

Häufig gestellte Fragen zu PPTP

Inhalt

[Einführung](#)

[Hardware](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument behandelt häufig gestellte Fragen zum Point-to-Point Tunnel Protocol (PPTP).

Weitere Informationen zu Dokumentkonventionen finden Sie in den [in Cisco Technical Tips verwendeten Konventionen](#).

Hardware

F. Wie kann ich feststellen, welche Plattformen PPTP unterstützen?

Antwort: Sie können mithilfe des [Feature Navigator-Tools](#) ermitteln, welche Cisco IOS® Software-Versionen PPTP unterstützen (nur registrierte Kunden). Mit diesem Tool können Sie Cisco IOS-Softwareversionen vergleichen, Cisco IOS-Software- und CatOS-Funktionen mit Versionen abgleichen und herausfinden, welche Softwareversion Sie zur Unterstützung Ihrer Hardware benötigen.

F. Wann wurde PPTP erstmals in der Cisco Secure PIX Firewall eingeführt?

Antwort: PPTP wurde erstmals in Version 5.1 der Cisco Secure PIX-Firewall eingeführt. Siehe [PIX 6.x: PPTP mit Radius-Authentifizierungskonfiguration - Beispiel](#) für weitere Informationen.

Hinweis: PPTP-Terminierung auf der PIX-Firewall wird in Version 7.x und höher nicht unterstützt.

F. Gibt es Einzelheiten zur Microsoft Point-to-Point Encryption (MPPE), die ich beachten muss?

Antwort: MPPE erfordert das Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). Sie funktioniert nur mit RADIUS- oder lokaler Authentifizierung, und der RADIUS-Server muss den MPPE-Keys-Attributwert unterstützen.

Diese Liste zeigt einige Plattformen und deren MPPE-Kompatibilität.

- Cisco Secure ACS für UNIX (CSUNIX) - Nein
- Registrar aufrufen - Nein

- Funk RADIUS - Ja
- Cisco Secure ACS für Windows - Ja
- Microsoft Windows 2000 Internet Authentication Server - Ja

F. Welche Version der Cisco IOS-Software unterstützt PPTP ursprünglich?

Antwort: PPTP wurde ursprünglich von der Cisco IOS Software, Version 12.0(5)XE5, auf den Cisco 7100/7200-Routern unterstützt. Anschließend wechselte es zur allgemeinen Unterstützung der Cisco IOS-Plattform in Version 12.1(5)T der Cisco IOS-Software.

F. Welche Kompatibilitätsprobleme sind mit den Microsoft PPTP-Produkten und dem VPN 3000 Concentrator bekannt?

Antwort: Diese Informationen basieren auf der VPN Concentrator-Software der Serie 3.5 und höher. VPN Concentrators der Serie 3000, Modelle 3005, 3015, 3030, 3060, 3080; und Microsoft-Betriebssysteme Windows 95 und höher.

- **Windows 95-DFÜ-Netzwerk (DUN) 1.2** Microsoft Point-to-Point Encryption (MPPE) wird unter DUN 1.2 nicht unterstützt. Installieren Sie Windows 95 DUN 1.3, um eine Verbindung über MPPE herzustellen. Sie können das [Microsoft DUN 1.3-Upgrade](#) von der Microsoft-Website herunterladen.
- **Windows NT 4.0** Windows NT wird vollständig für PPTP-Verbindungen mit dem VPN Concentrator unterstützt. Service Pack 3 (SP3) oder höher ist erforderlich. Wenn Sie SP3 ausführen, installieren Sie die PPTP-Leistungs- und Sicherheitspatches. Weitere Informationen zur [PPTP Performance and Security Upgrade for WinNT 4.0](#) finden Sie auf der Microsoft-Website. Die einzige Lösung dafür ist die Neuinstallation des NT 4.0 Server-Option Pack ohne anschließendes Hinzufügen des Service Packs. **Hinweis:** Das 128-Bit-Service Pack 5 behandelt MPPE-Schlüssel nicht korrekt, und PPTP kann keine Daten übergeben. In diesem Fall wird diese Meldung im Ereignisprotokoll angezeigt.

```
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.
```

Weitere Informationen finden Sie im Microsoft-Artikel [MPPE-Schlüssel nicht korrekt behandelt für eine 128-Bit-MS-CHAP-Anforderung](#) .

F. Unterstützen Cisco IOS-Router oder PIX-Firewalls die PTP-Passthrough- oder PPTP-over-Port Address Translation (PAT)-Funktion?

