

Chave manual do IPsec entre o exemplo de configuração do Roteadores

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Grupos de transformação sem correspondência](#)

[ACLs não correspondem](#)

[Um lado tem o cripto mapa e o outro não tem](#)

[A placa aceleradora do mecanismo de criptografia mecanismo está habilitada](#)

[Informações Relacionadas](#)

[Introdução](#)

Esta configuração de exemplo permite que você criptografe o tráfego entre as redes 12.12.12.x e 14.14.14.x com a ajuda da chave manual do IPsec. Para fins de teste, foram usados uma Lista de controle de acesso (ACL) e um ping estendido a partir do host 12.12.12.12 para 14.14.14.14.

O chave manual é geralmente somente necessário quando um dispositivo Cisco é configurado para cifrar o tráfego ao dispositivo de um outro vendedor que não apoia o Internet Key Exchange (IKE). Se o IKE é configurável em ambos os dispositivos, é preferível usar fechar automático. Os deslocamentos predeterminados do parâmetro de segurança do dispositivo Cisco (SPI) estão no decimal contudo que alguns vendedores fazem SPI no hexadecimal. Se este é o caso, a seguir a conversão está precisada às vezes.

[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 3640 and 1605 routers
- Software Release 12.3.3.a de Cisco IOS®

Nota: Em todas as Plataformas que contêm adaptadores da criptografia de hardware, a criptografia manual não é apoiada quando o adaptador da criptografia de hardware é permitido.

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 sua rede está viva, certifique-se de que você compreende o impacto potencial do comando any antes que você o use.

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 ferramenta [Command Lookup Tool](#) ([apenas para clientes registrados](#)) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurações

Este documento utiliza as seguintes configurações:

- [Configuração leve](#)
- [Configuração doméstica](#)

Configuração leve

```
light#show running-config Building configuration...
Current configuration : 1177 bytes ! version 12.3
service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname light ! boot-start-marker boot-
end-marker ! enable password cisco ! no aaa new-model ip
subnet-zero ! no crypto isakmp enable ! !--- IPsec
configuration crypto ipsec transform-set encrypt-des
esp-des esp-sha-hmac ! ! crypto map testcase 8 ipsec-
manual set peer 11.11.11.12 set session-key inbound esp
1001 cipher 1234abcd1234abcd authenticator 20 set
session-key outbound esp 1000 cipher abcd1234abcd1234
authenticator 20 set transform-set encrypt-des !---
Traffic to encrypt match address 100 ! ! interface
Ethernet2/0 ip address 12.12.12.12 255.255.255.0 half-
```

```
duplex<br>! interface Ethernet2/1 ip address 11.11.11.11
255.255.255.0 half-duplex !--- Apply crypto map. crypto
map testcase ! ip http server no ip http secure-server
ip classless ip route 0.0.0.0 0.0.0.0 11.11.11.12 ! ! !-
-- Traffic to encrypt access-list 100 permit ip host
12.12.12.12 host 14.14.14.14 ! ! ! ! line con 0 line aux
0 line vty 0 4 login ! ! !
```

Configuração doméstica

```
house#show running-config Current configuration : 1194
bytes ! version 12.3 service timestamps debug uptime
service timestamps log uptime no service password-
encryption ! hostname house ! ! logging buffered 50000
debugging enable password cisco ! no aaa new-model ip
subnet-zero ip domain name cisco.com ! ip cef ! ! no
crypto isakmp enable ! ! !--- IPsec configuration crypto
ipsec transform-set encrypt-des esp-des esp-sha-hmac !
crypto map testcase 8 ipsec-manual set peer 11.11.11.11
set session-key inbound esp 1000 cipher abcd1234abcd1234
authenticator 20 set session-key outbound esp 1001
cipher 1234abcd1234abcd authenticator 20 set transform-
set encrypt-des !--- Traffic to encrypt match address
100 ! ! interface Ethernet0 ip address 11.11.11.12
255.255.255.0 !--- Apply crypto map. crypto map testcase
! interface Ethernet1 ip address 14.14.14.14
255.255.255.0 ! ip classless ip route 0.0.0.0 0.0.0.0
11.11.11.11 no ip http server no ip http secure-server !
! !--- Traffic to encrypt access-list 100 permit ip host
14.14.14.14 host 12.12.12.12 ! ! line con 0 exec-timeout
0 0 transport preferred none transport output none line
vty 0 4 exec-timeout 0 0 password cisco login transport
preferred none transport input none transport output
none ! ! end
```

