

Preguntas frecuentes sobre PPTP

Contenido

[Introducción](#)

[Hardware](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

En este documento se tratan preguntas frecuentes sobre el Protocolo de tunelización punto a punto (PPTP).

Consulte las [Convenciones Utilizadas de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones de los documentos.

Hardware

Q. ¿Cómo puedo determinar qué plataformas soportan PPTP?

A. Puede determinar qué versiones de Cisco IOS® Software soportan [PPTP \(sólo clientes registrados\)](#). La herramienta le permite comparar las características de las versiones de Cisco IOS Software, hacer coincidir las características de Cisco IOS Software y CatOS con las versiones y descubrir qué versión de software necesita para soportar su hardware.

Q. ¿Cuándo se introdujo PPTP por primera vez en Secure PIX Firewall de Cisco?

A. PPTP se introdujo por primera vez en Cisco Secure PIX firewall, versión 5.1. Refiera a [PIX 6.x: PPTP con el ejemplo de configuración de la autenticación de RADIUS](#) para más información.

Nota: La terminación PPTP en la función del firewall PIX no es soportada en la versión 7.x y posterior.

Q. ¿Hay detalles sobre la Microsoft Point-to-Point Encryption (MPPE) que debo tener en cuenta?

A. MPPE requiere el Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). Funciona solamente con RADIUS o la autenticación local y el servidor RADIUS debe soportar el valor de atributo MPPE-Keys.

Esta lista muestra algunas plataformas y su compatibilidad con MPPE.

- Cisco Secure ACS para UNIX (CSUNIX) - No

- Access Registrar - No
- Funk RADIUS - Sí
- Cisco Secure ACS para Windows - Sí
- Microsoft Windows 2000 Internet Authentication Server - Sí

Q. ¿Qué versión de software Cisco IOS admitía PPTP en el comienzo?

A. PPTP fue soportado inicialmente en Cisco IOS Software Release 12.0(5)XE5 y en los routers Cisco 7100/7200. Luego se trasladó a la plataforma general de Cisco IOS que soporta Cisco IOS Software Release 12.1(5)T.

Q. ¿Cuáles son algunos de los problemas de compatibilidad conocidos con los productos PPTP de Microsoft y el VPN 3000 Concentrator?

A. Esta información se basa en el software VPN 3000 Series Concentrator, versiones 3.5 y posterior; VPN 3000 Series Concentrators, Modelos 3005, 3015, 3030, 3060, 3080; y sistemas operativos Microsoft Windows 95 y posteriores.

- **Windows 95 Dial-Up Networking (DUN) 1.2** Microsoft Point-to-Point Encryption (MPPE) no es soportado por DUN 1.2. Instale Windows 95 DUN 1.3 para conectarse con MPPE. [Puede descargar la actualización DUN 1.3 de Microsoft del sitio Web de Microsoft.](#)
- **Windows NT 4.0** Windows NT es soportado completamente para las conexiones PPTP en el VPN Concentrator. Se requiere Service Pack 3 (SP3) o superior. Si ejecuta SP3, instale las revisiones del Rendimiento para PPTP y de la Seguridad. [Consulte el sitio web de Microsoft para obtener información sobre el Rendimiento PPTP y la Actualización de seguridad para WinNT 4.0. La única resolución para esto es reinstalar el Option Pack del servidor NT 4.0 sin agregar luego el Service Pack.](#) **Nota:** El Service Pack 5 de 128 bits no maneja las claves MPPE adecuadamente y el PPTP puede no transmitir información. Cuando esto ocurre, el registro de acontecimientos muestra este mensaje.

```
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.
```

[Consulte el artículo de Microsoft Claves de MPPE que no se manejaron correctamente para una Solicitud MS-CHAP de 128 bits](#) para obtener más información.

Q. ¿Los routers Cisco IOS o los Firewalls PIX soportan las transferencias PPTP o PPTP sobre la función Traducción de Dirección de Puerto (PAT)?

A. Cisco IOS Software Releases 12.1T y posterior soportan la transferencia PPTP o la función PPTP sobre PAT. Consulte la sección [“NAT - Soporte para PPTP en una Configuración \(Traducción de Dirección de Puerto\) de Descarga” en Cisco IOS Software 12.1T Early Deployment Release Series para más información.](#) Consulte [Tunelización IP - Configuración de PPTP a Través de PAT a un Servidor PPTP de Microsoft](#) para configurar el PPTP sobre PAT o la transferencia PPTP en un router de Cisco IOS.

Las versiones de PIX 6.3 y posteriores admiten traspaso de PPTP o PPTP sobre PAT mediante la función PPTP fixup (Corrección de PPTP). Esta función permite que el tráfico PPTP atraviese el PIX cuando está configurado para PAT. El PIX realiza una inspección de estado del paquete PPTP en el proceso. Consulte la sección sobre [configuración PPTP](#) en [Configuración de la](#)

[Inspección de la Aplicación \(fixup\)](#) para configurar el fixup PPTP en el PIX. El comando fixup protocol pptp 1723 configura la reparación PPTP.

Troubleshooting

Q. ¿Qué puertos debería abrir en un firewall para acomodar los túneles PPTP?

A. Abra estos puertos.

- TCP/1723
- IP Protocol/47 GREConsulte [Permiso de Conexiones PPTP a Través del PIX](#) para obtener más información.

