VPN IPSec NAT オーバーロードを使用する PPPoE のための Cisco 827 の設定

目次

概要

通常 Cisco 827 ルータは DSL 宅内装置（CPE）です。 この設定例では、Cisco 827 は Point-to-Point Protocol over Ethernet（PPPoE）用に設定され、Cisco 3600 ルータとの LAN-to-LAN IPSec トンネルでピアとして使用されます。 Cisco 827 では Network Address Translation（NAT; ネットワーク アドレス変換）オーバーロードも行われ、内部ネットワークにインターネット接続を提供します。

はじめに

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

前提条件

この設定を行う際は、次のことを確認してください。

- Cisco 827 に IPSec VPN の設定を追加する前に PPPoE が動作していることを確認します。 Cisco 827 で PPPoE クライアントをデバッグするには、プロトコル スタックを考慮します。 次の順番でトラブルシューティングを実施します。DSL物理レイヤATM レイヤイーサネット レイヤPPP 層
- この設定例では、Cisco 827 にスタティック IP アドレスがあります。 Cisco 827 にダイナミ

ック IP アドレスがある場合は、このドキュメントの他に、NAT によるルータ ツー ルータ ダイナミック ツー スタティック IPSec（英語）を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

ネットワーク図

このドキュメントでは次の図に示すネットワーク

設定

このドキュメントでは次に示す設定を使用しています。

- Cisco 827（CPE）
- Router Light

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

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
```

Router Light

```
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
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

注: 次の **show** コマンドの表示を厳密に理解するには、IP Security のトラブルシューティング：debug コマンドの説明と使用（英語）を参照してください。

- **show crypto isakmp sa**：ピア間で構築された Internet Security Association Management Protocol（ISAKMP）セキュリティ アソシエーション（SA）を表示します。
- **show crypto ipsec sa**：ピア間に確立された IPSec SA を表示します。
- **show crypto engine connections active**：確立されたフェーズ 2 の各 SA と送信されたトラフィック量を表示します。

ルータIPSec が正常に機能しているときの show コマンド

- **show crypto isakmp sa**Cisco 827（CPE）Router Light
- **show crypto engine connections active**Cisco 827（CPE）Router Light
- **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:
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

トラブルシューティングのためのコマンド

注: debug コマンドを実行する前に、debug コマンドの重要な情報（英語）および IP Security のトラブルシューティング：debug コマンドの説明と使用（英語）を参照してください。

- **debug crypto ipsec**：IPSec ネゴシエーションのフェーズ 2 を表示します。
- **debug crypto isakmp**：ISAKMP ネゴシエーションのフェーズ 1 を表示します。
- **debug crypto engine**：暗号化されたトラフィックを表示します。
- **ping**：VPN トンネル間の接続性を表示します。**debug および show** コマンドと一緒に使用できます。

```
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
```

関連情報

- IPSec に関するサポートページ（英語）
- IP ルーティングに関するサポートページ
- IPsec 暗号化の概要
- Cisco 827 ルータのトラブルシューティング
- テクニカルサポート - Cisco Systems