Antwort: Die Cisco IOS Software-Versionen 12.1T und höher unterstützen die PPTP-Passthrough- oder PPTP-over-PAT-Funktion. Weitere Informationen finden Sie im Abschnitt "NAT - Support for PPTP in an Overload (Port Address Translation) Configuration" in der [Cisco IOS Software 12.1T Early Deployment Release Series](#). Informationen zur Konfiguration von PPTP über PAT oder PPTP-Passthrough auf einem Cisco IOS-Router finden Sie unter [IP Tunneling - Configuring PPTP Through PAT to a Microsoft PPTP Server](#).

PIX-Versionen 6.3 und höher unterstützen PPTP-Passthrough oder PPTP-over-PAT mithilfe der PPTP-Fixup-Funktion. Mit dieser Funktion kann PPTP-Datenverkehr den PIX passieren, wenn er für PAT konfiguriert wurde. PIX führt dabei eine Stateful PPTP-Paketprüfung durch. Weitere Informationen zur [PPTP-Konfiguration](#) in [Configuring Application Inspection \(Fixup\)](#) zum Konfigurieren der PPTP-Fixup-Konfiguration für PIX finden Sie im Abschnitt zur [Konfiguration](#). Der

Befehl `fixup protocol pptp 1723` konfiguriert die PPTP-Fixup-Konfiguration.

Fehlerbehebung

F. Welche Ports sollten auf einer Firewall geöffnet werden, um PPTP-Tunnel unterzubringen?

Antwort: Öffnen Sie diese Ports.

- TCP/1723
- IP-Protokoll/47 GRE
Weitere Informationen finden Sie unter [Zulassen von PPTP-Verbindungen über das PIX](#).

F. Was sind die bekannten PPTP-Fehler der Cisco IOS Software?

Antwort: Diese Fehler wurden identifiziert:

- [CSCdt46181](#) (nur [registrierte](#) Kunden) - Weitere Informationen finden Sie unter [Cisco IOS PPTP-Schwachstelle](#).
- [CSCdz47290](#) (nur [registrierte](#) Kunden) - PPTP Fast/Process Switching, das bei Aktivierung von Cisco Express Forwarding (CEF) global unterbrochen wird.
- [CSCdx86482](#) (nur [registrierte](#) Kunden) - PPTP-Tunneling ist defekt.
- [CSCdt11570](#) (nur [registrierte](#) Kunden) - 128-Bit Microsoft Point-to-Point Encryption (MPPE) funktioniert nicht auf dem Hardware Integrated Services Module (ISM).
- [CSCdt66607](#) (nur [registrierte](#) Kunden) - PPTP 128-Bit MPPE funktioniert nicht mit Cisco Secure ACS für Windows.
- [CSCdu19654](#) (nur [registrierte](#) Kunden) - PPTP schlägt fehl.
- [CSCdv50861](#) (nur [registrierte](#) Kunden) - MPPE verhandelt nicht mit Windows 2000.

Registrierte Kunden können Fehlerdetails anzeigen, indem sie das [Cisco Bug Toolkit](#) verwenden ([nur registrierte](#) Kunden), um weitere Informationen zu erhalten.

F. Welche Einschränkungen gelten für PPTP?

Antwort: Dies sind einige Einschränkungen von PPTP.

- PPTP unterstützt nur Cisco Express Forwarding (CEF) und Prozess-Switching. Fast Switching wird nicht unterstützt.
- Die Cisco IOS-Software unterstützt nur das freiwillige Tunneling als PPTP Network Server (PNS).
- Sie benötigen Crypto-Images für MPPE-Unterstützung. MPPE erfordert Microsoft Challenge Authentication Protocol (MS-CHAP)-Authentifizierung, MPPE wird von TACACS+ nicht unterstützt.

F. Welche wichtigen Debugereignisse sollten bei der Fehlerbehebung für PPTP auf einem Router berücksichtigt werden?

Antwort: Suchen Sie nach diesen Debuggen.

- debuggen aaa authentication
- debuggen aaa autorisierung
- Debug-Radius
- Debug-ppp-Aushandlung
- Debug-ppp-Authentifizierung
- debuggen von VPN-Ereignissen
- Debuggen von vPdn-Fehlern
- debuggen vpdn l2x-paket
- debuggen ppp mppe-Ereignisse
- Debug-ppp-Kapitel

Suchen Sie nach diesen wichtigen Ereignissen.

```

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

```

F. Was bedeutet es, wenn ich die Meldung "Fehler 734" erhalte und die Verbindung dann getrennt werde?

Antwort: Dieser Fehler weist darauf hin, dass Router und PC keine Authentifizierung aushandeln können. Wenn Sie beispielsweise die PC-Authentifizierungsprotokolle für Shiva PAP (SPAP) und Microsoft Challenge Authentication Protocol (MS-CHAP) Version 2 (wenn der Router Version 2 nicht ausführen kann) festlegen und den Router für CHAP festlegen, wird diese Ausgabe durch den Befehl **debug ppp negotiation** auf dem Router angezeigt.

