

PPTP Connection Through Zone Based Firewall Router with NAT Configuration Example

Document ID: 110353

Introduction

Prerequisites

Requirements

Components Used

Conventions

Background Information

Configure

Network Diagram

PPTP Router Configuration

PPTP Client Configuration and Settings

Verify

Troubleshoot

Related Information

Introduction

This sample configuration demonstrates how to configure a Router with Zone Based Firewall and NAT configuration to serve as a termination of Point-to-Point Tunneling Protocol (PPTP) connections.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Router 871
- Cisco IOS® Software Release 12.4T and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

The internal network has a server that users on the Internet can access once they are connected through PPTP that terminates on an Internet facing router. All other access to hosts on the internal network is denied from

outside users.

- IP address of the Internal server;0.22.22.10
- IP address of the Remote Client PC;0.66.83.50

All users on the internal network are allowed unrestricted access to the Internet. These internal users use PAT on the Router in order to reach the Internet. All traffic from the Internal users is inspected on passing through the Router.

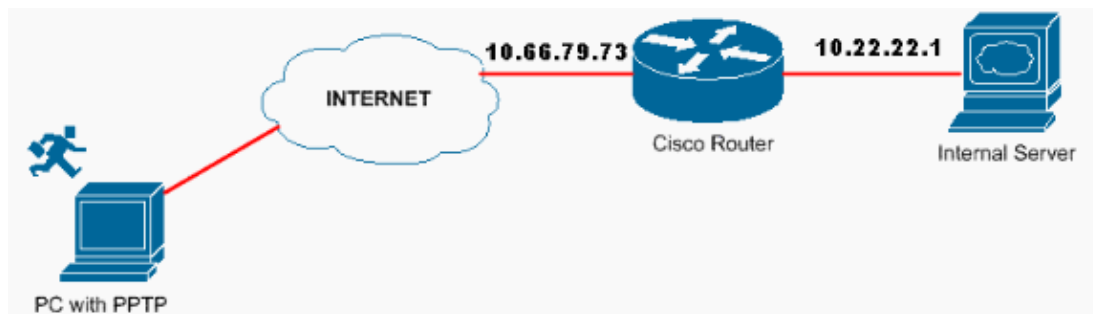
Configure

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

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



PPTP Router Configuration

This document uses this configuration.

These Cisco IOS commands are applicable to all platforms that support PPTP.

```
Router#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
  
!--- Enable virtual private dial-up networking.  
  
Router(config)#vpdn enable  
  
!--- Enters VPDN group configuration mode for the specified VPDN group.  
  
Router(config)#vpdn-group 1  
  
!--- Enters VPDN accept-dialin configuration mode  
!--- and enables the router to accept dial-in requests.  
  
Router(config-vpdn)#accept-dialin
```

!--- Specifies which PPTP protocol is used.

```
Router(config-ppdn-acc-in)#protocol pptp
```

*!--- Specifies the virtual template that is used
!--- in order to clone the virtual access interface.*

```
Router(config-ppdn-acc-in)#virtual-template 1  
Router(config-ppdn-acc-in)#exit
```

```
Router(config)#ip local pool defaultpool 192.168.100.1 192.168.100.254
```

*!--- Create virtual-template interface used for cloning
!--- virtual-access interfaces with the use of address pool defaultpool
!--- with Challenge Authentication Protocol (CHAP) authentication and MS-CHAP.*

```
Router(config)#interface virtual-template 1
```

```
Router(config-if)#encapsulation ppp  
Router(config-if)#peer default ip address pool defaultpool  
Router(config-if)#ip unnumbered FastEthernet4  
Router(config-if)#ppp authentication chap ms-chap
```

Note: Non-default commands are shown in **bold**.