Verificar

Esta seção fornece a informação que você pode se usar para confirmar corretamente suas funções da 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.

- **mostre IPsec cripto sa** — Mostra à fase duas associações de segurança.

Troubleshooting

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

Comandos para Troubleshooting

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.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos debug.

- **IPsec do debug crypto** — Indica as negociações de IPsec da fase dois.
- **debug crypto engine** — Exibe o tráfego que está criptografado.

Grupos de transformação sem correspondência

A luz tem o Ah-sha-hmac e a casa tem o ESP-DES.

```
*Mar  2 01:16:09.849: IPSEC(sa_request): ,
(key eng. msg.) OUTBOUND local= 11.11.11.11, remote= 11.11.11.12,
  local_proxy= 12.12.12.12/255.255.255.255/0/0 (type=1),
  remote_proxy= 14.14.14.14/255.255.255.255/0/0 (type=1),
  protocol= AH, transform= ah-sha-hmac ,
  lifedur= 3600s and 4608000kb,
  spi= 0xACD76816(2899798038), conn_id= 0, keysize= 0, flags= 0x400A
*Mar  2 01:16:09.849: IPSEC(manual_key_stuffing):
keys missing for addr 11.11.11.12/prot 51/spi 0.....
```

ACLs não correspondem

No side_A (o roteador "leve") há um host interno para host interno e no side_B (o roteador "base") há uma interface para interface. Os ACL devem sempre ser simétricos (estes não são).

```
hostname house
match address 101
access-list 101 permit ip host 11.11.11.12 host 11.11.11.11
!
```

```
hostname light
match address 100
access-list 100 permit ip host 12.12.12.12 host 14.14.14.14
```

Esta saída é tomada do side_A que inicia o sibilo:

```
nothing
```

```
light#show crypto engine connections active
ID Interface IP-Address State Algorithm Encrypt
Decrypt 2000 Ethernet2/1 11.11.11.11 set DES_56_CBC 5 0 2001 Ethernet2/1 11.11.11.11 set
DES_56_CBC 0 0
```

Esta saída é tomada do side_B quando o side_A está iniciando o sibilo:

```
house#
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
```

```
house#show crypto engine connections active
ID Interface IP-Address State Algorithm Encrypt
Decrypt 2000 Ethernet0 11.11.11.12 set DES_56_CBC 0 0 2001 Ethernet0 11.11.11.12 set DES_56_CBC
0 5
```

Esta saída é tomada do side_B que inicia o sibilo:

```
side_ B
```

```
%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet.
(ip) vrf/dest_addr= /12.12.12.12, src_addr= 14.14.14.14, prot= 1
```

Um lado tem o cripto mapa e o outro não tem

```
%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet.  
  (ip) vrf/dest_addr= /14.14.14.14, src_addr= 12.12.12.12, prot= 1
```

Esta saída é tomada do side_B que tem um crypto map:

```
house#show crypto engine connections active  
ID Interface      IP-Address      State  Algorithm      Encrypt  Decrypt  
2000 Ethernet0      11.11.11.12     set    DES_56_CBC      5        0  
2001 Ethernet0      11.11.11.12     set    DES_56_CBC      0        0
```

[A placa aceleradora do mecanismo de criptografia mecanismo está habilitada](#)

```
1d05h: %HW_VPN-1-HPRXERR: Hardware VPN0/13: Packet  
Encryption/Decryption error, status=4098.....
```

[Informações Relacionadas](#)

- [Negociação IPsec/Protocolos IKE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)