Configurando o roteador para roteador IPSec com sobrecarga de NAT e Cisco Secure VPN Client

Contents

Introduction

Esta configuração de exemplo criptografa o tráfego da rede atrás da Luz até a rede atrás da Casa (192.168.100.x à rede 192.168.200.x). A sobrecarga da Tradução de Endereço de Rede (NAT) também é realizada. As conexões de Cliente de VPN Criptografadas são permitidas na Luz com caracteres gerais, chaves pré-compartilhada e mode-config. O tráfego à Internet é traduzido, mas não criptografado.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Software Cisco IOS® versão 12.2.7 e 12.2.8T
- Cisco Secure VPN Client 1.1 (mostrado como 2.1.12 no menu IRE client **Help > About**)
- Cisco 3600 Routers**Observação:** se você usar os Cisco 2600 Series Routers para esse tipo de cenário de VPN, os roteadores deverão ser instalados com imagens de criptografia do

IPsec VPN IOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

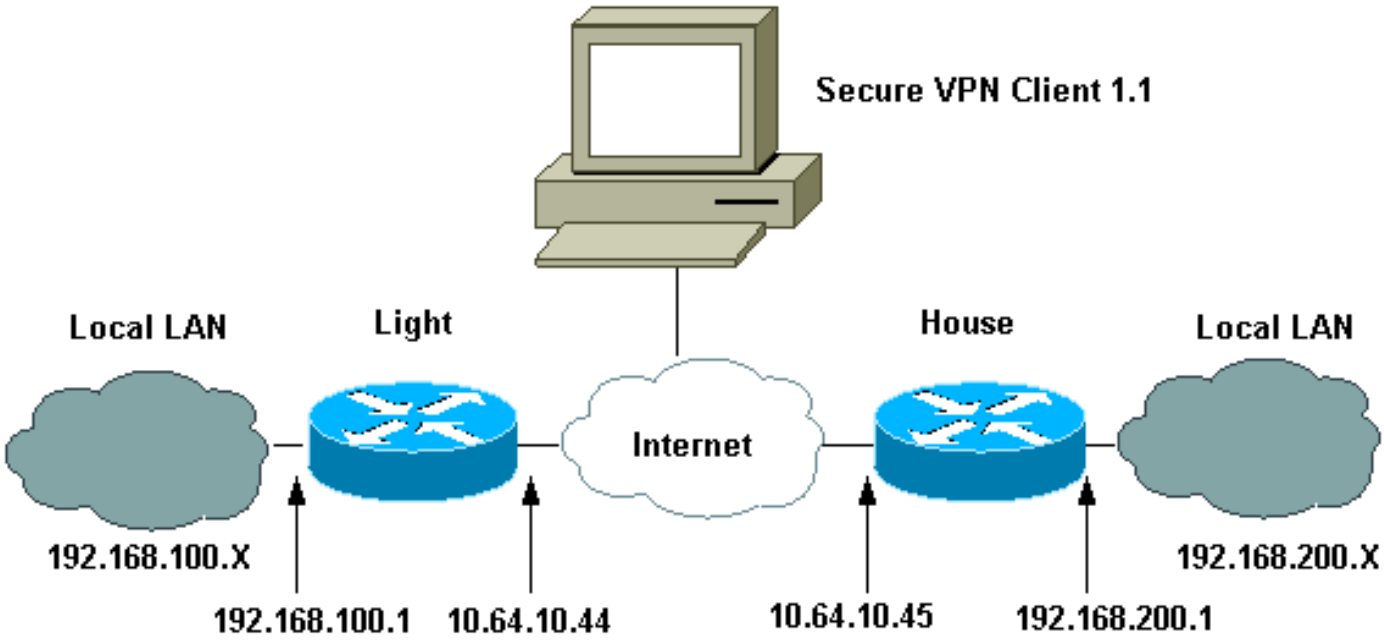
Configurar

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 neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza estas configurações.

