Domande frequenti su PPTP

Sommario

Introduzione

Questo documento contiene le domande frequenti sul protocollo PPTP (Point-to-Point Tunnel Protocol).

Fare riferimento a Convenzioni utilizzate nei suggerimenti tecnici Cisco per ulteriori informazioni sulle convenzioni usate.

Hardware

D. Come è possibile stabilire quali piattaforme supportano PPTP?

R. È possibile stabilire quali versioni del software Cisco IOS® supportano PPTP utilizzando lo strumento Feature Navigator (solo utenti registrati). Lo strumento permette di confrontare le versioni del software Cisco IOS, abbinare il software Cisco IOS e le funzionalità CatOS alle versioni e scoprire quale versione software è necessaria per supportare l'hardware.

D. Da quando il protocollo PPTP è stato introdotto per la prima volta nel firewall Cisco Secure PIX?

R. PPTP è stato introdotto per la prima volta in Cisco Secure PIX firewall versione 5.1. Per ulteriori informazioni, fare riferimento al documento PIX 6.x: Esempio di configurazione dell'autenticazione PPTP con Radius per ulteriori informazioni.

Nota: la terminazione PPTP sulla funzione PIX firewall non è supportata nella versione 7.x e successive.

D. Quali informazioni devo conoscere su Microsoft Point-to-Point Encryption (MPPE)?

R. MPPE richiede Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). Funziona solo con l'autenticazione RADIUS o locale e il server RADIUS deve supportare il valore dell'attributo MPPE-Keys.

Nell'elenco vengono mostrate alcune piattaforme e la relativa compatibilità MPPE.

- Cisco Secure ACS for UNIX (CSUNIX) - No
- Access Registrar - No
- Funk RADIUS - Sì
- Cisco Secure ACS per Windows - Sì
- Server di autenticazione Internet di Microsoft Windows 2000 - Sì

D. Quale versione del software Cisco IOS ha inizialmente supportato PPTP?

R. Il protocollo PPTP è stato inizialmente supportato nel software Cisco IOS versione 12.0(5)XE5 sui router Cisco 7100/7200. È stato quindi spostato sul supporto generale della piattaforma Cisco IOS nel software Cisco IOS versione 12.1(5)T.

D. Quali sono alcuni problemi noti di compatibilità con i prodotti Microsoft PPTP e VPN 3000 Concentrator?

R. Queste informazioni sono basate sul software VPN 3000 Concentrator versione 3.5 e successive; VPN serie 3000 concentrator, modelli 3005, 3015, 3030, 3060, 3080; e sistemi operativi Microsoft Windows 95 e versioni successive.

- **Windows 95 DUN (Dial-Up Networking) 1.2**Microsoft Point-to-Point Encryption (MPPE) non è supportato in DUN 1.2. Installare Windows 95 DUN 1.3 per connettersi utilizzando MPPE. È possibile scaricare l'aggiornamento Microsoft DUN 1.3 dal sito Web Microsoft.
- **Windows NT 4.0**Windows NT è completamente supportato per le connessioni PPTP al concentratore VPN. Service Pack 3 (SP3) o versione successiva. Se si esegue SP3, installare le patch di Prestazioni e protezione PPTP. Per informazioni sull'aggiornamento di prestazioni e sicurezza PPTP per WinNT 4.0, consultare il sito Web di Microsoft . L'unica soluzione consiste nel reinstallare il pacchetto di opzioni del server NT 4.0 senza aggiungere il service pack.**Nota:** il Service Pack 5 a 128 bit non gestisce correttamente le chiavi MPPE e il PPTP potrebbe non riuscire a passare i dati. In questo caso, il registro eventi visualizza questo messaggio.
  ```
  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.
  ```
  Per ulteriori informazioni, vedere l'articolo Microsoft MPPE Keys Not Handled Correct for a 128-Bit MS-CHAP Request .

