Domande frequenti su VPN Client

Sommario

Introduzione

Questo documento risponde alle domande frequenti sul client VPN Cisco.

Nota: di seguito sono riportate le convenzioni di denominazione per i vari client VPN:

- Solo Cisco Secure VPN Client versioni da 1.0 a 1.1a
- Cisco VPN 3000 Client solo versioni 2.x
- Cisco VPN Client 3.x e versioni successive

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Scarica software VPN Client

D. Dove posso scaricare il software Cisco VPN Client?

R. Per accedere al software Cisco VPN Client, è necessario eseguire l'accesso e disporre di un contratto di assistenza valido. Il software Cisco VPN Client può essere scaricato dalla pagina Download del software Cisco (solo utenti registrati). **Se al profilo Cisco.com non è associato un contratto di assistenza valido, non è possibile accedere e scaricare il software client VPN.**

Per ottenere un contratto di assistenza valido, è possibile:

- Se disponi di un contratto di acquisto diretto, contatta il team Cisco che gestisce gli account.
- Per acquistare un contratto di assistenza, contattare un partner o un rivenditore Cisco.
- Per aggiornare il profilo Cisco.com e richiedere l'associazione a un contratto di assistenza, utilizzare Profile Manager (solo utenti registrati).

D. L'area di download di Cisco VPN Client sembra essere vuota. Perché?

R. Quando si raggiunge l'area client VPN del Software Center (solo utenti registrati), assicurarsi di selezionare l'area di download per il sistema operativo desiderato nella parte centrale della pagina.

D. Come è possibile disabilitare la funzione Stateful Firewall durante l'installazione del client VPN Cisco?

R. Per le versioni VPN Client precedenti alla 5.0:

Fare riferimento alla sezione Modifiche alla documentazione delle Note sulla versione della regola 4.7 del client VPN per informazioni sui due argomenti "Uso di MSI per installare il client VPN Windows senza firewall stateful" e "Uso di InstallShield per installare il client VPN Windows senza firewall stateful".

Per le versioni client VPN dopo la versione 5.0:

A partire dalla versione 5.0.3.0560 di Cisco VPN Client, è stato aggiunto un flag di installazione MSI per evitare l'installazione del GUID nei file del firewall:

```
msiexec.exe /i vpnclient_setup.msi DONTINSTALLFIREWALL=1
```

Per ulteriori informazioni su questo argomento, fare riferimento alla sezione Ignorare l'installazione dei file del firewall quando non è necessario un firewall stateful.

D. Come disinstallare o aggiornare Cisco VPN Client?

R. Per informazioni su come disinstallare manualmente (InstallShield) e aggiornare Cisco VPN Client versione 3.5 e successive per Windows 2000 e Windows XP, consultare il documento sulla rimozione di una versione client VPN installata con MSI Installer.

Il software Cisco VPN Client per Windows 2000 e Windows XP può scaricare in modo sicuro gli aggiornamenti e le nuove versioni automaticamente tramite un tunnel da un concentratore VPN 3000 o da un altro server VPN in grado di inviare notifiche. Il prerequisito minimo per questa operazione è che gli utenti remoti devono avere installato il client VPN per Windows 4.6 o versioni successive sui loro PC per utilizzare la funzione di aggiornamento automatico.

Con questa funzione, denominata autoupdate, gli utenti non devono disinstallare una versione precedente del software, riavviare, installare la nuova versione e riavviare di nuovo. Al contrario, un amministratore rende disponibili aggiornamenti e profili su un server Web e, quando un utente remoto avvia il client VPN, il software rileva che è disponibile un download e lo ottiene automaticamente. Per ulteriori informazioni, vedere Gestione degli aggiornamenti automatici e Funzionamento dell'aggiornamento automatico.

Per informazioni su come configurare l'aggiornamento client su un'appliance Cisco ASA serie 5500 Adaptive Security utilizzando ASDM, fare riferimento alla configurazione dell'aggiornamento del software client con ASDM.

