

Configuration de Cisco 827 pour PPPoE avec chevauchement NAT IPsec VPN

Contenu

[Introduction](#)

[Avant de commencer](#)

[Conventions](#)

[Conditions préalables](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Informations connexes](#)

[Introduction](#)

Le routeur Cisco 827 est généralement un équipement client DSL (CPE). Dans cet exemple de configuration, le Cisco 827 est configuré pour le protocole PPPoE (Point-to-Point Protocol over Ethernet) et est utilisé comme homologue dans un tunnel IPsec LAN à LAN avec un routeur Cisco 3600. Le Cisco 827 effectue également une surcharge NAT (Network Address Translation) pour fournir une connexion Internet à son réseau interne.

[Avant de commencer](#)

[Conventions](#)

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

[Conditions préalables](#)

Lorsque vous examinez cette configuration, n'oubliez pas ce qui suit.

- Assurez-vous que PPPoE fonctionne avant d'ajouter une configuration pour VPN IPsec dans le Cisco 827. Pour déboguer le client PPPoE sur le Cisco 827, vous devez considérer la pile de protocoles. Vous devez effectuer le dépannage dans la séquence ci-dessous. Couche physique DSL Couche ATM Couche Ethernet Couche PPP
- Dans cet exemple de configuration, le Cisco 827 possède une adresse IP statique. Si votre

Cisco 827 dispose d'une adresse IP dynamique, reportez-vous à [Configuration d'IPSec dynamique à statique de routeur à routeur avec NAT](#) en plus de ce document.

Components Used

Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

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

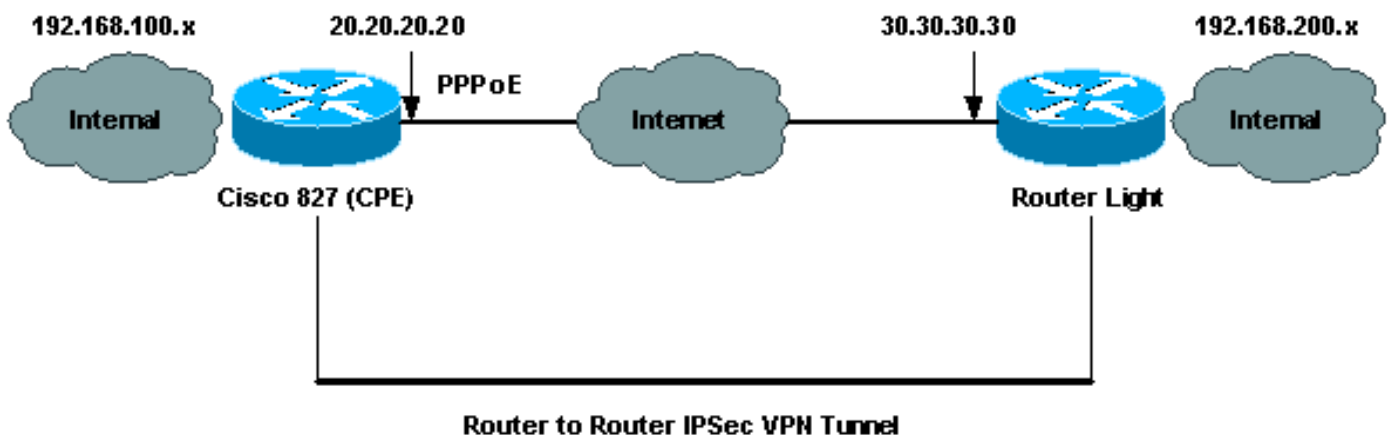
Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



Configurations

Ce document utilise les configurations présentées ci-dessous.

- [Cisco 827 \(CPE\)](#)
- [Voyant du routeur](#)

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement).

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
```

Voyant du routeur

```
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
```

Vérification

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque : Pour comprendre exactement ce que les commandes **show** suivantes indiquent, reportez-vous à [Dépannage de la sécurité IP - Compréhension et utilisation des commandes de débogage](#).

- **show crypto isakmp sa** - Affiche l'association de sécurité ISAKMP (Internet Security Association Management Protocol) créée entre homologues.
- **show crypto ipsec sa** - Affiche la SA IPsec construite entre homologues.
- **show crypto engine connections active** - Affiche chaque SA de phase 2 créée et la quantité de trafic envoyée.

Commande Good show du routeur IPsec

- **show crypto isakmp sa**Cisco 827 (CPE)Voyant du routeur
- **show crypto engine connections active**Cisco 827 (CPE)Voyant du routeur
- **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 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 pcp sas:

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Remarque : avant d'émettre des commandes **debug**, consultez [Informations importantes sur les commandes de débogage](#) et [Dépannage de la sécurité IP - Compréhension et utilisation des commandes de débogage](#).

- **debug crypto ipsec** - Affiche les négociations IPsec de la phase 2.
- **debug crypto isakmp** - Affiche les négociations ISAKMP de la phase 1.
- **debug crypto engine** - Affiche le trafic chiffré.
- **ping** - Affiche la connectivité via le tunnel VPN et peut être utilisée conjointement avec les commandes **debug** et **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
```

Informations connexes

- [Pages de support IPsec](#)
- [Pages de support du routage IP](#)
- [Présentation du chiffrement IPsec](#)
- [Dépannage du routeur Cisco 827](#)

- [Support technique - Cisco Systems](#)