

Configurando IPSec - Cisco Secure VPN Client para acesso de controle do roteador central

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

A seguinte configuração não seria de uso geral, mas foi projetada permitir a terminação do túnel de IPsec do Cisco Secure VPN Client em um roteador central. Enquanto o túnel é ativado, o PC recebe seu endereço IP do conjunto de endereços IP do roteador central (no nosso exemplo, o roteador está nomeado como "moss"), então o tráfego do conjunto pode chegar à rede local por trás do moss ou ser roteado e criptografado para a rede por trás do roteador afastado (em nosso exemplo, o roteador está nomeado como "carter"). Além disso, o tráfego da rede privada 10.13.1.X a 10.1.1.X é criptografado; os roteadores estão executando a sobrecarga NAT.

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

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

- Liberação 12.1.5.T do Cisco IOS® Software (c3640-io3s56i-mz.121-5.T)
- Cisco Secure VPN Client 1.1

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](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

[Configurar](#)

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

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes [registrados](#)).

[Diagrama de Rede](#)

Este documento utiliza a seguinte configuração de rede:

[Configurações](#)

Este documento utiliza as seguintes configurações:

- [Configuração moss](#)
- [Configuração do carter](#)

Configuração moss

```
Version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname moss
!
logging rate-limit console 10 except errors
enable password ww
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1 hash md5 authentication pre-share
crypto isakmp key cisco123 address 99.99.99.1 crypto
isakmp key cisco123 address 0.0.0.0 0.0.0.0 crypto
isakmp client configuration address-pool local RTP-POOL
! crypto ipsec transform-set rtpset esp-des esp-md5-hmac
! crypto dynamic-map rtp-dynamic 20 set transform-set
rtpset ! crypto map rtp client configuration address
initiate crypto map rtp client configuration address
```

```

respond !crypto map sequence for network to network
traffic crypto map rtp 1 ipsec-isakmp set peer
99.99.99.1 set transform-set rtpset match address 115 !-
-- crypto map sequence for VPN Client network traffic.
crypto map rtp 10 ipsec-isakmp dynamic rtp-dynamic !
call rsvp-sync ! interface Ethernet2/0 ip address
172.18.124.154 255.255.255.0 ip nat outside no ip route-
cache no ip mroute-cache half-duplex crypto map rtp !
interface Serial2/0 no ip address shutdown ! interface
Ethernet2/1 ip address 10.13.1.19 255.255.255.0 ip nat
inside half-duplex ! ip local pool RTP-POOL 192.168.1.1
192.168.1.254 ip nat pool ETH20 172.18.124.154
172.18.124.154 netmask 255.255.255.0 ip nat inside
source route-map nonat pool ETH20 overload ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1 ip route 10.1.1.0
255.255.255.0 172.18.124.158 ip route 99.99.99.0
255.255.255.0 172.18.124.158 no ip http server ! !---
Exclude traffic from NAT process. access-list 110 deny
ip 10.13.1.0 0.0.0.255 10.1.1.0 0.0.0.255 access-list
110 deny ip 10.13.1.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 110 permit ip 10.13.1.0 0.0.0.255 any !---
Include traffic in encryption process. access-list 115
permit ip 10.13.1.0 0.0.0.255 10.1.1.0 0.0.0.255 access-
list 115 permit ip 192.168.1.0 0.0.0.255 10.1.1.0
0.0.0.255 route-map nonat permit 10 match ip address 110
! dial-peer cor custom ! line con 0 transport input none
line aux 0 line vty 0 4 login ! end

```

Configuração do carter

```

Current configuration : 2059 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname carter
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1 hash md5 authentication pre-share
crypto isakmp key cisco123 address 172.18.124.154 !
crypto ipsec transform-set rtpset esp-des esp-md5-hmac !
!--- crypto map sequence for network-to-network traffic.
crypto map rtp 1 ipsec-isakmp set peer 172.18.124.154
set transform-set rtpset match address 115 ! call rsvp-
sync ! interface Ethernet0/0 ip address 99.99.99.1
255.255.255.0 ip nat outside half-duplex crypto map rtp
! interface FastEthernet3/0 ip address 10.1.1.1
255.255.255.0 ip nat inside duplex auto speed 10 ! ip
nat pool ETH00 99.99.99.1 99.99.99.1 netmask
255.255.255.0 ip nat inside source route-map nonat pool
ETH00 overload ip classless ip route 0.0.0.0 0.0.0.0
99.99.99.2 no ip http server ! !--- Exclude traffic from
NAT process. access-list 110 deny ip 10.1.1.0 0.0.0.255
10.13.1.0 0.0.0.255 access-list 110 deny ip 10.1.1.0

```

```
0.0.0.255 192.168.1.0 0.0.0.255 access-list 110 permit
ip 10.1.1.0 0.0.0.255 any !--- Include traffic in
encryption process. access-list 115 permit ip 10.1.1.0
0.0.0.255 10.13.1.0 0.0.0.255 access-list 115 permit ip
10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255 route-map nonat
permit 10 match ip address 110 ! line con 0 transport
input none line aux 0 line vty 0 4 password ww login !
end
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- show crypto ipsec sa – Mostra as associações de segurança da fase 2.
- show crypto isakmp sa - Mostra as associações de segurança da fase 1.

Troubleshooting

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

Comandos para Troubleshooting

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Nota: [Antes de emitir comandos de depuração, consulte as informações importantes sobre eles.](#)

- **IPsec do debug crypto** — Mostra as negociações de IPSEC de fase 2.
- debug crypto ipsec - Exibe as negociações ISAKMP da fase 1.
- **motor do debug crypto** — Mostra o tráfego que é cifrado.
- clear crypto isakmp — Limpa as associações de segurança relacionadas à fase 1.
- clear crypto sa — Limpa as associações de segurança relacionadas à fase 2.

Informações Relacionadas

- [Configurando a segurança da rede IPsec](#)
- [Configurando o protocolo de segurança do intercâmbio chave de Internet](#)
- [Página de Suporte do Cisco VPN Client](#)
- [Página de suporte do IPsec](#)
- [Suporte Técnico - Cisco Systems](#)