D. Desidero personalizzare i client VPN per Vista. Mi rendo conto che, con la nuova versione del client VPN per Vista, non esiste alcun file come oem.mst. Come

personalizzare le nuove versioni dei client VPN (5.x) o dove è possibile trovare questo file?

R. Il file MST non viene più fornito con il client VPN, ma è possibile scaricarlo dalla pagina Download Software (solo utenti registrati):

Nome file: Readme e MST per l'installazione nella versione internazionale di Windows.

Sistema operativo

D. Cisco fornisce un client VPN per Windows Vista?

R. La nuova versione di Cisco VPN Client 5.0.07 supporta Windows Vista sia su x86 (32 bit) che su x64. Per ulteriori informazioni, consultare le note sulla versione 5.0.07.0240.

Nota: Cisco VPN Client è supportato solo in un'installazione pulita di Windows Vista, il che significa che un aggiornamento di qualsiasi sistema operativo Windows a Windows Vista non è supportato con il software del client VPN. È necessario installare Windows Vista e quindi il software Vista VPN Client.

Nota: Se al profilo Cisco.com non è associato un contratto di assistenza valido, non è possibile accedere e scaricare il software VPN Client. Per ulteriori informazioni, vedere Download del software VPN Client.

Suggerimento: il client VPN Cisco AnyConnect è ora disponibile per i sistemi operativi Windows, che includono Vista a 32 e 64 bit. Il client AnyConnect supporta SSL e DTLS. Al momento non supporta IPSec. Inoltre, AnyConnect è disponibile solo per l'uso con un Cisco Adaptive Security Appliance con versione 8.0(2) o successive. Il client può essere utilizzato anche in modalità weblaunch con gli accessori IOS con versione 12.4(15)T. VPN 3000 non è supportato.

Il client VPN Cisco AnyConnect e ASA 8.0 possono essere ottenuti dal Software Center (solo utenti registrati). Per ulteriori informazioni sul client AnyConnect, consultare le note di rilascio del client VPN AnyConnect di Cisco. Per ulteriori informazioni sull'appliance ASA 8.0, consultare le note di rilascio delle appliance Cisco ASA serie 5500 Adaptive Security.

Nota: Se al profilo Cisco.com non è associato un contratto di assistenza valido, non è possibile accedere e scaricare il software AnyConnect VPN Client o ASA. Per ulteriori informazioni, vedere Download del software VPN Client.

D. Come configurare una connessione PPTP da un PC Microsoft Windows?

R. L'installazione dipende dalla versione di Microsoft Windows in uso. Contattare Microsoft per informazioni specifiche. Di seguito sono riportate le istruzioni di installazione per alcune delle versioni comuni di Windows:

Windows 95

1. Installare Msdun13.exe.
2. Scegliere **Programmi > Accessori > Connessione remota**.
3. Create una nuova connessione denominata "PPTP".

4. Selezionare la **scheda VPN** come dispositivo per la connessione.
5. Immettere l'indirizzo IP dell'interfaccia pubblica dello switch e fare clic su **Fine**.
6. Tornare alla connessione appena creata, fare clic con il pulsante destro del mouse e scegliere **Proprietà**.
7. In Protocolli di rete consentiti, deselezionare almeno **netbeui**.
8. Configurare l'impostazione **Opzioni avanzate**: Lasciare invariate le impostazioni predefinite per consentire allo switch e al client di negoziare automaticamente il metodo di autenticazione.Abilitare **Richiedi password crittografata** per forzare l'autenticazione CHAP (Challenge Handshake Authentication Protocol).Abilitare **Richiedi password crittografata** e **Richiedi crittografia dati** per forzare l'autenticazione MS-CHAP.