Router

```
Router#show run  
Building configuration...  
  
Current configuration : 3666 bytes  
!  
version 12.4  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname Router  
!  
boot-start-marker  
boot system flash flash:c870-advsecurityk9-mz.124-20.T3.bin  
boot-end-marker  
!  
logging message-counter syslog  
enable password cisco  
!  
aaa new-model  
!  
!  
aaa authentication login VTY local  
!  
  
!--- Define local authentication for PPP.  
  
!  
aaa authentication ppp default local  
!
```

```
!  
aaa session-id common  
!  
!  
dot11 syslog  
ip source-route  
!  
!  
ip cef  
ip domain name cisco.com  
!  
!  
vpdn enable  
!  
  
!--- Enable VDPN.  
  
!  
vpdn-group PPTP-VPDN  
!  
  
!--- Default PPTP VPDN group.  
  
!  
accept-dialin  
  protocol pptp  
  virtual-template 1  
!  
!  
  
!--- Defining local username and password.  
  
!  
username cisco privilege 15 password 0 cisco  
!  
archive  
  log config  
  hidekeys  
!  
!  
ip ssh version 1  
!  
  
!--- Defining Zone-Based Policy Firewall Class-Maps.  
  
!  
class-map type inspect match-all PPTP-Pass-Through-Traffic  
  match access-group name PPTP-PASS-THROUGH  
class-map type inspect match-any All-Traffic  
  match protocol tcp  
  match protocol udp  
  match protocol icmp  
class-map type inspect match-all Router-Access-Traffic  
  match access-group name Router-Access  
class-map type inspect match-all PPTP-Terminated-Traffic  
  match access-group name PPTP-TERMINATED  
!  
!  
  
!--- Defining Zone-Based Policy Firewall Policy-Maps.  
  
!  
policy-map type inspect PPTP-In-Policy  
  class type inspect All-Traffic  
    inspect  
  class class-default
```

```

    drop
policy-map type inspect Out-In-Policy
  class type inspect PPTP-Pass-Through-Traffic
    pass
  class class-default
    drop
policy-map type inspect In-Out-Policy
  class type inspect PPTP-Pass-Through-Traffic
    pass
  class type inspect All-Traffic
    inspect
  class class-default
    drop
policy-map type inspect Out-Self-Policy
  class type inspect Router-Access-Traffic
    pass
  class type inspect PPTP-Terminated-Traffic
    pass
  class class-default
    drop
!
!---- Defining the different zones.
!
zone security outside
zone security inside
zone security pptp
!
!---- Defining the zone-pairs for different flows of traffic.
!
zone-pair security outside-self source outside destination self
  service-policy type inspect Out-Self-Policy
zone-pair security pptp-in source pptp destination inside
  service-policy type inspect PPTP-In-Policy
zone-pair security inside-outside source inside destination outside
  service-policy type inspect In-Out-Policy
!
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
  description "Connected to Outside Network"
  ip address 10.66.79.73 255.255.255.224
!
!---- Defines the interface as external for NAT.
!
ip nat outside
ip virtual-reassembly
!
!---- Defines the interface as part of the outside zone.
!
zone-member security outside
speed 100

```

```

full-duplex
!

!--- Create virtual-template interface used for cloning
!--- virtual-access interfaces with the use of address pool defaultpool
!--- with CHAP authentication and MS-CHAP.

!
interface Virtual-Templat1
 ip unnumbered FastEthernet4
!

!--- Defines the interface as part of the ptp zone.

!
zone-member security ptp
peer default ip address pool defaultpool
ppp authentication chap ms-chap
!
interface Dot11Radio0
 no ip address
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role root
!
interface Vlan1
 description "Connected to Inside Network"
 ip address 10.22.22.1 255.255.255.0
!

!--- Defines the interface as internal for NAT.

!
ip nat inside
 ip virtual-reassembly
!

!--- Defines the interface as part of the inside zone.

!
zone-member security inside
!

!--- Enable Create IP pool named test and specify IP range.

!
ip local pool defaultpool 192.168.100.1 192.168.100.254
 ip forward-protocol nd
 ip route 0.0.0.0 0.0.0.0 10.66.79.65
 no ip http server
 no ip http secure-server
!

!--- Indicates that any packets received on the inside interface
!--- matched by access list NO-NAT share one public IP address (the
!--- address on Fa4).
!--- Note that traffic from the internal network to the remote clients
!--- is not natted.

!
ip nat inside source list NO-NAT interface FastEthernet4 overload
!

!--- Traffic from internal network to remote clients is denied from
!--- being natted.

!

```

```

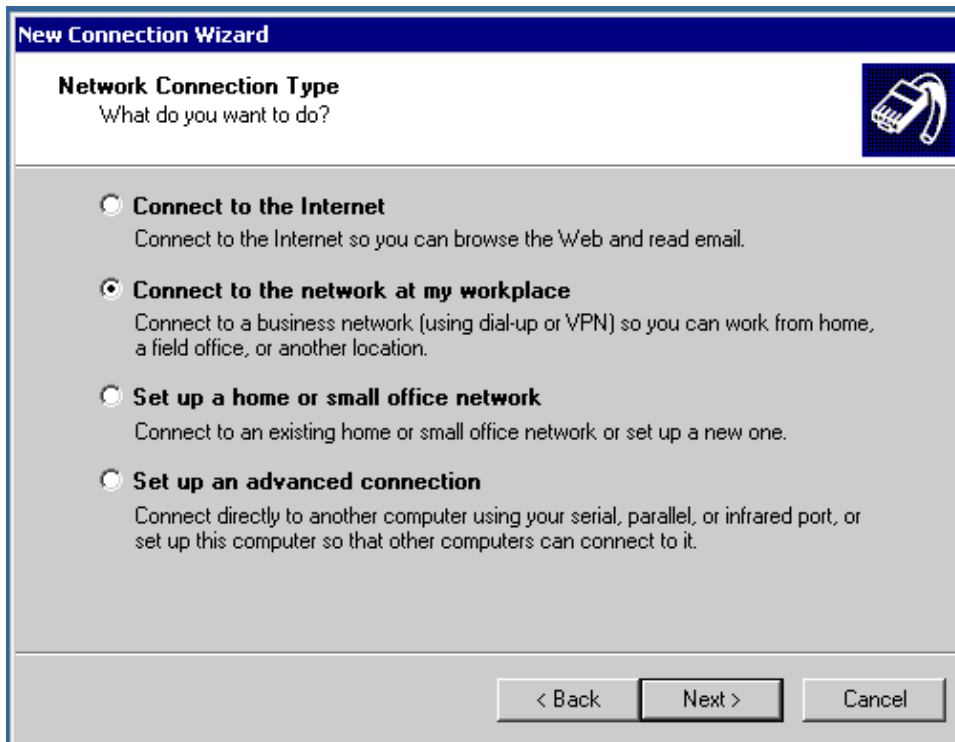
ip access-list extended NO-NAT
deny ip 10.22.22.0 0.0.0.255 192.168.100.0 0.0.0.255
permit ip 10.22.22.0 0.0.0.255 any
!
!
!--- Passing PPTP traffic includes allowing GRE IP protocol 47.
!
ip access-list extended PPTP-PASS-THROUGH
permit gre any any
!
!--- PPTP terminated traffic involves GRE and TCP port 1723 traffic.
!
ip access-list extended PPTP-TERMINATED
permit gre any any
permit tcp any any eq 1723
!
!--- Allowing Telnet, SSH and HTTPS access
!
ip access-list extended Router-Access
permit tcp any any eq telnet
permit tcp any any eq 22
permit tcp any any eq 443
!
control-plane
!
!
line con 0
no modem enable
line aux 0
line vty 0 4
login authentication VTY
transport input telnet ssh
!
scheduler max-task-time 5000
end

