

Profissional da configuração: IPSec local a local VPN entre um exemplo de configuração de dois IOS Router

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configuração](#)

[Diagrama de Rede](#)

[Roteador uma configuração de Cisco CP](#)

[Configuração do roteador B Cisco CP](#)

[Configuração de CLI do roteador B](#)

[Verificar](#)

[IOS Router - comandos show](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento fornece uma configuração de exemplo para o túnel de IPsec do LAN para LAN (site para site) entre dois Roteadores do ^{® do} Cisco IOS que usam o [Cisco Configuration Professional \(Cisco CP\)](#). As rotas estáticas são usadas por simplicidade.

[Pré-requisitos](#)

[Requisitos](#)

Certifique-se de que você cumpre esta exigência antes que você tente esta configuração:

- A conectividade IP fim-a-fim deve ser estabelecida antes de começar esta configuração.

[Componentes Utilizados](#)

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

- Cisco 1841 Router com Cisco IOS Software Release 12.4(15T)

- Versão 2.5 de Cisco CP

Note: Refira a [configuração de roteador básico usando o Cisco Configuration Professional](#) a fim permitir que o roteador seja configurado por Cisco CP.

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.

Configuração

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Note: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do [RFC 1918](#), que foram usados em um ambiente de laboratório.

- [Roteador uma configuração de Cisco CP](#)
- [Configuração do roteador B Cisco CP](#)
- [Configuração de CLI do roteador B](#)

Roteador uma configuração de Cisco CP

Execute estas etapas a fim configurar o túnel do VPN de Site-para-Site no roteador do Cisco IOS:

1. Escolha **configuram o > segurança > o VPN > o VPN de Site-para-Site**, e clicam o botão de rádio ao lado de **criam um VPN de Site-para-Site**. Clique o **lançamento a tarefa selecionada**.
2. Escolha o **assistente passo a passo** a fim continuar com a configuração, e clique-o **em seguida**.
3. Na próxima janela, forneça a informação da conexão de VPN nos espaços respectivos. Escolha a relação do túnel VPN do menu suspenso. Aqui, **FastEthernet0** é escolhido. Na seção da identidade do par, escolha o **par com endereço IP estático** e forneça o endereço IP de Um ou Mais Servidores Cisco ICM NT do peer remoto. Então, forneça as chaves pré-compartilhada (*cisco123* neste exemplo) na seção da autenticação. Ultimamente, clique **em seguida**.
4. O clique **adiciona** a fim adicionar as propostas IKE que especificam o algoritmo de criptografia, o algoritmo de autenticação, e o método das trocas de chave.
5. Forneça o método do algoritmo de criptografia, do algoritmo de autenticação, e das trocas de chave, e clique então a **APROVAÇÃO**. O algoritmo de criptografia, o algoritmo de autenticação, e os valores do método das trocas de chave devem combinar com os dados a ser fornecidos no roteador B.

6. Clique em Next.
7. Nesta nova janela, os detalhes ajustados da transformação são fornecidos. O grupo da transformação especifica a criptografia e os algoritmos de autenticação usados para proteger dados no VPN escavam um túnel. O clique **adiciona** a fim fornecer estes detalhes. Você pode adicionar todo o número de grupos Transform como necessário usando este método.
8. Forneça os detalhes ajustados da transformação (integridade e algoritmos de criptografia), e clique a **APROVAÇÃO**.
9. Escolha exigido **transformam o grupo** a ser usado do menu suspenso, e clicam-no **em seguida**.
10. No seguinte indicador, forneça os detalhes sobre o tráfego a ser protegido através do túnel VPN. Forneça a fonte e as redes de destino do tráfego a ser protegido de modo que o tráfego entre a fonte e as redes de destino especificadas seja protegido. Neste exemplo, a rede da fonte é *10.10.10.0* e a rede de destino é *10.20.10.0*. Clique em Next.
11. **Revestimento do** clique na próxima janela para terminar a configuração no roteador A.