Windows 98

1. Per installare la funzionalità PPTP, completare i seguenti passaggi: Scegliere **Start > Impostazioni > Pannello di controllo > Nuovo hardware**, quindi fare clic su **Avanti**.Fare clic su **Seleziona dall'elenco**, scegliere **Scheda di rete**, quindi fare clic su **Avanti**.Scegliere **Microsoft** nel pannello sinistro e **Microsoft VPN Adapter** nel pannello destro.
2. Per configurare la funzionalità PPTP, completare la procedura seguente: Scegliere **Start > Programmi > Accessori > Comunicazioni > Connessione remota**.Fare clic su **Crea nuova connessione** e scegliere **Microsoft VPN Adapter** per Selezionare un dispositivo. Indirizzo IP server VPN= endpoint tunnel 3000.
3. Completare questa procedura per modificare il PC in modo da consentire anche il protocollo PAP (Password Authentication Protocol): **Nota:** l'autenticazione predefinita di Windows 98 prevede l'utilizzo della crittografia della password (CHAP o MS-CHAP).Scegliere **Proprietà > Tipi di server**.Deselezionare **Richiedi password crittografata**. In quest'area è possibile configurare la crittografia dei dati (Microsoft Point-to-Point Encryption [MPPE] o nessuna MPPE).

Windows 2000

1. Scegliere **Start > Programmi > Accessori > Comunicazioni > Rete e connessioni remote**.
2. Fare clic su **Crea nuova connessione** e quindi su **Avanti**.
3. Scegliere **Connetti a una rete privata tramite Internet e Componi una connessione prima** (non selezionare questa opzione se si dispone di una LAN), quindi fare clic su **Avanti**.
4. Immettere il nome host o l'indirizzo IP dell'endpoint del tunnel (3000).
5. Se è necessario modificare il tipo di password, scegliere **Proprietà > Protezione per la connessione > Avanzate**. Il valore predefinito è MS-CHAP e MS-CHAP v2 (non CHAP o PAP). In quest'area è possibile configurare la crittografia dei dati (MPPE o MPPE assente).

Windows NT

Fare riferimento a Installazione, configurazione e utilizzo di PPTP con client e server Microsoft .

D. Quali versioni del sistema operativo supportano Cisco VPN Client?

R. Il supporto per sistemi operativi aggiuntivi viene aggiunto costantemente per il client VPN. Per verificare questa condizione, fare riferimento ai requisiti di sistema nelle note sulla versione per il client VPN 5.0.07 o a Hardware Cisco e client VPN che supportano IPsec/PPTP/L2TP.

Note:

- Il client VPN include il supporto per workstation dual-processor e dual-core per Windows XP e Windows Vista.
- Windows VPN Client Release 4.8.00.440 è la versione finale che ha ufficialmente supportato il sistema operativo Windows 98.
- Windows VPN Client Release 4.6.04.0043 è la versione finale che ha ufficialmente supportato il sistema operativo Windows NT.
- Cisco VPN Client versione 5.0.07 supporta Windows Vista e Windows 7 nelle edizioni x86 (32 bit) e x64 (64 bit).
- Cisco VPN Client supporta solo Windows XP a 32 bit, ma Windows XP a 64 bit non è supportato.**Nota:** il supporto per Windows Vista a 32 bit era disponibile in tutte le versioni 5.x. A Cisco VPN client versione 5.0.07 è stato aggiunto il supporto per 64 bit.

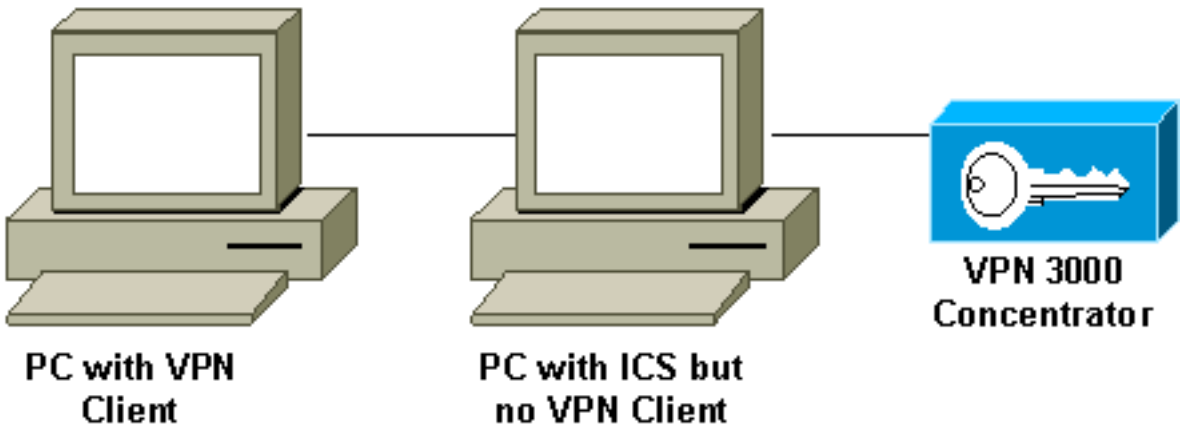
D. Per caricare il client VPN è necessario essere un amministratore dei computer Windows NT/2000?