```

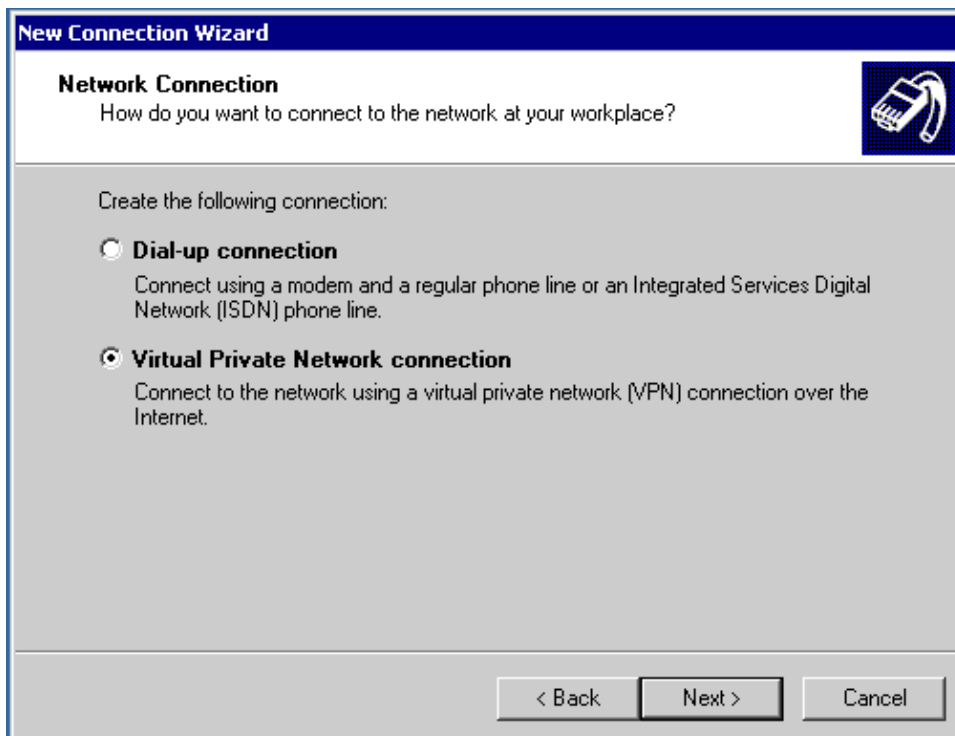
PPTP Client Configuration and Settings

Complete these steps:

1. Choose **Start > Settings > Network and Dial-up Connections > Make New Connection**.
2. After the Network Connection Wizard window appears, choose **Network Connection Type > Connect to the network at my workplace** and click **Next**.



3. Choose **Virtual Private Network connection**.



4. Specify a **Connection Name**.

New Connection Wizard

Connection Name
Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

Company Name

Cisco Systems

For example, you could type the name of your workplace or the name of a server you will connect to.

< Back Next > Cancel

5. Specify a Destination Address in the Host or IP address field and click **Next**.

New Connection Wizard

VPN Server Selection
What is the name or address of the VPN server?