- Configuração leve
- Configuração doméstica
- Configuração de cliente de VPN

Configuração leve

```
 Current configuration : 2047 bytes
 !
 version 12.2
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname Light
 !
 boot system flash:c3660-ik9o3s-mz.122-8T
 !
 ip subnet-zero
 !
 ip audit notify log
 ip audit po max-events 100
 ip ssh time-out 120
 ip ssh authentication-retries 3
 !
!--- IPsec Internet Security Association and !--- Key
Management Protocol (ISAKMP) policy. crypto isakmp
policy 5
  hash md5
  authentication pre-share
!--- ISAKMP key for static LAN-to-LAN tunnel !---
without extended authenticaton (xauth). crypto isakmp
key cisco123 address 10.64.10.45 no-xauth
!--- ISAKMP key for the dynamic VPN Client. crypto
isakmp key 123cisco address 0.0.0.0 0.0.0.0
!--- Assign the IP address to the VPN Client. crypto
isakmp client configuration address-pool local test-pool
 !
 !
 !
 crypto ipsec transform-set testset esp-des esp-md5-hmac
 !
 crypto dynamic-map test-dynamic 10
  set transform-set testset
 !
 !
!--- VPN Client mode configuration negotiation, !---
such as IP address assignment and xauth. crypto map test
client configuration address initiate
 crypto map test client configuration address respond
!--- Static crypto map for the LAN-to-LAN tunnel. crypto
map test 5 ipsec-isakmp
  set peer 10.64.10.45
  set transform-set testset
!--- Include the private network-to-private network
traffic !--- in the encryption process. match address
115
!--- Dynamic crypto map for the VPN Client. crypto map
test 10 ipsec-isakmp dynamic test-dynamic
 !


 call rsvp-sync
 !
 !
 !
 !
 !
 fax interface-type modem
```

```
 mta receive maximum-recipients 0
 !
 controller E1 2/0
 !
 !
 !
 interface FastEthernet0/0
  ip address 10.64.10.44 255.255.255.224
  ip nat outside
  duplex auto
  speed auto
  crypto map test
 !
 interface FastEthernet0/1
  ip address 192.168.100.1 255.255.255.0
  ip nat inside
  duplex auto
  speed auto
 !
 interface BRI4/0
  no ip address
  shutdown
 !
 interface BRI4/1
  no ip address
  shutdown
 !
 interface BRI4/2
  no ip address
  shutdown
 !
 interface BRI4/3
  no ip address
  shutdown
 !
  !--- Define the IP address pool for the VPN Client. ip
local pool test-pool 192.168.1.1 192.168.1.254
!--- Exclude the private network and VPN Client !---
traffic from the NAT process. ip nat inside source
route-map nonat interface FastEthernet0/0 overload
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.64.10.33
 ip http server
 ip pim bidir-enable
 !
!--- Exclude the private network and VPN Client !---
traffic from the NAT process. access-list 110 deny   ip
192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
 access-list 110 deny   ip 192.168.100.0 0.0.0.255
192.168.1.0 0.0.0.255
 access-list 110 permit ip 192.168.100.0 0.0.0.255 any
!--- Include the private network-to-private network
traffic !--- in the encryption process. access-list 115
permit ip 192.168.100.0 0.0.0.255 192.168.200.0
0.0.0.255
 !
!--- Exclude the private network and VPN Client !---
traffic from the NAT process. route-map nonat permit 10
  match ip address 110
 !
 !
 dial-peer cor custom
 !
 !
```

```
 !
 !
 !
 line con 0
 line 97 108
 line aux 0
 line vty 0 4
 !
 end
```