R. Sì, per installare il client VPN su Windows NT e Windows 2000 è necessario disporre dei privilegi di amministratore, in quanto questi sistemi operativi richiedono i privilegi di amministratore per il binding ai driver di rete esistenti o per l'installazione di nuovi driver di rete. Il software client VPN è un software di rete. Per installarlo, è necessario disporre dei privilegi di amministratore.

D. Il client VPN Cisco può funzionare con Condivisione connessione Internet (ICS) Microsoft installato sullo stesso computer?

R. No, il client Cisco VPN 3000 non è compatibile con Microsoft ICS sullo stesso computer. Prima di installare il client VPN, è necessario disinstallare ICS. Per ulteriori informazioni, vedere Disattivazione di ICS durante la preparazione all'installazione o all'aggiornamento a Cisco VPN Client 3.5.x su Microsoft Windows XP.

Anche se l'utilizzo del client VPN e di ICS sullo stesso PC non funziona, questa soluzione funziona.



D. Il mio client VPN sembra connettersi solo a determinati indirizzi. Viene eseguito Windows XP. Cosa devo fare?

R. Verificare che il firewall incorporato in Windows XP sia disattivato.

D. Il client VPN Cisco è compatibile con il firewall con stato di Windows XP?

R. Il problema è stato risolto. Per ulteriori informazioni, consultare l'ID bug Cisco CSCdx15865 (solo utenti registrati) in Bug Toolkit.

D. Quando si installa il client VPN in Windows XP e Windows 2000, l'interfaccia multiutente è disattivata?

R. L'installazione disattiva la schermata iniziale e il cambio rapido utente. Per ulteriori informazioni, consultare l'ID bug Cisco CSCdu24073 (solo utenti registrati) in Bug Toolkit.

D. Come posso fare in modo che il client VPN per Linux si sposti in background dopo l'esecuzione? Se si avvia una connessione come vpnclient connect foo, si accede, ma la shell viene restituita.

A. Dopo l'accesso, digitare:

- **^Z**
- **bg**

D. Quando si installa Cisco VPN Client su Windows XP Home Edition, la barra delle applicazioni non è visibile. Come è possibile annullare questa operazione?

R. Scegliere **Pannello di controllo > Connessioni di rete > Rimuovi bridge di rete** per regolare questa impostazione.

D. Quando si tenta di installare il client VPN Linux su RedHat 8.0, viene visualizzato un errore che indica che il modulo non può essere caricato perché il modulo è stato compilato con GCC 2 e il kernel è stato compilato con GCC 3.2. Come procedere?

R. Ciò è dovuto al fatto che la nuova versione di RedHat ha una versione più recente del compilatore GCC (3.2+), che causa il malfunzionamento del client VPN Cisco corrente. Il problema è stato risolto ed è disponibile in Cisco VPN 3.6.2a. Per ulteriori informazioni, consultare l'ID bug Cisco CSCdy49082 (solo utenti registrati) in Bug Toolkit o scaricare il software dal VPN Software Center (solo utenti registrati).