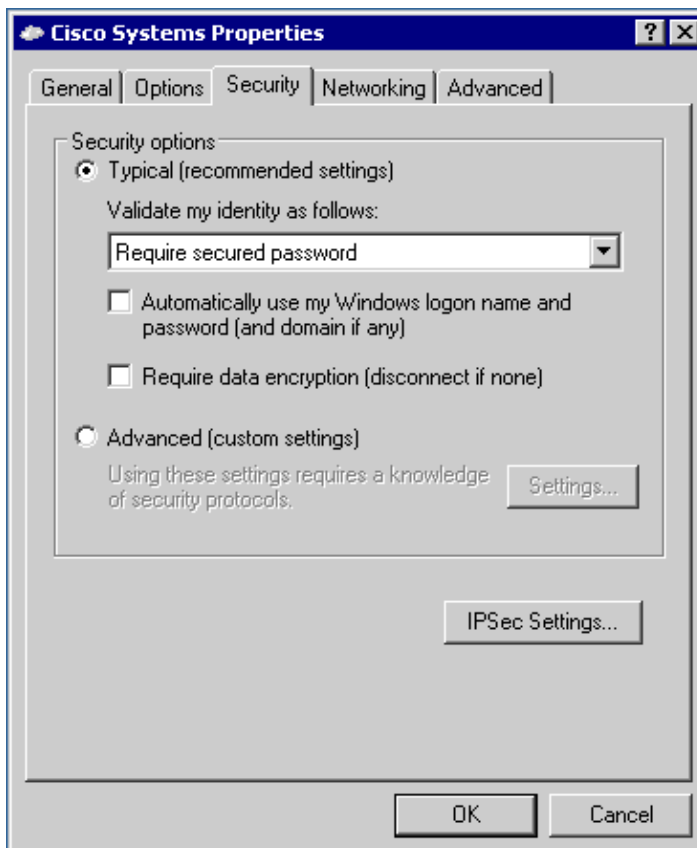
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

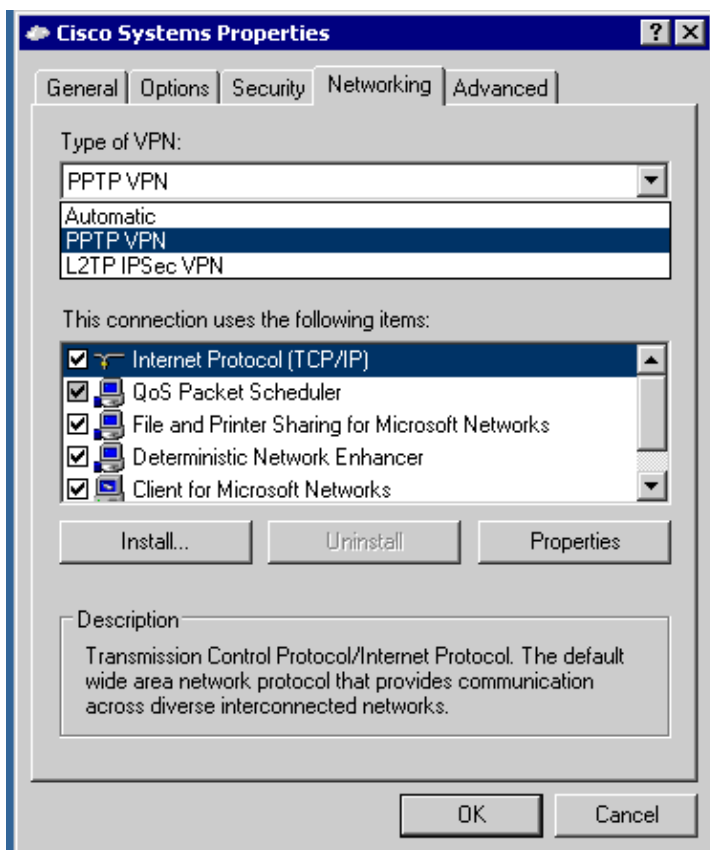
10.66.79.73

< Back Next > Cancel

6. Choose **Start > Settings > Network and Dial up connections** and select the recently configured connection.
7. After this window appears, choose **Properties > Security** in order to set the option properly.
8. Choose **Advanced (customer settings) > Settings**, and choose the appropriate encryption (Data Encryption) level and authentication (allow these protocols) if needed.



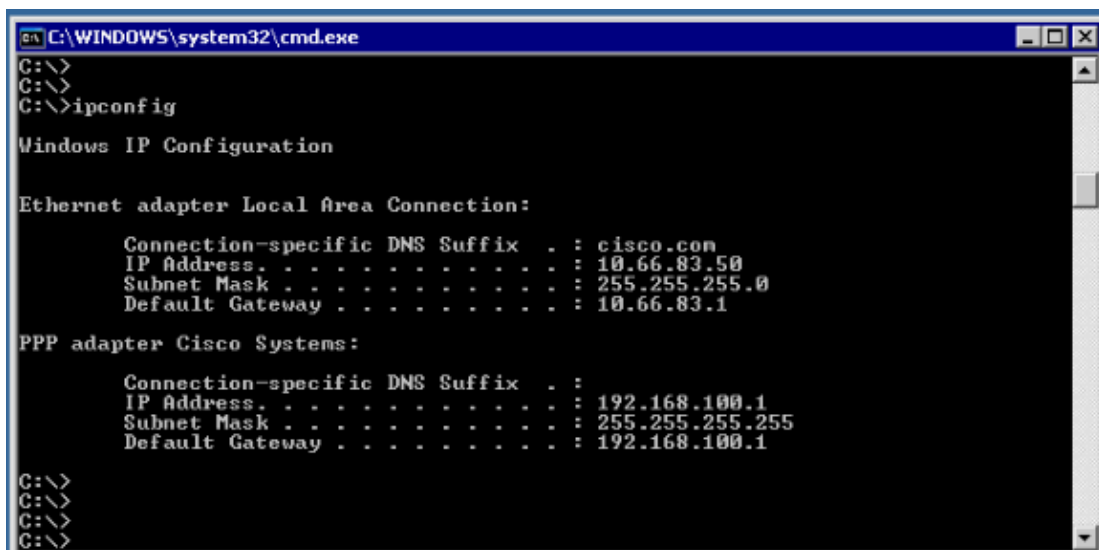
9. Choose **Networking > Type of VPN > PPTP VPN** and click **OK**.



