

Configurazione di Cisco 827 per PPPoE con sovraccarico VPN IPSec NAT

Sommario

[Introduzione](#)

[Operazioni preliminari](#)

[Convenzioni](#)

[Prerequisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

Il router Cisco 827 è in genere un'apparecchiatura DSL per la sede del cliente (CPE). In questa configurazione di esempio, Cisco 827 è configurato per il protocollo PPPoE (Point-to-Point over Ethernet) e viene utilizzato come peer in un tunnel IPSec LAN-LAN con un router Cisco 3600. Cisco 827 sta anche sovraccaricando Network Address Translation (NAT) per fornire la connessione Internet per la rete interna.

[Operazioni preliminari](#)

[Convenzioni](#)

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

[Prerequisiti](#)

Quando si considera questa configurazione, tenere presente quanto segue.

- Prima di aggiungere una configurazione per VPN IPSec in Cisco 827, verificare che il protocollo PPPoE funzioni. Per eseguire il debug del client PPPoE su Cisco 827, è necessario considerare lo stack di protocolli. La risoluzione dei problemi deve essere eseguita nella sequenza riportata di seguito. Livello fisico DSL Livello ATM Layer Ethernet Livello PPP
- In questa configurazione di esempio, Cisco 827 ha un indirizzo IP statico. Se il Cisco 827 ha

un indirizzo IP dinamico, vedere [Configurazione di IPSec da router a router dinamico a statico con NAT](#) in aggiunta al presente documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni software e hardware riportate di seguito.

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

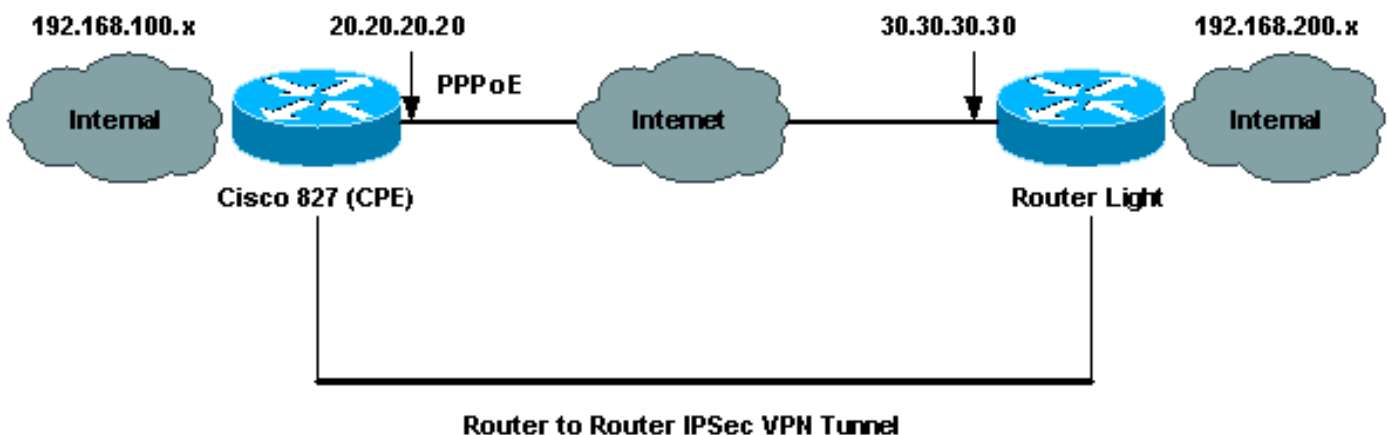
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Esempio di rete

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



Configurazioni

Questo documento utilizza le configurazioni mostrate di seguito.

- [Cisco 827 \(CPE\)](#)
- [Luce router](#)

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

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
```

Luce 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

```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

Nota: per informazioni esatte sui comandi **show** riportati di seguito, consultare [Risoluzione dei problemi di sicurezza IP - Comprensione e uso dei comandi di debug](#).

- **show crypto isakmp sa:** visualizza l'associazione di sicurezza (SA) ISAKMP (Internet Security Association Protocol) creata tra peer.
- **show crypto ipsec sa:** visualizza l'associazione di protezione IPsec creata tra peer.
- **show crypto engine connections active:** visualizza tutte le associazioni di protezione per la fase 2 create e la quantità di traffico inviato.

Comando Good show IPsec del router

- **show crypto isakmp sa**Cisco 827 (CPE)Luce router
- **mostra connessioni del motore di crittografia attive**Cisco 827 (CPE)Luce 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 pcsp 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 pcsp 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 pcsp 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:

[Risoluzione dei problemi](#)

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

[Comandi per la risoluzione dei problemi](#)

Nota: prima di usare i comandi di **debug**, consultare le [informazioni importanti sui comandi di debug](#) e sulla [risoluzione dei problemi di sicurezza IP - Comprensione e uso dei comandi di debug](#).

- **debug crypto ipsec:** visualizza le negoziazioni IPsec della fase 2.
- **debug crypto isakmp:** visualizza le negoziazioni ISAKMP della fase 1.
- **debug crypto engine:** visualizza il traffico crittografato.
- **ping:** visualizza la connettività attraverso il tunnel VPN e può essere utilizzata con i comandi **debug** e **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
```

[Informazioni correlate](#)

- [Pagine di supporto IPsec](#)
- [Pagine di supporto per il routing IP](#)
- [Introduzione alla crittografia IPsec](#)
- [Risoluzione dei problemi del router Cisco 827](#)

- [Supporto tecnico – Cisco Systems](#)