Configuração do roteador B Cisco CP

Execute estas etapas a fim configurar o túnel do VPN de Site-para-Site no roteador do Cisco IOS (roteador B):

1. Escolha **configuram o > segurança > o VPN > o VPN de Site-para-Site**, e clicam o botão de rádio ao lado de **criam um VPN de Site-para-Site**. Clique o **lançamento a tarefa selecionada**.
2. Escolha o **assistente passo a passo** a fim continuar com a configuração, e clique-o **em seguida**.
3. Na próxima janela, forneça a informação da conexão de VPN nos espaços respectivos. Escolha a relação do túnel VPN do menu suspenso. Aqui, **FastEthernet0** é escolhido. Na seção da identidade do par, escolha o **par com endereço IP estático** e forneça o endereço IP de Um ou Mais Servidores Cisco ICM NT do peer remoto. Então, forneça as chaves pré-compartilhada (*cisco123* neste exemplo) na seção da autenticação. Ultimamente, clique **em seguida**.
4. O clique **adiciona** a fim adicionar as propostas IKE que especificam o algoritmo de criptografia, o algoritmo de autenticação, e o método das trocas de chave.
5. Forneça o método do algoritmo de criptografia, do algoritmo de autenticação, e das trocas de chave, e clique então a **APROVAÇÃO**. O algoritmo de criptografia, o algoritmo de autenticação, e os valores do método das trocas de chave devem combinar com os dados fornecidos no roteador A.
6. Clique em Next.
7. Nesta nova janela, os detalhes ajustados da transformação são fornecidos. O grupo da transformação especifica a criptografia e os algoritmos de autenticação usados para proteger dados no VPN escavam um túnel. O clique **adiciona** a fim fornecer estes detalhes. Você pode adicionar todo o número de grupos Transform como necessário usando este método.
8. Forneça os detalhes ajustados da transformação (integridade e algoritmos de criptografia), e clique a **APROVAÇÃO**.
9. Escolha exigido **transformam o grupo** a ser usado do menu suspenso, e clicam-no **em seguida**.
10. No seguinte indicador, forneça os detalhes sobre o tráfego a ser protegido através do túnel

VPN. Forneça a fonte e as redes de destino do tráfego a ser protegido de modo que o tráfego entre a fonte e as redes de destino especificadas seja protegido. Neste exemplo, a rede da fonte é *10.20.10.0* e a rede de destino é *10.10.10.0*. Clique em Next.

11. Este indicador mostra o sumário da configuração do VPN de Site-para-Site. Verifique a **conectividade de VPN do teste após ter configurado** a caixa de seleção se você quer testar a conectividade de VPN. Aqui, a caixa é verificada enquanto a Conectividade precisa de ser verificada. Clique em Finish.
12. **Começo** do clique a fim verificar a conectividade de VPN.
13. Na próxima janela, o resultado do teste da conectividade de VPN é fornecido. Aqui, você pode ver se o túnel é para cima ou para baixo. Neste exemplo de configuração, o túnel está “acima de”, segundo as indicações do verde. Isto termina a configuração no roteadorB do Cisco IOS e mostra que o túnel está acima.