10. Enter the username and password to be used for the PPTP connection.



11. The Verifying username and password window appears.
12. The Registering your computer on the network window appears.
13. If you verify the Remote PC, you get an IP address from the configured pool.



Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

1. Router#show vpdn

```

%No active L2TP tunnels

PPTP Tunnel and Session Information Total tunnels 1 sessions 1

LocID Remote Name      State      Remote Address  Port  Sessions VPDN Group

```

```
3          estab  10.66.83.50    1040  1          PPTP-VPDN
```

```
LocID RemID TunID Intf   Username      State   Last Chg Uniq ID
3      32768 3      Vi2.1  cisco        estab   00:00:57 2
```

2. Router#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0	unassigned	YES	unset	up	up
FastEthernet1	unassigned	YES	unset	up	down
FastEthernet2	unassigned	YES	unset	up	down
FastEthernet3	unassigned	YES	unset	up	down
FastEthernet4	10.66.79.73	YES	manual	up	up
Dot11Radio0	unassigned	YES	unset	down	down
SSLVPN-VIF0	unassigned	NO	unset	up	up
Vlan1	10.22.22.1	YES	manual	up	up
NV10	unassigned	NO	unset	up	up
Virtual-Template1	10.66.79.73	YES	TFTP	down	down
Virtual-Access1	unassigned	YES	unset	down	down
Virtual-Access2	unassigned	YES	unset	up	up
Virtual-Access2.1	10.66.79.73	YES	TFTP	up	up

3. Router#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.66.79.65 to network 0.0.0.0

```
C    10.22.22.0/24 is directly connected, Vlan1
    10.0.0.0/27 is subnetted, 1 subnets
C    10.66.79.64 is directly connected, FastEthernet4
    192.168.100.0/32 is subnetted, 1 subnets
C    192.168.100.1 is directly connected, Virtual-Access2.1
S*   0.0.0.0/0 [1/0] via 10.66.79.65
```

4. Router#show users

Line	User	Host(s)	Idle	Location
* 0 con 0		idle	00:00:00	

Interface	User	Mode	Idle	Peer Address
Vi2.1	cisco	PPPoVPDN	-	192.168.100.1

5. Ping from the connected client to the Internal Server

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\snallasa\Desktop>ping 10.22.22.10

Pinging 10.22.22.10 with 32 bytes of data:

Reply from 10.22.22.10: bytes=32 time<1ms TTL=128
Reply from 10.22.22.10: bytes=32 time<1ms TTL=128
Reply from 10.22.22.10: bytes=32 time<1ms TTL=128
Reply from 10.22.22.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.22.22.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\snallasa\Desktop>
```

6. Router#show policy-map type inspect zone-pair sessions

```
policy exists on zp outside-self
Zone-pair: outside-self

Service-policy inspect : Out-Self-Policy

Class-map: Router-Access-Traffic (match-all)
  Match: access-group name Router-Access
  Pass
    14 packets, 358 bytes

Class-map: PPTP-Terminated-Traffic (match-all)
  Match: access-group name PPTP-TERMINATED
  Pass
    52 packets, 4466 bytes

Class-map: class-default (match-any)
  Match: any
  Drop
    21 packets, 1680 bytes

policy exists on zp pptp-in
Zone-pair: pptp-in

Service-policy inspect : PPTP-In-Policy

Class-map: All-Traffic (match-any)
  Match: protocol tcp
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol udp
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol icmp
    1 packets, 40 bytes
    30 second rate 0 bps

Inspect

Class-map: class-default (match-any)
  Match: any
```

```
Drop
  0 packets, 0 bytes

policy exists on zp inside-outside
Zone-pair: inside-outside

Service-policy inspect : In-Out-Policy
```

```
Class-map: PPTP-Pass-Through-Traffic (match-all)
Match: access-group name PPTP-PASS-THROUGH
Pass
  4 packets, 320 bytes
```

```
Class-map: All-Traffic (match-any)
Match: protocol tcp
  31 packets, 868 bytes
  30 second rate 0 bps
Match: protocol udp
  20 packets, 1271 bytes
  30 second rate 0 bps
Match: protocol icmp
  0 packets, 0 bytes
  30 second rate 0 bps
```

