2. Incorpore o registro URL, como mostrado aqui:`HubIOSCA(ca-trustpoint)#`**`enrollment url http://1.1.1.1:80`**Neste caso, uma verificação da revogação CRL não é feita.`HubIOSCA(ca-trustpoint)#`**`revocation-check none`**
3. Emita o **Ca cripto autenticam o** comando do **iosca** a fim receber o certificado de raiz.`HubIOSCA(config)#`**`crypto ca authenticate iosca`**O certificado tem estes atributos:`Fingerprint MD5: 441446A1 CA3C32B6 3B680204 452A00B2 Fingerprint SHA1: 6C09E064 E4B09087 DDFFADCD 2E9C6853 1669BF39Do you accept this certificate? [yes/no]: `**`yes`**`Trustpoint CA certificate accepted.`
4. Emita o **Ca cripto registram o** comando do **iosca** a fim obter o certificado de identidade.`Start certificate enrollment... Create a challenge password. You need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons, your password is not saved in the configuration. Please make a note of it.Password:Re-enter password: The subject name in the certificate includes: HubIOSCA.cisco.com Include the router serial number in the subject name? [yes/no]: `**`no`**` Include an IP address in the subject name? [no]: `**`no`**` Request certificate from CA? [yes/no]: `**`yes`**` Certificate request sent to Certificate Authority The `**`show crypto ca certificate iosca verbose`**` command shows the fingerprint.`
5. Emita o comando **cripto CERT do pki da mostra** a fim verificar que os Certificados estiveram instalados.`HubIOSCA#`**`show crypto pki cert`**`Certificate Status: Available Certificate Serial Number: 02 Certificate Usage: General Purpose Issuer: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Subject: Name: HubIOSCA.cisco.com hostname=HubIOSCA.cisco.com Validity Date: start date: 19:11:55 UTC Aug 11 2006 end date: 19:11:55 UTC Aug 11 2007 Associated Trustpoints: iosca CA Certificate Status: Available Certificate Serial Number: 01 Certificate Usage: Signature Issuer: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Subject: cn=iosca.cisco.com L\=RTP ST\=NC C\=US Validity Date: start date: 19:01:54 UTC Aug 11 2006 end date: 19:01:54 UTC Aug 10 2009 Associated Trustpoints: iosca cisco`**Nota:** Porque o server de CA é igualmente um ipsec peer, o roteador de hub precisa de autenticar e registrar a CA o server que está no mesmo roteador.

Configuração do hub

Configuração do hub

```
HubIOSCA#show crypto pki certCertificate  Status: Available
Certificate Serial Number: 02  Certificate Usage: General
Purpose  Issuer:    cn=iosca.cisco.com L\=RTP ST\=NC C\=US
Subject:    Name: HubIOSCA.cisco.com
hostname=HubIOSCA.cisco.com  Validity Date:    start date:
19:11:55 UTC Aug 11 2006    end   date: 19:11:55 UTC Aug 11
2007  Associated Trustpoints: iosca CA Certificate  Status:
Available  Certificate Serial Number: 01  Certificate Usage:
Signature  Issuer:    cn=iosca.cisco.com L\=RTP ST\=NC C\=US
Subject:    cn=iosca.cisco.com L\=RTP ST\=NC C\=US  Validity
Date:    start date: 19:01:54 UTC Aug 11 2006    end   date:
19:01:54 UTC Aug 10 2009  Associated Trustpoints: iosca cisco
```

Configuração de raio

Configuração de raio

```
HubIOSCA#show crypto pki certCertificate  Status: Available
Certificate Serial Number: 02  Certificate Usage: General
Purpose  Issuer:    cn=iosca.cisco.com L\=RTP ST\=NC C\=US
Subject:    Name: HubIOSCA.cisco.com
hostname=HubIOSCA.cisco.com  Validity Date:    start date:
19:11:55 UTC Aug 11 2006    end   date: 19:11:55 UTC Aug 11
2007  Associated Trustpoints: iosca CA Certificate  Status:
Available  Certificate Serial Number: 01  Certificate Usage:
Signature  Issuer:    cn=iosca.cisco.com L\=RTP ST\=NC C\=US
Subject:    cn=iosca.cisco.com L\=RTP ST\=NC C\=US  Validity
Date:    start date: 19:01:54 UTC Aug 11 2006    end   date:
19:01:54 UTC Aug 10 2009  Associated Trustpoints: iosca cisco
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

O certificado de autenticação falha para um túnel L2L.

Às vezes, a negociação de IPSec pode falhar quando você usa um certificado de CA válido para a autenticação de ISAKMP. A negociação do túnel VPN trabalha com chaves pré-compartilhada porque as chaves pré-compartilhada são pacotes realmente pequenos. Se o certificado de autenticação precisa de enviar transversalmente o certificado inteiro, este cria pacotes grandes que obtém fragmentado. A fragmentação impede o certificado a ser autenticada corretamente entre os dispositivos.

Abaixe o MTU e comute-o FULL-frente e verso a fim resolver este problema. Ajuste o valor MTU a um tamanho que não tenha que ser fragmentado:

```
Router(config)#interface type [slot_#/]port_#Router(config-if)#ip mtu MTU_size_in_bytes
```

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems