為PPPoE配置Cisco 827並配置VPN IPSec NAT過載

目錄

簡介

Cisco 827路由器通常是DSL客戶端裝置(CPE)。 在此示例配置中，Cisco 827配置為乙太網點對點協定(PPPoE)，並在帶有Cisco 3600路由器的LAN到LAN IPSec隧道中用作對等體。Cisco 827還執行網路地址轉換(NAT)過載，為其內部網路提供網際網路連線。

開始之前

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

必要條件

考慮此配置時，請記住以下內容。

- 在為Cisco 827中的IPSec VPN新增配置之前，請確保PPPoE工作正常。要在Cisco 827上調試PPPoE客戶端，必須考慮協定棧。您應按以下順序進行故障排除。DSL實體層ATM層乙太網層PPP層
- 在此示例配置中，Cisco 827具有靜態IP地址。如果您的Cisco 827具有動態IP地址，除本文檔外，請參閱使用NAT配置路由器到路由器的動態到靜態IPSec。

採用元件

本檔案中的資訊是根據以下軟體和硬體版本。

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

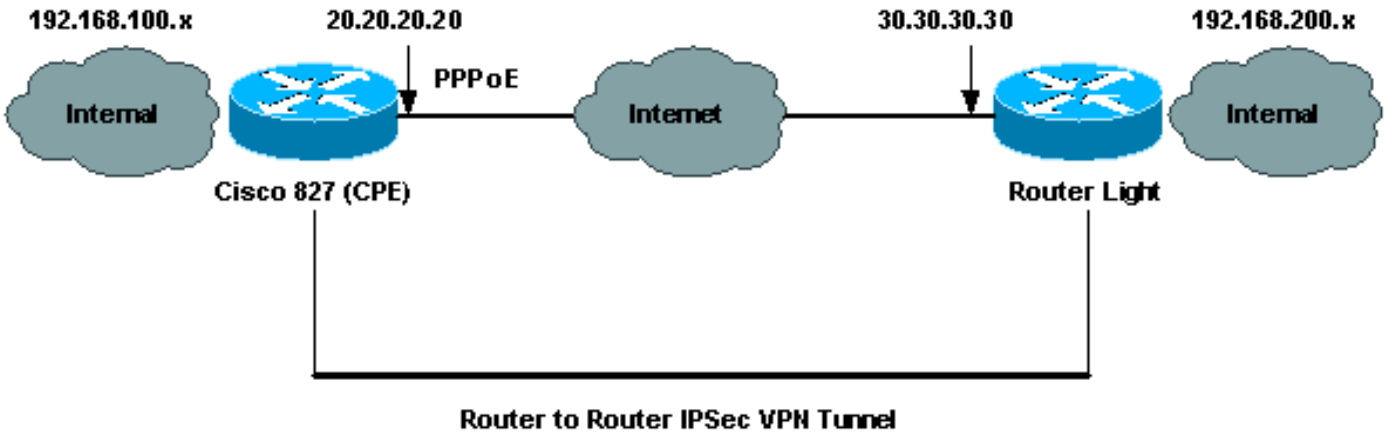
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

設定

本節提供用於設定本文件中所述功能的資訊。

網路圖表

本文檔使用下圖所示的網路設定。



組態

本文檔使用如下所示的配置。

- 思科827(CPE)
- 路由器指示燈

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

思科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
```

路由器指示燈

```
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
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

注意：要準確瞭解以下show**命令**的含義，請參閱IP安全故障排除 — 瞭解和使用Debug命令**。**

- **show crypto isakmp sa** — 顯示對等體之間構建的網際網路安全關聯管理協定(ISAKMP)安全關聯(SA)。
- **show crypto ipsec sa** — 顯示對等體之間構建的IPSec SA。
- **show crypto engine connections active** — 顯示每個階段2 SA的構建和已傳送流量。

路由器IPSec良好show命令

- **show crypto isakmp sa**思科827(CPE)路由器指示燈
- **show crypto engine connections active**思科827(CPE)路由器指示燈
- **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:
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

注意：發出debug指令之前，請先參閱有關Debug指令的重要資訊和IP安全性疑難排解 — 瞭解和使用Debug指令。

- **debug crypto ipsec** — 顯示第2階段的IPSec協商。
- **debug crypto isakmp** — 顯示第1階段的ISAKMP協商。
- **debug crypto engine** — 顯示加密的流量。
- **ping** — 顯示通過VPN隧道的連線，並可與**debug**和**show**命令結合使用。

```
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
```

相關資訊

- IPSec支援頁面
- IP路由支援頁面
- IPSec加密簡介
- 思科827路由器故障排除
- 技術支援 - Cisco Systems