```
Inspect
```

```
Number of Half-open Sessions = 6
```

```
Half-open Sessions
```

```
Session 83B5B920 (10.22.22.10:2135)=>(10.66.79.245:443) https:tcp SIS_OPENING
  Created 00:00:26, Last heard 00:00:26
  Bytes sent (initiator:responder) [0:0]
Session 83B5BB20 (10.66.79.241:138)=>(10.66.79.255:138) netbios-dgm:udp SIS_OPENING
  Created 00:00:26, Last heard 00:00:13
  Bytes sent (initiator:responder) [406:0]
Session 83B5BD20 (192.168.212.14:138)=>(192.168.212.255:138) netbios-dgm:udp SIS_OPENING
  Created 00:00:23, Last heard 00:00:23
  Bytes sent (initiator:responder) [233:0]
Session 83B5C120 (10.22.22.10:2138)=>(10.66.79.245:443) https:tcp SIS_OPENING
  Created 00:00:19, Last heard 00:00:19
  Bytes sent (initiator:responder) [0:0]
Session 83B5C320 (10.22.22.10:2142)=>(10.66.79.245:443) https:tcp SIS_OPENING
  Created 00:00:12, Last heard 00:00:12
  Bytes sent (initiator:responder) [0:0]
Session 83B5C520 (10.22.22.10:2145)=>(10.66.79.245:443) https:tcp SIS_OPENING
  Created 00:00:05, Last heard 00:00:05
  Bytes sent (initiator:responder) [0:0]
```

```
Class-map: class-default (match-any)
Match: any
Drop
  0 packets, 0 bytes
```

7. Router#show debugging

```
PPP:
  PPP authentication debugging is on
  PPP protocol negotiation debugging is on
VPN:
  VPDN events debugging is on
```

```
!--- When the PPTP User is connecting
```

```
*Mar 13 02:22:40.535: VPDN Received L2TUN socket message <xCRQ - Session Incoming>
*Mar 13 02:22:40.547: VPDN Tnl/Sn 2 2 L2TUN socket session accept requested
```