Q. ¿Cuáles son los bugs PPTP que se observan con frecuencia en Cisco IOS Software?

A. Se han identificado estos bug:

- [CSCdt46181 \(clientes registrados solamente\)](#) - Refiera a la [vulnerabilidad del Cisco IOS PPTP](#) para más información.
- [CSCdz47290 \(clientes registrados solamente\)](#) - PPTP rápido/process switching roto cuando el Cisco Express Forwarding (CEF) se habilita global.
- [CSCdx86482 \(clientes registrados solamente\)](#) - Tunelización de PPTP se ha roto.
- [CSCdt11570 \(clientes registrados solamente\)](#) - Microsoft Point-to-Point Encryption (MPPE) del 128-bit no trabaja en el módulo integrated services del hardware (ISMO).
- [CSCdt66607 \(clientes registrados solamente\)](#) - El 128-bit MPPE PPTP no trabaja con el Cisco Secure ACS for Windows.
- [CSCdu19654 \(clientes registrados solamente\)](#) - El PPTP falla.
- [CSCdv50861 \(clientes registrados solamente\)](#) - El MPPE no negocia con el Windows 2000.

Los clientes registrados pueden ver a los detalles del bug usando el [juego de herramientas del bug Cisco \(clientes registrados solamente\)](#) para más información.

Q. ¿Cuáles son algunas de las limitaciones para PPTP?

A. Estas son algunas de las limitaciones para PPTP.

- PPTP sólo admite Cisco Express Forwarding (CEF) y conmutación de procesos. Fast switching no es soportado.
- Cisco IOS Software soporta solamente la tunelización voluntaria como el PPTP Network Server (PNS).
- Necesita imágenes crypto para soporte de MPPC. El MPPE requiere la autenticación Microsoft Challenge Authentication Protocol (MS-CHAP) y MPPE compatible con TACACS+.

Q. ¿Qué eventos de depuración significativos debería buscar al tratar de resolver un problema de PPTP en un router?

A. Busque estos 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

Busque estos eventos importantes.

```
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. ¿Qué significa cuando aparece el mensaje "Error 734" y luego se desconecta?

A. Este error indica que el router y la PC no pueden negociar la autenticación. Por ejemplo, si configura los protocolos de autenticación del equipo para Shiva PAP (SPAP) y Microsoft Challenge Authentication Protocol (MS-CHAP) versión 2 (cuando el router no puede realizar la versión 2), y configura el router para la CHAP, el **comando debug ppp negotiation** en el router mostrará este resultado.

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

Otro ejemplo es cuando el router se configura para **vpdn group 1 ppp encrypt mppe 40 required** y el equipo se configura como "no se permite encriptación". El equipo no se conecta y produce el "Error el 734", y el **comando debug ppp negotiation** en el router muestra este resultado.

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

Q. ¿Qué significa "Error 742"?

A. Este error significa que la computadora remota no soporta el tipo de encriptación de datos requerida. Por ejemplo, si configura el equipo en "encriptado solamente" y elimina el **comando ppp encrypt mppe auto** del router, el equipo y el router no pueden coincidir en cuanto a la encriptación. El comando **debug ppp negotiation** muestra este resultado.

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

Otro ejemplo incluye el problema en el router MPPE RADIUS. Si configura el router para el **ppp encrypt mppe auto required** y el equipo para el "encriptación permitida con la autenticación a un servidor RADIUS que no devuelve la clave MPPE", se producirá el error en el equipo denominado "Error 742: El equipo remoto no soporta el tipo de encriptación de datos requerida". La depuración del router muestra un "Call-Clear-Request" (Petición de eliminación de llamada) (Bytes 9 y 10 = 0x000C = 12 = Call-Clear-Request por RFC) como se muestra aquí.

```
00:45:58: Tn1 17 PPTP: CC I 001000011A2B3C4D000C000000000000
00:45:58: Vi1 Tn1/Cl 17/17 PPTP: CC I ClearRQ
```

Q. Creo que tengo un problema de tunelización dividida. ¿Qué debo hacer cuando

un túnel PPTP aparece en una PC, el router PPTP tiene una métrica más alta que la predeterminada anteriormente y pierdo conectividad?

A. Ejecute un archivo por lotes (batch.bat) para modificar el Ruteo de Microsoft y resolver este problema. Elimine el valor predeterminado y reinstale la ruta predeterminada (debe conocer la dirección IP que fue asignada al cliente PPTP, por ejemplo 192.168.1.1).

En este ejemplo, la red dentro del router es 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. ¿Cuáles son algunos problemas que deben considerarse al resolver problemas de PPTP?

A. Varios de los problemas relacionados con Microsoft que deben ser considerados al solucionar problemas de PPTP se enumeran aquí. La información detallada se encuentra disponible en la Base de datos de conocimiento de Microsoft en los links proporcionados.

- [Cómo Mantener las Conexiones RAS Activas después de Cerrar una Sesión](#) Las conexiones de Windows Remote Access Service (RAS) se desconectan automáticamente cuando cierra una sesión de un cliente RAS. Puede permanecer conectado si activa la clave de registro de KeepRasConnections en el cliente RAS.
- [No se Alerta al Usuario cuando se Inicia Sesión con las Credenciales Guardadas en Caché](#) Si abre sesión en un dominio desde una estación de trabajo basada en Windows o el servidor miembro y el controlador de dominio no pueden ser localizados, no recibe un mensaje de error que indique este problema. En su lugar, se abre una sesión en el equipo local con las credenciales guardadas en caché.
- [Cómo Escribir un Archivo LMHOSTS para la Validación de Dominio y Otros Problemas de Resolución de Nombre](#) Si tiene problemas de resolución de nombre en su red TCP/IP, posiblemente necesite utilizar los archivos Lmhosts para resolver los nombres de NETBIOS. Siga el procedimiento específico para crear un archivo Lmhosts para validación de dominios y resolución de nombres.

Información Relacionada

- [Página de soporte de PPTP](#)
- [Página de Soporte de PIX](#)
- [Página de soporte de concentradores VPN Serie 3000](#)
- [RFC 2637: Protocolo de Tunelización punto a Punto \(PPTP\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)