Configuração doméstica

```
Current configuration : 1689 bytes
 !
 version 12.2
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname house
 !
 boot system flash:c3660-jk8o3s-mz.122-7.bin
 !
 ip subnet-zero
 !
 !
 no ip domain-lookup
 !
 ip audit notify log
 ip audit po max-events 100
 ip ssh time-out 120
 ip ssh authentication-retries 3
 !
!--- IPsec ISAKMP policy. crypto isakmp policy 5
  hash md5
  authentication pre-share
!--- ISAKMP key for static LAN-to-LAN tunnel without
xauth authenticaton. crypto isakmp key cisco123 address
10.64.10.44 no-xauth
 !
 !
 crypto ipsec transform-set testset esp-des esp-md5-hmac
 !
!--- Static crypto map for the LAN-to-LAN tunnel. crypto
map test 5 ipsec-isakmp
  set peer 10.64.10.44
  set transform-set testset
!--- Include the private network-to-private network
traffic !--- in the encryption process.  match address
115
 !
 call rsvp-sync
 cns event-service server
 !
 !
 !
 !
 !
 fax interface-type modem
 mta receive maximum-recipients 0
 !
 !
 !
```

```
 interface FastEthernet0/0
  ip address 10.64.10.45 255.255.255.224
  ip nat outside
  duplex auto
  speed auto
  crypto map test
 !
 interface FastEthernet0/1
  ip address 192.168.200.1 255.255.255.0
  ip nat inside
  duplex auto
  speed auto
 !
 interface BRI2/0
  no ip address
  shutdown
 !
 interface BRI2/1
  no ip address
  shutdown
 !
 interface BRI2/2
  no ip address
  shutdown
 !
 interface BRI2/3
  no ip address
  shutdown
 !
 interface FastEthernet4/0
  no ip address
  shutdown
  duplex auto
  speed auto
 !
  !--- Exclude the private network traffic !--- from the
dynamic (dynamic association to a pool) NAT process. ip
nat inside source route-map nonat interface
FastEthernet0/0 overload
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.64.10.33
 no ip http server
 ip pim bidir-enable
 !
  !--- Exclude the private network traffic from the NAT
process. access-list 110 deny   ip 192.168.200.0
0.0.0.255 192.168.100.0 0.0.0.255
 access-list 110 permit ip 192.168.200.0 0.0.0.255 any
!--- Include the private network-to-private network
traffic !--- in the encryption process. access-list 115
permit ip 192.168.200.0 0.0.0.255 192.168.100.0
0.0.0.255
  !--- Exclude the private network traffic from the NAT
process. route-map nonat permit 10
  match ip address 110
 !
 !
 !
 dial-peer cor custom
 !
 !
 !
 !
 !
```

```
 line con 0
 line aux 0
 line vty 0 4
  login
 !
 end
```

Configuração de cliente de VPN

```
Network Security policy:
       1- TOLIGHT
       My Identity
       Connection security: Secure
       Remote Party Identity and addressing
       ID Type: IP subnet
       192.168.100.0
       255.255.255.0
       Port all Protocol all

  Connect using secure tunnel
         ID Type: IP address
         10.64.10.44


  Pre-shared Key=123cisco


  Authentication (Phase 1)
         Proposal 1
         Authentication method: pre-shared key
         Encryp Alg: DES
         Hash Alg: MD5
         SA life: Unspecified
         Key Group: DH 1


  Key exchange (Phase 2)
         Proposal 1
         Encapsulation ESP
         Encrypt Alg: DES
         Hash Alg: MD5
         Encap: tunnel
         SA life: Unspecified
         no AH


  2- Other Connections
         Connection security: Non-secure
         Local Network Interface
         Name: Any
         IP Addr: Any
         Port: All
```

Verificar

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

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

- **show crypto ipsec sa** — Mostra as SAs (Security Associations, associações de segurança) da fase 2.
- **show crypto isakmp sa** — Mostra as SAs da fase 1.

Troubleshoot

Use esta seção para resolver problemas de configuração.

Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a 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.

- **debug crypto ipsec** — Mostra as negociações de IPsec da fase 2.
- **debug crypto ipsec - Exibe as negociações ISAKMP da fase 1.**
- **debug crypto engine** —Mostra o tráfego que está criptografado.
- **clear crypto isakmp** — Limpa as SAs relacionadas à fase 1.
- **clear crypto sa** —Limpa as SAs relacionadas à fase 2.

Informações Relacionadas

- Configuração da segurança de rede IPSec
- Configurando o protocolo de segurança do intercâmbio chave de Internet
- Página do suporte de protocolo do IPsec Negotiation/IKE
- Páginas de Suporte do Cisco Secure VPN Client
- Suporte Técnico - Cisco Systems