```
*Mar 13 02:22:40.547: VPDN Tnl/Sn 2 2 Setting up dataplane for L2-L2, no idb
*Mar 13 02:22:40.567: VPDN Received L2TUN socket message <xCCN - Session Connected>
*Mar 13 02:22:40.595: VPDN uid:1 VPDN session up
*Mar 13 02:22:40.607: ppp1 PPP: Send Message[Dynamic Bind Response]
*Mar 13 02:22:40.607: ppp1 PPP: Using vpn set call direction
*Mar 13 02:22:40.607: ppp1 PPP: Treating connection as a callin
*Mar 13 02:22:40.607: ppp1 PPP: Session handle[8000003] Session id[1]
*Mar 13 02:22:40.607: ppp1 PPP: Phase is ESTABLISHING, Passive Open
*Mar 13 02:22:40.607: ppp1 LCP: State is Listen
*Mar 13 02:22:42.563: ppp1 LCP: I CONFREQ [Listen] id 1 len 21
*Mar 13 02:22:42.563: ppp1 LCP: MRU 1400 (0x01040578)
*Mar 13 02:22:42.563: ppp1 LCP: MagicNumber 0x069878CA (0x0506069878CA)
*Mar 13 02:22:42.563: ppp1 LCP: PFC (0x0702)
*Mar 13 02:22:42.563: ppp1 LCP: ACFC (0x0802)
*Mar 13 02:22:42.563: ppp1 LCP: Callback 6 (0x0D0306)
*Mar 13 02:22:42.563: ppp1 PPP: Authorization NOT required
*Mar 13 02:22:42.563: ppp1 LCP: O CONFREQ [Listen] id 1 len 15
*Mar 13 02:22:42.563: ppp1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 13 02:22:42.563: ppp1 LCP: MagicNumber 0x14AF18DB (0x050614AF18DB)
*Mar 13 02:22:42.563: ppp1 LCP: O CONFREQ [Listen] id 1 len 7
*Mar 13 02:22:42.563: ppp1 LCP: Callback 6 (0x0D0306)
*Mar 13 02:22:42.567: ppp1 LCP: I CONFACK [REQsent] id 1 len 15
*Mar 13 02:22:42.567: ppp1 LCP: AuthProto CHAP (0x0305C22305)
*Mar 13 02:22:42.567: ppp1 LCP: MagicNumber 0x14AF18DB (0x050614AF18DB)
*Mar 13 02:22:42.567: ppp1 LCP: I CONFREQ [ACKrcvd] id 2 len 18
*Mar 13 02:22:42.567: ppp1 LCP: MRU 1400 (0x01040578)
*Mar 13 02:22:42.567: ppp1 LCP: MagicNumber 0x069878CA (0x0506069878CA)
*Mar 13 02:22:42.567: ppp1 LCP: PFC (0x0702)
*Mar 13 02:22:42.567: ppp1 LCP: ACFC (0x0802)
*Mar 13 02:22:42.567: ppp1 LCP: O CONFNAK [ACKrcvd] id 2 len 8
*Mar 13 02:22:42.567: ppp1 LCP: MRU 1500 (0x010405DC)
*Mar 13 02:22:42.571: ppp1 LCP: I CONFREQ [ACKrcvd] id 3 len 18
*Mar 13 02:22:42.571: ppp1 LCP: MRU 1400 (0x01040578)
*Mar 13 02:22:42.571: ppp1 LCP: MagicNumber 0x069878CA (0x0506069878CA)
*Mar 13 02:22:42.571: ppp1 LCP: PFC (0x0702)
*Mar 13 02:22:42.571: ppp1 LCP: ACFC (0x0802)
*Mar 13 02:22:42.571: ppp1 LCP: O CONFNAK [ACKrcvd] id 3 len 8
*Mar 13 02:22:42.571: ppp1 LCP: MRU 1500 (0x010405DC)
*Mar 13 02:22:42.571: ppp1 LCP: I CONFREQ [ACKrcvd] id 4 len 18
*Mar 13 02:22:42.571: ppp1 LCP: MRU 1500 (0x010405DC)
*Mar 13 02:22:42.571: ppp1 LCP: MagicNumber 0x069878CA (0x0506069878CA)
*Mar 13 02:22:42.571: ppp1 LCP: PFC (0x0702)
*Mar 13 02:22:42.571: ppp1 LCP: ACFC (0x0802)
*Mar 13 02:22:42.575: ppp1 LCP: O CONFACK [ACKrcvd] id 4 len 18
*Mar 13 02:22:42.575: ppp1 LCP: MRU 1500 (0x010405DC)
*Mar 13 02:22:42.575: ppp1 LCP: MagicNumber 0x069878CA (0x0506069878CA)
*Mar 13 02:22:42.575: ppp1 LCP: PFC (0x0702)
*Mar 13 02:22:42.575: ppp1 LCP: ACFC (0x0802)
*Mar 13 02:22:42.575: ppp1 LCP: State is Open
*Mar 13 02:22:42.575: ppp1 PPP: Phase is AUTHENTICATING, by this end
*Mar 13 02:22:42.575: ppp1 CHAP: O CHALLENGE id 1 len 33 from "Router"
*Mar 13 02:22:42.575: ppp1 LCP: I IDENTIFY [Open] id 5 len 18 magic 0x069878CA MSRAS
*Mar 13 02:22:42.579: ppp1 LCP: I IDENTIFY [Open] id 6 len 31 magic 0x069878CA MSRAS
*Mar 13 02:22:42.579: ppp1 CHAP: I RESPONSE id 1 len 26 from "cisco"
*Mar 13 02:22:42.579: ppp1 PPP: Phase is FORWARDING, Attempting Forward
*Mar 13 02:22:42.579: ppp1 PPP: Phase is AUTHENTICATING, Unauthenticated User
*Mar 13 02:22:42.579: ppp1 PPP: Sent CHAP LOGIN Request
*Mar 13 02:22:42.583: ppp1 PPP: Received LOGIN Request PASS
*Mar 13 02:22:42.583: ppp1 PPP: Phase is FORWARDING, Attempting Forward
*Mar 13 02:22:42.583: ppp1 PPP: Send Message[Connect Local]
L2X_ADJ: Vi2.1:midchain adj reqd for ip 0.0.0.0, cid 0
L2X_ADJ: Vi2.1:midchain adj reqd for ip 0.0.0.0, cid 0
*Mar 13 02:22:42.619: VPDN Vi2.1 Virtual interface created for unknown, bandwidth 10
*Mar 13 02:22:42.619: VPDN Vi2.1 Setting up dataplane for L2-L3, Vi2.1
*Mar 13 02:22:42.623: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
L2X_ADJ: Vi2.1:allocated ctx, size 1
```

