

Configuración de un Cisco 827 para PPPoE con sobrecarga de NAT IPsec VPN

Contenido

[Introducción](#)

[Antes de comenzar](#)

[Convenciones](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

[Introducción](#)

El Cisco 827 Router suele ser un Customer Premises Equipment (CPE) DSL. En esta configuración de ejemplo, el Cisco 827 se configura para Point-to-Point Protocol over Ethernet (PPPoE) y se utiliza como peer en un túnel IPsec de LAN a LAN con un Cisco 3600 Router. El Cisco 827 también está haciendo overloading (sobrecarga) de Traducción de Direcciones de Red (NAT) para proporcionar la conexión a Internet a su red interna.

[Antes de comenzar](#)

[Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

[Prerequisites](#)

Al considerar esta configuración, por favor recuerde lo siguiente:

- Asegúrese de que PPPoE funciona antes de agregar una configuración para VPN IPsec en el Cisco 827. Para depurar el cliente PPPoE en el Cisco 827, debe considerar la pila de protocolos. Debería resolver el problema en la siguiente secuencia. Capa física DSL
Capa ATM
Capa Ethernet
Capa PPP
- En esta configuración de ejemplo, el Cisco 827 tiene una dirección IP estática. Si su Cisco

827 tiene una dirección IP dinámica, consulte [Configuración de IPsec Dinámico a Estático de Router a Router con NAT](#) además de este documento.

Componentes Utilizados

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

- Cisco 827 12.1(5)YB4
- Cisco 3600 12.1(5)T8
- Cisco 6400 12.1(1)DC1

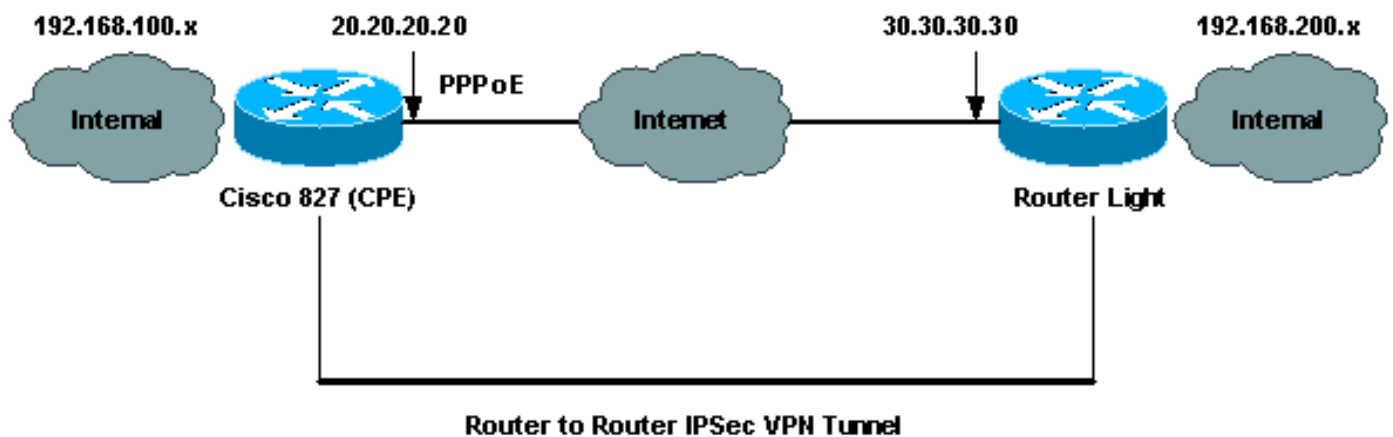
La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Configurar

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

Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.



Configuraciones

Este documento usa las configuraciones detalladas a continuación.

- [Cisco 827 \(CPE\)](#)
- [Luz del router](#)

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la [Command Lookup Tool](#) ([sólo](#) clientes registrados) .

Cisco 827 (CPE)

```
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 827
!
logging rate-limit console 10 except errors
!
ip subnet-zero
no ip finger
!
no ip dhcp-client network-discovery
vpdn enable

no vpdn logging
!
vpdn-group pppoe
  request-dialin
  protocol pppoe
!
!
!
crypto isakmp policy 20
  encr 3des
  authentication pre-share
  group 2
crypto isakmp key sharedkey address 30.30.30.30
!
!
crypto ipsec transform-set dsltest esp-3des esp-md5-hmac
!
crypto map test 10 ipsec-isakmp
  set peer 30.30.30.30
  set transform-set dsltest
  match address 101
!
interface Ethernet0
  ip address 192.168.100.100 255.255.255.0
  ip nat inside
!
interface ATM0
  no ip address
  no atm ilmi-keepalive
  bundle-enable
  dsl operating-mode ansi-dmt
!
interface ATM0.1 point-to-point
  pvc 0/33
  !--- This is usually provided by the ISP. protocol pppoe
  pppoe-client dial-pool-number 1 ! ! interface Dialer1 ip
  address 20.20.20.20 255.255.255.0 !--- This is provided
  by the ISP. !--- Another variation is ip address
negotiated.

  ip mtu 1492
  ip Nat outside
  encapsulation ppp
  no ip route-cache
  no ip mroute-cache
```

```
dialer pool 1
ppp authentication chap callin
ppp chap hostname testuser
ppp chap password 7 00071A1507545A545C
crypto map test
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
no ip http server
!
ip Nat inside source route-map nonat interface Dialer1
overload
access-list 1 permit 192.168.100.0 0.0.0.255
access-list 101 permit ip 192.168.100.0 0.0.0.255
192.168.200.0 0.0.0.255
access-list 105 deny ip 192.168.100.0 0.0.0.255
192.168.200.0 0.0.0.255
access-list 105 permit ip 192.168.100.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 105
!
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
 login
!
scheduler max-task-time 5000
end
```