D. I router Cisco IOS o i firewall PIX supportano la funzionalità PPTP pass-through o PPTP over Port Address Translation (PAT)?

R. Il software Cisco IOS versione 12.1T e successive supporta la funzionalità PPTP pass-through o PPTP over PAT. Per ulteriori informazioni, consultare la sezione "NAT - Support for PPTP in an Overload (Port Address Translation) Configuration" del software Cisco IOS versione 12.1T. Per ulteriori informazioni, fare riferimento al documento sulla configurazione del tunneling IP tramite PPTP su un server PPTP Microsoft per configurare il pass-through PPTP su PAT o PPTP su un router Cisco IOS.

Le versioni PIX 6.3 e successive supportano PPTP pass-through o PPTP over PAT utilizzando la funzione di correzione PPTP. Questa funzione consente al traffico PPTP di attraversare il PIX quando configurato per PAT. Il PIX esegue l'ispezione dei pacchetti PPTP con stato durante il processo. Fare riferimento alla sezione sulla configurazione PPTP in Configurazione dell'ispezione

dell'applicazione (correzione) per configurare la correzione PPTP sul PIX. Il comando **fixup protocol pptp 1723** configura la correzione PPTP.

Risoluzione dei problemi

D. Quali porte è necessario aprire su un firewall per supportare i tunnel PPTP?

R. Aprire queste porte.

- TCP/1723
- Protocollo IP/47 GREPer ulteriori informazioni, fare riferimento a Autorizzazione delle connessioni PPTP tramite PIX.

D. Quali sono i bug noti relativi al software Cisco IOS PPTP?

A. Sono stati identificati i seguenti bug:

- CSCdt46181 (solo utenti registrati) - Per ulteriori informazioni, fare riferimento a Cisco IOS PPTP Vulnerability.
- CSCdz47290 (solo utenti registrati) - La commutazione veloce/processo PPTP viene interrotta quando Cisco Express Forwarding (CEF) è abilitato a livello globale.
- CSCdx86482 (solo utenti registrati) - Il tunneling PPTP si è interrotto.
- CSCdt11570 (solo utenti registrati) - Microsoft Point-to-Point Encryption (MPPE) a 128 bit non funziona su ISM (Hardware Integrated Services Module).
- CSCdt6607 (solo utenti registrati) - PPTP MPPE a 128 bit non funziona con Cisco Secure ACS per Windows.
- CSCdu19654 (solo utenti registrati) - Errore PPTP.
- CSCdv50861 (solo utenti registrati) - MPPE non negozia con Windows 2000.

Gli utenti registrati possono visualizzare i dettagli dei bug usando Cisco Bug Toolkit (solo utenti registrati) per ulteriori informazioni.

D. Quali sono alcuni limiti di PPTP?

R. Queste sono alcune limitazioni di PPTP.

- PPTP supporta solo Cisco Express Forwarding (CEF) e la commutazione di contesto. L'opzione di commutazione veloce non è supportata.
- Il software Cisco IOS supporta solo il tunneling volontario come PPTP Network Server (PNS).
- Sono necessarie immagini crittografiche per il supporto di MPPE. MPPE richiede l'autenticazione MS-CHAP (Microsoft Challenge Authentication Protocol) e MPPE non è supportato con TACACS+.

D. Quali eventi di debug significativi è necessario cercare quando si risolvono i problemi relativi a PPTP su un router?

R. Cercate questi debug.

- debug autenticazione aaa
- autorizzazione debug aaa
- raggio di debug
- negoziazione ppp di debug
- debug autenticazione ppp
- debug di eventi vpdn
- debug di errori vpdn
- debug vpdn l2x-packet
- debug eventi ppp mppe
- debug ppp chap

Cerca questi eventi significativi.

```
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
```

D. Cosa significa quando ricevo il messaggio "Errore 734" e mi scollego?

R. Questo errore indica che il router e il PC non possono negoziare l'autenticazione. Ad esempio, se si impostano i protocolli di autenticazione PC per Shiva PAP (SPAP) e Microsoft Challenge Authentication Protocol (MS-CHAP) versione 2 (quando il router non è in grado di eseguire la versione 2) e si imposta il router per CHAP, il comando **debug ppp negotiation** sul router visualizza questo output.