```

*Mar 13 02:22:42.627: VPDN Received L2TUN socket message <Dataplane UP>
*Mar 13 02:22:42.627: ppp1 PPP: Bind to [Virtual-Access2.1]
*Mar 13 02:22:42.631: Vi2.1 PPP: Send Message[Static Bind Response]
*Mar 13 02:22:42.631: Vi2.1 PPP: Phase is AUTHENTICATING, Authenticated User
*Mar 13 02:22:42.631: Vi2.1 CHAP: O SUCCESS id 1 len 4
*Mar 13 02:22:42.635: Vi2.1 PPP: Phase is UP
*Mar 13 02:22:42.639: Vi2.1 IPCP: O CONFREQ [Closed] id 1 len 10
*Mar 13 02:22:42.639: Vi2.1 IPCP: Address 10.66.79.73 (0x03060A424F49)
*Mar 13 02:22:42.639: Vi2.1 PPP: Process pending ncp packets
*Mar 13 02:22:42.643: Vi2.1 CCP: I CONFREQ [Not negotiated] id 7 len 10
*Mar 13 02:22:42.643: Vi2.1 CCP: MS-PPC supported bits 0x01000001 (0x120601000001)
*Mar 13 02:22:42.643: Vi2.1 LCP: O PROTREJ [Open] id 2 len 16 protocol CCP (0x80FD01)
*Mar 13 02:22:42.643: Vi2.1 IPCP: I CONFREQ [REQsent] id 8 len 34
*Mar 13 02:22:42.643: Vi2.1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 13 02:22:42.643: Vi2.1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 13 02:22:42.643: Vi2.1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 13 02:22:42.643: Vi2.1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 13 02:22:42.643: Vi2.1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 13 02:22:42.643: Vi2.1 IPCP: Pool returned 192.168.100.1
*Mar 13 02:22:42.643: Vi2.1 IPCP: O CONFREQ [REQsent] id 8 len 28
*Mar 13 02:22:42.647: Vi2.1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 13 02:22:42.647: Vi2.1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 13 02:22:42.647: Vi2.1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 13 02:22:42.647: Vi2.1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 13 02:22:42.647: Vi2.1 IPCP: I CONFACK [REQsent] id 1 len 10
*Mar 13 02:22:42.647: Vi2.1 IPCP: Address 10.66.79.73 (0x03060A424F49)
*Mar 13 02:22:42.647: Vi2.1 IPCP: I CONFREQ [ACKrcvd] id 9 len 10
*Mar 13 02:22:42.651: Vi2.1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 13 02:22:42.651: Vi2.1 IPCP: O CONFNAK [ACKrcvd] id 9 len 10
*Mar 13 02:22:42.651: Vi2.1 IPCP: Address 192.168.100.1 (0x0306C0A86401)
*Mar 13 02:22:42.651: Vi2.1 IPCP: I CONFREQ [ACKrcvd] id 10 len 10
*Mar 13 02:22:42.651: Vi2.1 IPCP: Address 192.168.100.1 (0x0306C0A86401)
*Mar 13 02:22:42.651: Vi2.1 IPCP: O CONFACK [ACKrcvd] id 10 len 10
*Mar 13 02:22:42.651: Vi2.1 IPCP: Address 192.168.100.1 (0x0306C0A86401)
*Mar 13 02:22:42.651: Vi2.1 IPCP: State is Open
L2X_ADJ: Vi2.1:adj notify change, event 2
L2X_ADJ: Vi2.1:midchain stacking IP 0.0.0.0 to 10.66.83.50 (VRF 0)
L2X_ADJ: Vi2.1:adj notify change, event 8
L2X_ADJ: Vi2.1:adj notify change, event 3
*Mar 13 02:22:42.655: Vi2.1 IPCP: Install route to 192.168.100.1
*Mar 13 02:22:43.623: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access2, changed state to up

```

!--- When the PPTP User is disconnecting

```

*Mar 13 02:23:05.571: Vi2.1 LCP: I TERMREQ [Open] id 11 len 16 (0x069878CA003CCD7400)
*Mar 13 02:23:05.571: Vi2.1 LCP: O TERMACK [Open] id 11 len 4
*Mar 13 02:23:05.575: Vi2.1 PPP: Sending Acct Event[Down] id[4]
*Mar 13 02:23:05.575: Vi2.1 PPP: Phase is TERMINATING
*Mar 13 02:23:05.779: VPDN Received L2TUN socket message <CDN - Session Disconnected>
*Mar 13 02:23:05.779: VPDN Vi2.1 disconnect (AAA) IETF: 1/user-request Ascend: 28/PE
*Mar 13 02:23:05.779: VPDN Vi2.1 vpdn shutdown session, result=2, error=6, vendor_err=0
*Mar 13 02:23:05.779: VPDN Vi2.1 VPDN/AAA: accounting stop sent
*Mar 13 02:23:05.783: VPDN Vi2.1 Unbinding session from idb
*Mar 13 02:23:05.783: Vi2.1 VPDN: Resetting interface
*Mar 13 02:23:05.783: Vi2.1 PPP: Block vaccess from being freed [0x19]
*Mar 13 02:23:05.783: Vi2.1 PPP: Received Disconnect from Lower Layer
L2X_ADJ: Vi2.1:midchain unstacking IP 0.0.0.0
L2X_ADJ: Vi2.1:adj notify change, event 8
L2X_ADJ: Vi2.1:removed ctx
*Mar 13 02:23:05.807: Vi2.1 LCP: State is Closed
*Mar 13 02:23:05.807: Vi2.1 PPP: Phase is DOWN
*Mar 13 02:23:05.807: Vi2.1 IPCP: State is Closed
*Mar 13 02:23:05.807: Vi2.1 PPP: Unlocked by [0x1] Still Locked by [0x18]

```

```
*Mar 13 02:23:05.807: Vi2.1 PPP: Unlocked by [0x10] Still Locked by [0x8]
*Mar 13 02:23:05.811: Vi2.1 PPP: Unlocked by [0x8] Still Locked by [0x0]
*Mar 13 02:23:05.811: Vi2.1 PPP: Free previously blocked vaccess
```

Troubleshoot

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

1. Make sure that traffic destined to the Router allows for TCP port 1723 and GRE traffic.
2. Make sure that PPTP pass through traffic allows GRE through the Router.
3. Be careful of defect CSCsr41631; this is overcome with the use of different zones for the External interface and the Virtual–Template interface.

Related Information

- [Cisco IOS Firewall](#)
- [Technical Support & Documentation – 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: May 18, 2009

Document ID: 110353