Luz del router

```
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname light
!
boot system flash:c3660-jk2s-mz.121-5.T8.bin
logging buffered 4096 debugging
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip cef
!
crypto isakmp policy 20
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key sharedkey address 20.20.20.20
!
crypto ipsec transform-set dsltest esp-3des esp-md5-hmac
!
crypto map test 10 ipsec-isakmp
 set peer 20.20.20.20
 set transform-set dsltest
```

```
match address 101
!
call rsvp-sync
cns event-service server
!
!
!
controller E1 2/0
!
!
interface FastEthernet0/0
 ip address 192.168.200.200 255.255.255.0
 ip Nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 30.30.30.30 255.255.255.0
 ip Nat outside
 duplex auto
 speed auto
 crypto map test
!
interface Serial1/0
 no ip address
 shutdown
!
interface Serial1/1
 no ip address
 shutdown
!
interface Serial1/2
 no ip address
 shutdown
!
interface Serial1/3
 no ip address
 shutdown
!
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
!
ip kerberos source-interface any
ip Nat inside source route-map nonat interface
FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.1
ip http server
!
access-list 101 permit ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
```

```
access-list 105 deny ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
access-list 105 permit ip 192.168.200.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 105
!
!
dial-peer cor custom
!
!
line con 0
 exec-timeout 0 0
 transport input none
line 97 108
line aux 0
line vty 0 4
 login
!
end
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Nota: Para entender exactamente lo que indican los siguientes **comandos show**, consulte [Resolución de problemas de seguridad IP - Introducción y uso de comandos de depuración](#).

- **show crypto isakmp sa** - Muestra la Asociación de seguridad (SA) del Protocolo de administración de asociaciones de seguridad de Internet (ISAKMP) construida entre los pares.
- **show crypto ipsec sa** - Muestra la SA IPsec construida entre peers.
- **show crypto engine connections active**: muestra cada Fase 2 SA generada y la cantidad de tráfico enviado.

Comando IPsec Good show del router

- **show crypto isakmp sa**Cisco 827 (CPE)Luz del router
- **show crypto engine connections active**Cisco 827 (CPE)Luz del router
- **show crypto ipsec sa**

```
827#show crypto ipsec sa
```

```
interface: Dialer1
Crypto map tag: test, local addr. 20.20.20.20
```

```
local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
current_peer: 30.30.30.30
PERMIT, flags={origin_is_acl,}
```

#pkts encaps: 208, #pkts encrypt: 208, #pkts digest 208
#pkts decaps: 208, #pkts decrypt: 208, #pkts verify 208
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 2, #recv errors 0

local crypto endpt.: 20.20.20.20, remote crypto endpt.: 30.30.30.30
path mtu 1500, media mtu 1500
current outbound spi: 4FE59EF2

inbound esp sas:
spi: 0x3491ACD6(881962198)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: test
sa timing: remaining key lifetime (k/sec): (4607840/3301)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcg sas:

outbound esp sas:
spi: 0x4FE59EF2(1340448498)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: test
sa timing: remaining key lifetime (k/sec): (4607837/3301)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcg sas:

interface: Virtual-Access1
Crypto map tag: test, local addr. 20.20.20.20

local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
current_peer: 30.30.30.30
PERMIT, flags={origin_is_acl,}
#pkts encaps: 208, #pkts encrypt: 208, #pkts digest 208
#pkts decaps: 208, #pkts decrypt: 208, #pkts verify 208
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 2, #recv errors 0

local crypto endpt.: 20.20.20.20, remote crypto endpt.: 30.30.30.30
path mtu 1500, media mtu 1500
current outbound spi: 4FE59EF2

inbound esp sas:
spi: 0x3491ACD6(881962198)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: test
sa timing: remaining key lifetime (k/sec): (4607840/3301)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

```
inbound pcp sas:

outbound esp sas:
spi: 0x4FE59EF2(1340448498)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: test
sa timing: remaining key lifetime (k/sec): (4607837/3301)
IV size: 8 bytes
replay detection support: Y
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

Nota: Antes de ejecutar **comandos debug**, consulte [Información Importante sobre Comandos Debug](#) y [Solución de Problemas de Seguridad IP - Introducción y Uso de Comandos Debug](#).

- **debug crypto ipsec** - Muestra los IPSec Negotiations de la fase 2.
- **debug crypto isakmp** - Muestra las negociaciones ISAKMP de la fase 1.
- **debug crypto engine** - Muestra el tráfico cifrado.
- **ping** - Muestra la conectividad a través del túnel VPN y puede ser usado en conjunto con los comandos debug y show.

```
827#ping
Protocol [ip]:
Target IP address: 192.168.200.200
Repeat count [5]: 100
Datagram size [100]: 1600
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.100.100
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 1600-byte ICMP Echos to 192.168.200.200, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 264/266/276 ms
```

Información Relacionada

- [Páginas de Soporte de IPsec](#)
- [Páginas de Soporte de IP Routing](#)
- [Introducción al cifrado IPsec](#)

- [Resolución de problemas del router 827 de Cisco](#)
- [Soporte Técnico - Cisco Systems](#)