

Configuring a Cisco 827 for PPPoE with VPN IPSec NAT Overloading

Document ID: 22340

Introduction

Before You Begin

Conventions

Prerequisites

Components Used

Configure

Network Diagram

Configurations

Verify

Troubleshoot

Troubleshooting Commands

Related Information

Introduction

The Cisco 827 router is usually a DSL customer premises equipment (CPE). In this sample configuration, the Cisco 827 is configured for Point-to-Point Protocol over Ethernet (PPPoE) and is used as a peer in a LAN-to-LAN IPSec tunnel with a Cisco 3600 router. The Cisco 827 is also doing Network Address Translation (NAT) overloading to provide Internet connection for its internal network.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

When considering this configuration, please remember the following.

- Make sure that PPPoE is working before adding a configuration for IPSec VPN in the Cisco 827. To debug the PPPoE Client on the Cisco 827, you must consider the protocol stack. You should troubleshoot in the sequence below.
 1. DSL Physical Layer
 2. ATM Layer
 3. Ethernet Layer
 4. PPP Layer
- In this sample configuration, the Cisco 827 has a static IP address. If your Cisco 827 has a dynamic IP address, please see Configuring Router-to-Router Dynamic-to-Static IPSec with NAT in addition to this document.

Components Used

The information in this document is based on the software and hardware versions below.

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

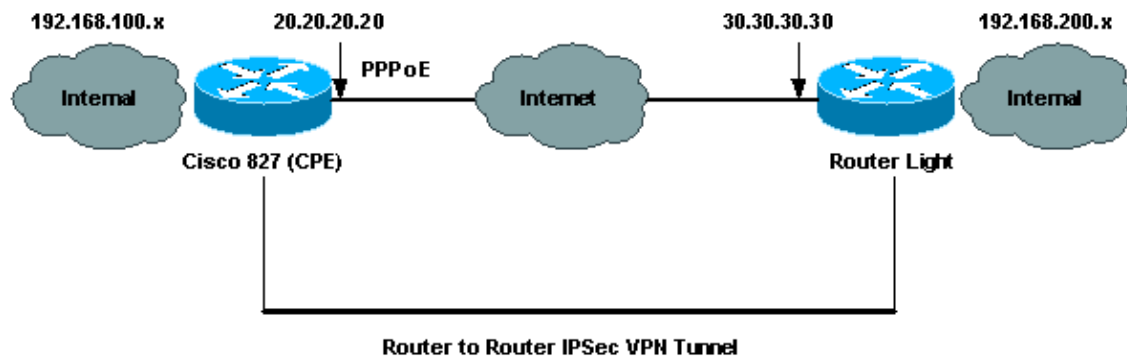
The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Configure

In this section, you are presented with the information to configure the features described in this document.

Network Diagram

This document uses the network setup shown in the diagram below.



Configurations

This document uses the configurations shown below.

- Cisco 827 (CPE)
- Router Light

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Cisco 827 (CPE)
<pre>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</pre>

```
!
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
```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: To understand exactly what the following **show** commands indicate, please refer to IP Security Troubleshooting – Understanding and Using Debug Commands.

- **show crypto isakmp sa** – Shows the Internet Security Association Management Protocol (ISAKMP) security association (SA) built between peers.
- **show crypto ipsec sa** – Shows the IPSec SA built between peers.
- **show crypto engine connections active** – Shows each Phase 2 SA built and the amount of traffic sent.

Router IPSec Good show Command

- **show crypto isakmp sa**

Cisco 827 (CPE)

dst	src	state	conn-id	slot
30.30.30.30	20.20.20.20	QM_IDLE	1	0

Router Light

dst	src	state	conn-id	slot
30.30.30.30	20.20.20.20	QM_IDLE	1	0

- **show crypto engine connections active**

Cisco 827 (CPE)

ID	Interface	IP Address	State	Algorithm	Encrypt	Decrypt
1	<none>	<none>	set	HMAC_SHA+3DES_56_C	0	0
2000	Dialer 1	20.20.20.20	set	HMAC_MD5+3DES_56_C	0	104
2001	Dialer 1	20.20.20.20	set	HMAC_MD5+3DES_56_C	104	0

Router Light

ID	Interface	IP Address	State	Algorithm	Encrypt	Decrypt
1	FastEthernet0/1	30.30.30.30	set	HMAC_SHA+3DES_56	0	0
1960	FastEthernet0/1	30.30.30.30	set	HMAC_MD5+3DES_56_C	0	104
1961	FastEthernet0/1	30.30.30.30	set	HMAC_MD5+3DES_56_C	104	0

• **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:

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Note: Before issuing **debug** commands, please see Important Information on Debug Commands and IP Security Troubleshooting – Understanding and Using Debug Commands.

- **debug crypto ipsec**– Shows the IPSec negotiations of phase 2.
- **debug crypto isakmp**– Shows the ISAKMP negotiations of phase 1.
- **debug crypto engine** – Shows the traffic that is encrypted.
- **ping** – Shows the connectivity through the VPN tunnel and can be used in conjunction with **debug** and **show** commands.

```
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
```

Related Information

- [IPSec Support Pages](#)
 - [IP Routing Support Pages](#)
 - [An Introduction to IPSec Encryption](#)
 - [Troubleshooting the Cisco 827 Router](#)
 - [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 02, 2006

Document ID: 22340
