

Configuración de IPSec Router a Router con Sobrecarga NAT y Cisco Secure VPN Client

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

[Introducción](#)

En esta configuración de ejemplo se cifra el tráfico procedente de la red que se encuentra detrás de Light a la red que se encuentra detrás de House (red de 192.168.100.x a 192.168.200.x). También se efectúa una sobrecarga de NAT (Traducción de Dirección de Red). Las conexiones de cliente VPN cifradas se permiten en Light con comodín, claves precompartidas y configuración de modo. El tráfico a Internet se traduce pero no se cifra.

[Prerequisites](#)

[Requirements](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Cisco IOS® versión 12.2.7 y 12.2.8T
- Cisco Secure VPN Client 1.1 (mostrado como 2.1.12 en el **menú IRE client Help > About**)
- Routers 3600 Cisco **Nota:** Si utiliza los Cisco 2600 Series Routers para este tipo de escenario de VPN, los routers deben instalarse con imágenes de IPsec VPN IOS criptográficas.

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.

Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento.](#)

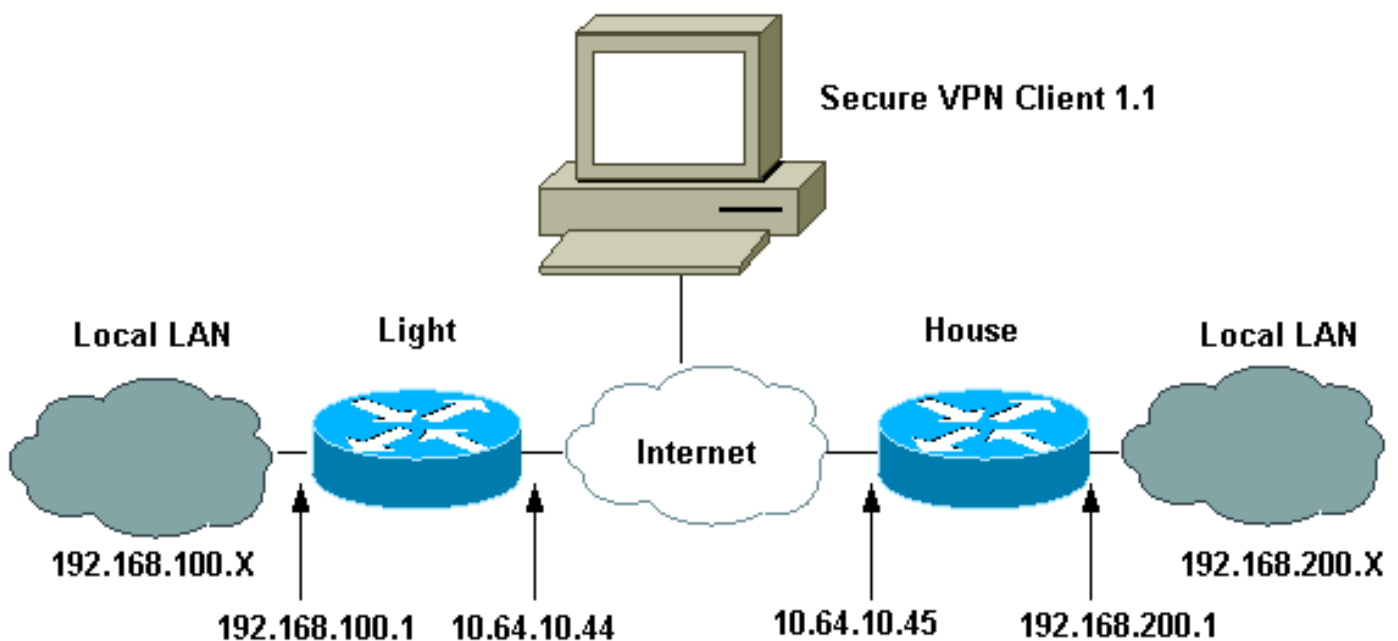
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la [Command Lookup Tool](#) (sólo [clientes registrados](#)) para obtener más información sobre los comandos utilizados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

Este documento usa estas configuraciones.

- [Configuración de luz](#)
- [Configuración base](#)
- [Configuración de cliente VPN](#)

Configuración de luz

```
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
```

Configuración base

```
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
```

Configuración de cliente 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
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

- **show crypto ipsec sa:** muestra las asociaciones de seguridad (SA) de fase 2.
- **show crypto isakmp sa**—Muestra las SA de la fase 1.

Troubleshoot

Use esta sección para resolver problemas de configuración.

Comandos para resolución de problemas

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte [Información Importante sobre Comandos Debug](#) antes de utilizar los comandos debug.

- **depuración crypto ipsec** — Muestra los IPsec Negotiations de la Fase 2.
- **debug crypto isakmp** — muestra las negociaciones ISAKMP para la fase 1.
- **debug crypto engine** — muestra el tráfico codificado.
- **clear crypto isakmp**: borra las SA relacionadas con la fase 1.
- **clear crypto sa**: borra las SA relacionadas con la fase 2.

Información Relacionada

- [Configuración de seguridad de red IPsec](#)
- [Configuración del protocolo de seguridad de intercambio de claves de Internet](#)
- [Página de Soporte del Protocolo IKE/la Negociación de IPsec](#)
- [Páginas de soporte de Cisco Secure VPN Client](#)
- [Soporte Técnico - Cisco Systems](#)