PPTP Frequently Asked Questions

Document ID: 18761

Contents

Introduction
Hardware
Troubleshoot
Related Information

Introduction

This document addresses frequently asked questions about Point−to−Point Tunnel Protocol (PPTP).

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

Hardware

Q. How can I determine what platforms support PPTP?

A. You can determine which Cisco IOS® Software releases support PPTP by using the Feature Navigator tool (registered customers only) . The tool allows you to compare Cisco IOS software releases, match Cisco IOS software and CatOS features to releases, and find out which software release you need to support your hardware.

Q. When was PPTP first introduced in the Cisco Secure PIX Firewall?

A. PPTP was first introduced in Cisco Secure PIX firewall version 5.1. Refer to PIX 6.x: PPTP with Radius Authentication Configuration Example for more information.

Note: PPTP termination on the PIX firewall feature is not supported in version 7.x and later.

Q. Are there details about Microsoft Point−to−Point Encryption (MPPE) that I need to be aware of?

A. MPPE requires Microsoft Challenge Handshake Authentication Protocol (MS−CHAP). It only works with RADIUS or local authentication, and the RADIUS server must support the MPPE−Keys attribute value.

This list shows some platforms and their MPPE compatibility.

- Cisco Secure ACS for UNIX (CSUNIX) − No
- Access Registrar − No
- Funk RADIUS − Yes
- Cisco Secure ACS for Windows − Yes
- Microsoft Windows 2000 Internet Authentication Server − Yes

Q. What version of Cisco IOS software supported PPTP initially?

A. PPTP was initially supported in Cisco IOS Software Release 12.0(5)XE5 on the Cisco 7100/7200 routers. It then moved to Cisco IOS general platform support in Cisco IOS Software Release 12.1(5)T.

Q. What are some known compatibility issues with the Microsoft PPTP products and the VPN 3000 Concentrator?

A. This information is based on VPN 3000 Series Concentrator software releases 3.5 and later; VPN 3000 Series Concentrators, Models 3005, 3015, 3030, 3060, 3080; and Microsoft Operating Systems Windows 95 and later.

- **Windows 95 Dial−Up Networking (DUN) 1.2**

  Microsoft Point−to−Point Encryption (MPPE) is not supported under DUN 1.2. Install Windows 95 DUN 1.3 to connect using MPPE. You can download the Microsoft DUN 1.3 upgrade from the Microsoft web site.
- **Windows NT 4.0**

  Windows NT is fully supported for PPTP connections to the VPN Concentrator. Service Pack 3 (SP3) or later is required. If you run SP3, install the PPTP Performance and Security patches. Refer to Microsoft's web site for information about the PPTP Performance and Security Upgrade for WinNT 4.0 . The only resolution for this is to reinstall the NT 4.0 Server Option Pack without adding the Service Pack afterwards.

  Note: The 128−bit Service Pack 5 does not handle MPPE keys correctly, and PPTP can fail to pass data. When this occurs, the event log shows this message.

  ```
  103 12/09/1999 09:08:01.550 SEV=6 PPP/4 RPT=3 80.50.0.4
  User [ testuser ]
  disconnected. Experiencing excessive packet decrypt failure.
  ```

  Refer to the Microsoft article MPPE Keys Not Handled Correctly for a 128−Bit MS−CHAP Request for more information.

Q. Do Cisco IOS routers or PIX Firewalls support PPTP pass through or PPTP over Port Address Translation (PAT) feature?

A. Cisco IOS Software Releases 12.1T and later support PPTP pass through or PPTP over PAT feature. Refer to the "NAT − Support for PPTP in an Overload (Port Address Translation) Configuration" section in Cisco IOS Software 12.1T Early Deployment Release Series for more information. Refer to IP Tunneling − Configuring PPTP Through PAT to a Microsoft PPTP Server to configure PPTP over PAT or PPTP pass through on a Cisco IOS router.

PIX versions 6.3 and later support PPTP pass through or PPTP over PAT using the PPTP fixup feature. This feature allows PPTP traffic to traverse the PIX when configured for PAT. The PIX performs stateful PPTP packet inspection in the process. Refer to the section on PPTP configuration in Configuring Application Inspection (Fixup) to configure PPTP fixup on the PIX. The **fixup protocol pptp 1723** command configures PPTP fixup.

Troubleshoot

Q. What ports should I open on a firewall in order to accommodate PPTP tunnels?

A. Open these ports.

- TCP/1723
- IP Protocol/47 GRE

Refer to Permitting PPTP Connections Through the PIX for more information.

Q. What are the known Cisco IOS Software PPTP bugs?

A. These bugs have been identified:

- CSCdt46181 (registered customers only) − Refer to Cisco IOS PPTP Vulnerability for more information.
- CSCdz47290 (registered customers only) − PPTP fast/process switching broken when Cisco Express Forwarding (CEF) is enabled globally.
- CSCdx86482 (registered customers only) − PPTP tunneling has broken.
- CSCdt11570 (registered customers only) − 128−bit Microsoft Point−to−Point Encryption (MPPE) does not work on hardware Integrated Services Module (ISM).
- CSCdt66607 (registered customers only) − PPTP 128−bit MPPE does not work with Cisco Secure ACS for Windows.
- CSCdu19654 (registered customers only) − PPTP fails.
- CSCdv50861 (registered customers only) − MPPE does not negotiate with Windows 2000.