Configuração de CLI do roteador B

```
roteador B

Building configuration...

Current configuration : 2403 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7
1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!

!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
used during an IKE negotiation. Encryption and Policy
details are hidden !--- as the default values are
chosen. crypto isakmp policy 2
authentication pre-share

!--- Specifies the pre-shared key "cisco123" which
should !--- be identical at both peers. This is a global
!--- configuration mode command. crypto isakmp key
cisco123 address 172.16.1.1
```

```
!  
!  
!--- Configuration for IPsec policies. !--- Enables the  
crypto transform configuration mode, !--- where you can  
specify the transform sets that are used !--- during an  
IPsec negotiation. crypto ipsec transform-set Router-  
IPSEC esp-des esp-sha-hmac  
!  
  
!--- Indicates that IKE is used to establish !--- the  
IPsec Security Association for protecting the !---  
traffic specified by this crypto map entry. crypto map  
SDM_CMAP_1 1 ipsec-isakmp  
description Tunnel to172.16.1.1  
  
!--- Sets the IP address of the remote end. set peer  
172.16.1.1  
  
!--- Configures IPsec to use the transform-set !---  
"Router-IPSEC" defined earlier in this configuration.  
set transform-set Router-IPSEC  
  
!--- Specifies the interesting traffic to be encrypted.  
match address 100  
!  
!  
!  
!--- Configures the interface to use the !--- crypto map  
"SDM_CMAP_1" for IPsec. interface FastEthernet0 ip  
address 172.17.1.1 255.255.255.0 duplex auto speed auto  
crypto map SDM_CMAP_1  
!  
interface FastEthernet1  
ip address 10.20.10.2 255.255.255.0  
duplex auto  
speed auto  
!  
interface FastEthernet2  
no ip address  
!  
interface Vlan1  
ip address 10.77.241.109 255.255.255.192  
!  
ip classless  
ip route 10.10.10.0 255.255.255.0 172.17.1.2  
ip route 10.77.233.0 255.255.255.0 10.77.241.65  
ip route 172.16.1.0 255.255.255.0 172.17.1.2  
!  
!  
ip nat inside source route-map nonat interface  
FastEthernet0 overload  
!  
ip http server  
ip http authentication local  
ip http secure-server  
!  
!--- Configure the access-lists and map them to the  
Crypto map configured. access-list 100 remark SDM_ACL  
Category=4  
access-list 100 remark IPsec Rule  
access-list 100 permit ip 10.20.10.0 0.0.0.255  
10.10.10.0 0.0.0.255  
!  
!
```

```

!
!--- This ACL 110 identifies the traffic flows using
route map access-list 110 deny ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
  match ip address 110
!
control-plane
!
!
line con 0
  login local
line aux 0
line vty 0 4
  privilege level 15
  login local
  transport input telnet ssh
!
end

```

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.

- [IOS Router - comandos show](#)

IOS Router - comandos show

- **mostre isakmp cripto sa** — Mostra todo o IKE atual SA em um par.

```
RouterB# show crypto isakmp sa
```

dst	src	state	conn-id	slot	status
172.17.1.1	172.16.1.1	QM_IDLE	3	0	ACTIVE

- **mostre IPsec cripto sa** — Mostra todo o sas de IPsec atual em um par.

```
RouterB# show crypto ipsec sa
```

```
interface: FastEthernet0
```

```
  Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
```

```
current_peer 172.16.1.1 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
```

```
#pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
```

```
path mtu 1500, ip mtu 1500
```

```
current outbound spi: 0xB7C1948E(3082917006)
```

```
inbound esp sas:
spi: 0x434C4A7F(1129073279)
transform: esp-des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
sa timing: remaining key lifetime (k/sec): (4578719/3004)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0xB7C1948E(3082917006)
transform: esp-des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
sa timing: remaining key lifetime (k/sec): (4578719/3002)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

- **active do show crypto engine connections** — Conexões atual e informação das mostras sobre pacotes criptografado e descriptografado.

```
RouterB#show crypto engine connections active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
3	FastEthernet0	172.17.1.1	set	HMAC_SHA+DES_56_CB	0	0
2001	FastEthernet0	172.17.1.1	set	DES+SHA	0	59
2002	FastEthernet0	172.17.1.1	set	DES+SHA	59	0

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

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.

Note: Refira a [informação importante em comandos Debug](#) e em [Troubleshooting de Segurança IP: Compreendendo e usando comandos debug](#) antes que você usar **comandos debug**.

- **IPsec 7 do debug crypto** — Indica as negociações de IPSEC de fase 2.**isakmp 7 do debug crypto** — Indica as negociações de ISAKMP de fase 1.
- **IPsec do debug crypto** — Indica as negociações de IPSEC de fase 2.**isakmp do debug crypto** — Indica as negociações de ISAKMP de fase 1.

Informações Relacionadas

- [Guia de início rápido do Cisco Configuration Professional](#)

- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)