Configurar un Cisco 827 para el PPPoE con VPN IPSec la sobrecarga de NAT

Contenido

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.

prerrequisitos

Al considerar esta configuración, por favor recuerde lo siguiente:

- Aseegurese que el PPPoE está trabajando antes de agregar una configuración para el IPSec VPN en el Cisco 827. Para hacer el debug de al Cliente de PPPoE en el Cisco 827, usted debe considerar la pila del protocolo. Debería resolver el problema en la siguiente secuencia.Capa física DSLCapa ATMCapa EthernetCapa PPP
- En esta configuración de muestra, el Cisco 827 tiene un IP Address estático. Si su Cisco 827

tiene un IP Address dinámico, vea por favor configurar el IPSec dinámica a estática 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

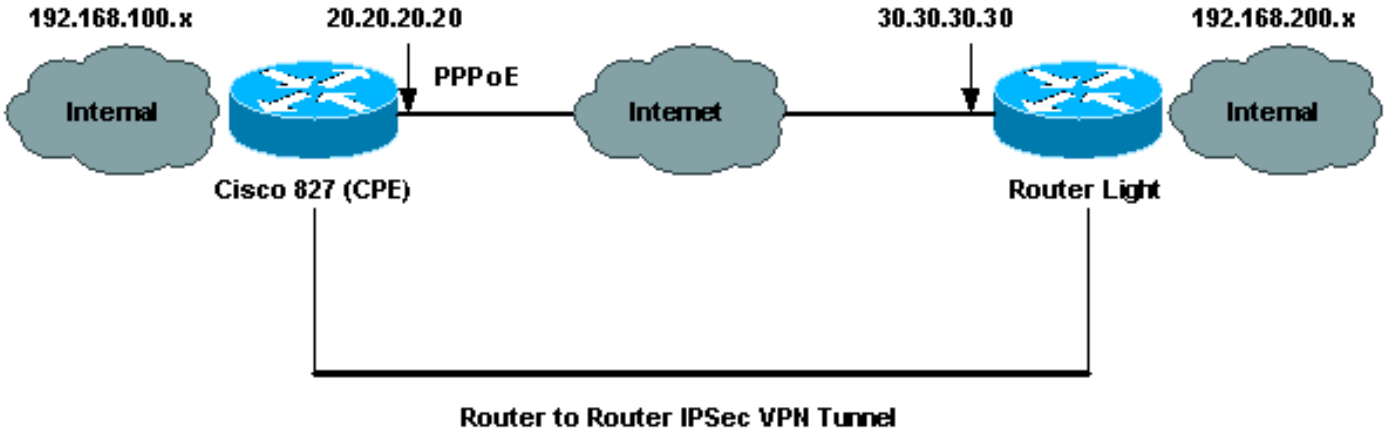
La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese 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

Note: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para 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
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
```

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.

Note: Para entender exactamente lo que indican los **comandos show** siguientes, satisfaga refieren al Troubleshooting de IP Security - entendiendo y con los comandos Debug.

- **muestre isakmp crypto sa** - Muestra la asociación de seguridad del protocolo internet security association management (ISAKMP) (SA) construida entre los pares.
- **muestre IPSec crypto sa** - Muestra IPSec SA construido entre los pares.
- show crypto engine connections active: muestra cada Fase 2 SA generada y la cantidad de tráfico enviado.

Router IPSec buen comando show

- **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 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:

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:
```

Troubleshooting

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

Comandos para resolución de problemas

Note: Antes de publicar los **comandos debug**, vea por favor la información importante en los comandos Debug y el Troubleshooting de IP Security - entendiendo y con los comandos Debug.

- **el IPSec del debug crypto** muestra los IPSec Negotiations de la fase 2.
- **el debug crypto ISAKMP** muestra negociaciones ISAKMP de la fase 1.
- **motor del debug crypto** - Muestra el tráfico se cifra que.
- 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
- Una introducción a la encripción de IPSec
- Resolución de problemas del router 827 de Cisco
- Soporte Técnico - Cisco Systems