Registered customers can view bug details by using the Cisco Bug Toolkit (registered customers only) for more information.

Q. What are some limitations to PPTP?

A. These are some limitations to PPTP.

- PPTP only supports Cisco Express Forwarding (CEF) and process−switching. Fast switching is not supported.
- Cisco IOS software only supports voluntary tunneling as PPTP Network Server (PNS).
- You need crypto images for MPPE support. MPPE requires Microsoft Challenge Authentication Protocol (MS−CHAP) authentication, and MPPE is not supported with TACACS+.

Q. What significant debugging events should I look for when I troubleshoot PPTP on a router?

A. Look for these debugs.

- **debug aaa authentication**
- **debug aaa authorization**
- **debug radius**
- **debug ppp negotiation**

- **debug ppp authentication**
- **debug vpdn events**
- **debug vpdn errors**
- **debug vpdn l2x−packet**
- **debug ppp mppe events**
- **debug ppp chap**

Look for these significant events.

```
SCCRQ = Start−Control−Connection−Request −
   message code bytes 9 and 10 = 0001
SCCRP = Start−Control−Connection−Reply
OCRQ = Outgoing−Call−Request −
   message code bytes 9 and 10 = 0007
OCRP = Outgoing−Call−Reply
```

Q. What does it mean when I receive the message "Error 734" and then get disconnected?

A. This error indicates that the router and the PC cannot negotiate authentication. For example, if you set the PC authentication protocols for Shiva PAP (SPAP) and Microsoft Challenge Authentication Protocol (MS−CHAP) version 2 (when the router is unable to do version 2), and you set the router for CHAP, then the **debug ppp negotiation** command on the router displays this output.

```
04:30:55: Vi1 LCP: Failed to negotiate with peer
```

Another example is if the router is set for **vpdn group 1 ppp encrypt mppe 40 required** and the PC is set for "no encryption allowed." The PC does not connect and produces an "Error 734," and the **debug ppp negotiation** command on the router displays this output.

```
04:51:55: Vi1 LCP: I PROTREJ
      [Open] id 3 len 16 protocol CCP (0x80FD0157000A120601000020)
```

Q. What does "Error 742" mean?

A. This error means that the remote computer does not support the required data encryption type. For example, if you set the PC for "encrypted only" and delete the **pptp encrypt mppe auto** command from the router, then the PC and the router cannot agree on encryption. The **debug ppp negotiation** command shows this output.

```
04:41:09: Vi1 LCP: O PROTREJ
      [Open] id 5 len 16 protocol CCP (0x80FD0102000A1206010000B0)
```

Another example involves the router MPPE RADIUS problem. If you set the router for **ppp encrypt mppe auto required** and the PC for "encryption allowed with authentication to a RADIUS server not returning the MPPE key," then you get an error on the PC that states, "`Error 742: The remote computer does not support the required data encryption type`." The router debug shows a "Call−Clear−Request" (bytes 9 and 10 = 0x000C = 12 = Call−Clear−Request per RFC) as seen here.

```
00:45:58: Tnl 17 PPTP: CC I 001000011A2B3C4D000C000000000000
00:45:58: Vi1 Tnl/Cl 17/17 PPTP: CC I ClearRQ
```

Q. I think I have a split tunneling issue. What should I do when a PPTP tunnel comes up on a PC, the PPTP router has a higher metric than the previous default, and I lose connectivity?

A. Run a batch file (batch.bat) to modify the Microsoft routing to resolve this problem. Delete the default and reinstall the default route (you must know the IP address that the PPTP client was assigned, such as 192.168.1.1).

In this example, the network inside the router is 10.13.1.x.

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 161.44.17.1 metric 1
route add 10.13.1.0 mask 255.255.255.0 192.168.1.1 metric 1
```

Q. What are some issues to consider when I troubleshoot PPTP?

A. Several Microsoft−related issues to consider when you troubleshoot PPTP are listed here. Detailed information is available from the Microsoft Knowledge Base at the links provided.

- How to Keep RAS Connections Active After Logging Off

  Windows Remote Access Service (RAS) connections are automatically disconnected when you log off from a RAS client. You can remain connected by enabling the **KeepRasConnections** registry key on the RAS client.
- User Is Not Alerted When Logging On With Cached Credentials

  If you are logging on to a domain from a Windows−based workstation or member server and the domain controller cannot be located, you do not receive an error message indicating this issue. Instead, you are logged on to the local computer using cached credentials.
- How to Write an LMHOSTS File for Domain Validation and Other Name Resolution Issues

  If you experience name resolution issues on your TCP/IP network, you might need to use Lmhosts files to resolve NetBIOS names. You must follow a specific procedure to create an Lmhosts file to use in name resolution and domain validation.

Related Information

- **PPTP Support Page**
- **PIX Support Page**
- **VPN 3000 Series Concentrators Support Page**
- **RFC 2637: Point−to−Point Tunneling Protocol (PPTP)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 24, 2009 Document ID: 18761