

配置 Cisco 827 上带VPN IPSec NAT 超载的 PPPoE

目录

[简介](#)

[开始使用前](#)

[规则](#)

[先决条件](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

简介

Cisco 827 路由器通常是 DSL 客户端前置设备 (CPE)。在此示例配置中，思科827配置用于以太网点对点协议(PPPoE的)，用作使用思科3600路由器的LAN-to-LAN IPSec隧道中的对端。Cisco 827 还会执行网络地址转换 (NAT) 超载以便为其内部网络提供 Internet 连接。

开始使用前

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

先决条件

当考虑此配置时，请牢记下列各项。

- 为Cisco 827中的IPSec VPN添加配置之前，确保PPPoE正在运行。要在 Cisco 827 上调试 PPPoE 客户端，必须考虑协议堆栈。应按以下顺序排除故障。DSL 物理层ATM 层以太网层 PPP 层
- 在此示例配置中，Cisco 827 具有一个静态 IP 地址。如果您的 Cisco 827 具有一个动态 IP 地址，请参阅[通过 NAT 配置路由器间动态到静态 IPSec](#) 以及本文。

使用的组件

本文档中的信息基于以下软件和硬件版本。

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

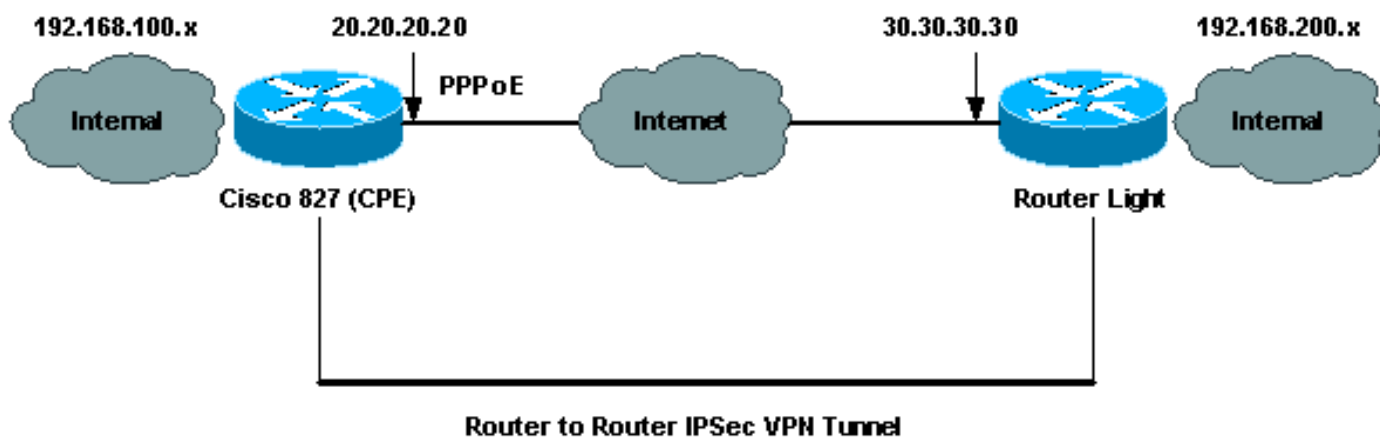
本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用下图所示的网络设置。



配置

本文档使用如下所示的配置。

- [Cisco 827 \(CPE\)](#)
- [路由器灯](#)

注意：要查找本文档所用命令的其他信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

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
```

路由器灯

```
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
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

[命令输出解释程序工具](#) ([仅限注册用户](#)) 支持某些 **show** 命令，使用此工具可以查看对 **show** 命令输出的分析。

注意： [要正确地](#)了解以下show命令显示了什么，请参见[IP安全故障排除-了解和使用debug命令](#)。

- **show crypto isakmp sa** - 显示对等体之间建立的 Internet 安全关联管理协议 (ISAKMP) 安全关联 (SA)。
- **show crypto ipsec sa** - 显示对等体之间建立的 IPsec SA。
- **show crypto engine connections active** - 显示已建立的每个阶段 2 SA 和已发送的流量。

Router IPsec Good show 命令

- **show crypto isakmp sa**[Cisco 827 \(CPE\)路由器灯](#)
- **show crypto engine connections active**[Cisco 827 \(CPE\)路由器灯](#)
- **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 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:

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

注意：在发出 `debug` 命令之前，请参阅[关于debug命令和IP安全故障排除的重要信息-了解和使用debug命令](#)。

- `debug crypto ipsec` - 显示第 2 阶段的 IPsec 协商。
- `debug crypto isakmp` 显示第 1 阶段的 ISAKMP 协商。
- [debug crypto engine](#) - 显示加密的流量。
- `ping` - 通过 VPN 隧道显示连接，并且可与 `debug and show` 命令配合使用。

```
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
```

[相关信息](#)

- [IPSec 支持页](#)
- [IP 路由支持页](#)
- [IPSec 加密简介](#)
- [Cisco 827 路由器故障排除](#)
- [技术支持 - Cisco Systems](#)