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

Ein weiteres Beispiel ist, wenn der Router für die **vPdn-Gruppe 1 ppp verschlüsselt mppe 40** festgelegt ist und der PC für "no encryption allowed" festgelegt ist. Der PC stellt keine Verbindung her und gibt einen "Fehler 734" aus. Der Befehl **debug ppp negotiation** auf dem Router zeigt diese Ausgabe an.

```

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

```

F. Was bedeutet "Fehler 742"?

Antwort: Dieser Fehler bedeutet, dass der Remote-Computer den erforderlichen Datenverschlüsselungstyp nicht unterstützt. Wenn Sie z. B. den PC auf "Nur verschlüsselt" festlegen und den Befehl **pptp encrypt mppe auto** vom Router löschen, dann können sich PC und Router nicht auf die Verschlüsselung einigen. Der Befehl **debug ppp negotiation** zeigt diese Ausgabe.

```

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

```

Ein weiteres Beispiel betrifft das MPPE RADIUS-Problem des Routers. Wenn Sie den Router für **PPP-Verschlüsselung automatisch erforderlich** und den PC für "Verschlüsselung zulässig mit Authentifizierung an einen RADIUS-Server, der den MPPE-Schlüssel nicht zurückgibt" festlegen,

wird auf dem PC ein Fehler mit der Angabe "Fehler 742: Der Remote-Computer unterstützt nicht die erforderliche Datenverschlüsselung." Das Router-Debug zeigt eine "Call-Clear-Request" (Byte 9 und 10 = 0x000C = 12 = Call-Clear-Request pro RFC), wie hier gezeigt.

```
00:45:58: Tnl 17 PPTP: CC I 001000011A2B3C4D000C000000000000
```

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

F. Ich glaube, ich habe ein Problem mit getrenntem Tunneling. Was muss ich tun, wenn ein PPTP-Tunnel auf einem PC gestartet wird, der PPTP-Router eine höhere Metrik als der vorherige Standard hat und die Verbindung unterbrochen wird?

Antwort: Führen Sie eine Batchdatei (Batch.bat) aus, um das Microsoft-Routing zu ändern und dieses Problem zu beheben. Löschen Sie den Standardwert, und installieren Sie die Standardroute neu (Sie müssen die IP-Adresse kennen, der der PPTP-Client zugewiesen wurde, z. B. 192.168.1.1).

In diesem Beispiel ist das Netzwerk im Router 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
```

F. Welche Probleme sollten bei der Fehlerbehebung für PPTP beachtet werden?

Antwort: Hier werden einige Microsoft-bezogene Probleme aufgelistet, die Sie bei der Fehlerbehebung für PPTP berücksichtigen sollten. Ausführliche Informationen finden Sie in der Microsoft Knowledge Base unter den angegebenen Links.

- [So halten Sie RAS-Verbindungen nach der Abmeldung aktiv](#) RAS-Verbindungen (Windows Remote Access Service) werden automatisch getrennt, wenn Sie sich von einem RAS-Client abmelden. Sie können die Verbindung beibehalten, indem Sie den Registrierungsschlüssel **KeepRasConnections** auf dem RAS-Client aktivieren.
- [Der Benutzer wird nicht benachrichtigt, wenn er sich mit zwischengespeicherten Anmeldeinformationen anmeldet.](#) Wenn Sie sich von einer Windows-basierten Workstation oder einem Mitgliedserver in einer Domäne anmelden und der Domänencontroller nicht gefunden werden kann, erhalten Sie keine Fehlermeldung, die auf dieses Problem hinweist. Stattdessen sind Sie mit zwischengespeicherten Anmeldeinformationen am lokalen Computer angemeldet.
- [Schreiben einer LMHOSTS-Datei für Probleme mit der Domänenvalidierung und anderen Namensauflösung](#) Wenn Probleme mit der Namensauflösung in Ihrem TCP/IP-Netzwerk auftreten, müssen Sie möglicherweise Lmhosts-Dateien verwenden, um NetBIOS-Namen aufzulösen. Sie müssen eine bestimmte Prozedur befolgen, um eine Lmhosts-Datei zu erstellen, die in der Namensauflösung und Domänenvalidierung verwendet werden soll.

Zugehörige Informationen

- [PPTP-Support-Seite](#)
- [PIX-Support-Seite](#)
- [Support-Seite für VPN Concentrators der Serie 3000](#)

- [RFC 2637: Point-to-Point Tunneling Protocol \(PPTP\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)