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

Inoltre, se il router è impostato per il **gruppo vpdn 1, la crittografia mppe 40 è obbligatoria** e il PC è impostato per "nessuna crittografia consentita". Il PC non si connette e genera un "Errore 734" e il comando **debug ppp negotiation** sul router visualizza questo output.

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

D. Cosa significa "Errore 742"?

R. Questo errore indica che il computer remoto non supporta il tipo di crittografia dei dati richiesto. Ad esempio, se si imposta il PC come "solo crittografato" e si elimina il comando **pptp encrypt mppe auto** dal router, il PC e il router non possono accettare la crittografia. Il comando **debug ppp negotiation** visualizza questo output.

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

Un altro esempio riguarda il problema MPPE RADIUS del router. Se si imposta il router per **ppp encrypt mppe auto richiesto** e il PC per "crittografia consentita con autenticazione su un server RADIUS che non restituisce la chiave MPPE", sul PC viene visualizzato un messaggio di errore del tipo "`Errore 742: Il computer remoto non supporta il tipo di crittografia dei dati richiesto.`" Il debug del router mostra una "Call-Clear-Request" (byte 9 e 10 = 0x000C = 12 = Call-Clear-Request per RFC) come mostrato di seguito.

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

D: Credo di avere un problema di split tunneling. Cosa fare quando su un PC viene visualizzato un tunnel PPTP, il router PPTP ha una metrica più alta rispetto al valore predefinito precedente e la connettività viene interrotta?

R. Per risolvere il problema, eseguire un file batch (batch.bat) per modificare il routing di Microsoft. Eliminare il percorso predefinito e reinstallare quello predefinito (è necessario conoscere l'indirizzo IP assegnato al client PPTP, ad esempio 192.168.1.1).

Nell'esempio, la rete all'interno del router è 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
```

D. Quali sono alcuni problemi da considerare quando si esegue la risoluzione dei problemi relativi a PPTP?

R. Di seguito sono elencati diversi problemi relativi a Microsoft da considerare per la risoluzione dei problemi relativi a PPTP. Informazioni dettagliate sono disponibili nella Microsoft Knowledge Base tramite i collegamenti forniti.

- Come mantenere attive le connessioni RAS dopo la disconnessioneLe connessioni del Servizio di accesso remoto Windows (RAS) vengono disconnesse automaticamente quando si esegue la disconnessione da un client RAS. È possibile rimanere connessi abilitando la chiave del Registro di sistema **KeepRasConnections** nel client RAS.
- L'Utente Non Viene Avvisato Quando Accede Con Credenziali Memorizzate Nella CacheSe si accede a un dominio da una workstation basata su Windows o da un server membro e non è possibile individuare il controller di dominio, non verrà visualizzato alcun messaggio di errore. È stato invece eseguito l'accesso al computer locale utilizzando le credenziali memorizzate nella cache.
- Come scrivere un file LMHOSTS per la convalida del dominio e altri problemi di risoluzione dei nomiSe si verificano problemi di risoluzione dei nomi sulla rete TCP/IP, potrebbe essere necessario utilizzare i file Lmhosts per risolvere i nomi NetBIOS. Per creare un file Lmhosts da utilizzare nella risoluzione dei nomi e nella convalida del dominio, è necessario seguire una procedura specifica.

Informazioni correlate

- Pagina di supporto PPTP
- Pagina di supporto PIX
- Pagina di supporto per VPN serie 3000 concentrator
- RFC 2637: Protocollo PPTP (Point-to-Point Tunneling Protocol)
- Documentazione e supporto tecnico – Cisco Systems