D. Perché il software disabilita Cambio rapido utente quando installo il client VPN 3.1 su Windows XP?

R. Microsoft disattiva automaticamente Cambio rapido utente in Windows XP quando viene specificato un file GINA.dll nel Registro di sistema. Il client VPN Cisco installa CSgina.dll per implementare la funzionalità "Avvia prima di accedere". Se è necessario Cambio rapido utente, disattivare la funzione "Avvia prima di accedere". Per ulteriori informazioni, consultare l'ID bug Cisco CSCdu24073 (solo utenti registrati) in Bug Toolkit.

D. Il client VPN IPSec supporta la funzionalità di avvio prima dell'accesso (SBL, Start Before Logon) in Windows 7?

R. La funzionalità SBL non è supportata sui client VPN IPsec di Windows7. È supportata sui client VPN AnyConnect.

Messaggi di errore

D. Quando si installa Cisco VPN Client 4.x, viene visualizzato questo messaggio di errore: **Avviso 201: Il sottosistema VPN necessario non è disponibile. Impossibile connettersi al server VPN remoto**

R. Questo problema può essere causato dai pacchetti firewall installati nel computer client VPN. Per evitare la visualizzazione di questo messaggio di errore, verificare che nel PC non siano installati o in esecuzione programmi firewall o antivirus.

D. Dopo l'aggiornamento a Mac OS X 10.3 (noto come "Panther"), il client VPN Cisco 4.x visualizza questi messaggi di errore: **Connessione VPN sicura terminata localmente dal client Motivo: Impossibile contattare il gateway di sicurezza**

R. Per utilizzare Cisco VPN Client 4.x con Mac OS X 10.3 ("Panther"), è necessario aggiungere UseLegacyIKEPort=0 al profilo (file .pcf) presente nella directory /etc/CiscoSystemsVPNClient/Profiles/.

D. Quando si tenta di disinstallare il client VPN, viene visualizzato questo messaggio di errore: **Messaggio di errore: impossibile trovare il file di disinstallazione...** Qual è il significato di questo messaggio di errore e come è possibile completare la disinstallazione?

R. Controllare il Pannello di controllo della rete per verificare che il DNE (Deterministic NDIS Extender) non sia stato installato. Per controllare la presenza del file di disinstallazione, scegliere anche **Microsoft > Versione corrente > Disinstalla**. Rimuovere il file **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{5624C000-B109-11D4-9DB4-00E0290FCAC5}** e ripetere la disinstallazione.

D. Non è possibile installare il client VPN su Windows 2000 Professional. Viene visualizzato questo messaggio di errore: **Impossibile installare un file di supporto per l'installazione.** Fallimento Catastrofico. Cosa devo fare?

R. Rimuovere il tasto **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall**. Riavviare il computer e reinstallare il client VPN.

Nota: per trovare la chiave corretta per il software Cisco VPN Client nel percorso HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\<*chiave da determinare*>, andare a HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\, quindi fare clic su **VPN Client**. Nella finestra a destra, visualizzare il percorso di disinstallazione (sotto la colonna Nome). Nella colonna Dati corrispondente viene visualizzato il valore della chiave del client VPN. Prendere nota di questa chiave, andare su HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\, selezionare la chiave determinata ed eliminarla.

Per ulteriori informazioni, fare riferimento a Initialization Error Troubleshooting (Risoluzione dei problemi di errore di inizializzazione) e all'ID bug Cisco CSCdv15391 (solo utenti registrati) nel Bug Toolkit.

D. Quando si tenta di installare il client VPN Linux su RedHat 8.0, viene visualizzato un messaggio di errore che indica che il modulo non può essere caricato perché il modulo è stato compilato con GCC 2 e il kernel è stato compilato con GCC 3.2. Come procedere?

R. Questo problema si verifica perché la nuova versione di RedHat ha una versione più recente del compilatore GCC (3.2+), che causa il malfunzionamento del client VPN Cisco corrente. Il problema è stato risolto ed è disponibile in Cisco VPN 3.6.2a. Per ulteriori informazioni, vedere l'ID bug Cisco CSCdy49082 (solo utenti registrati) in Bug Toolkit o scaricare il software dal VPN Software Center (solo utenti registrati).

D. Viene visualizzato il messaggio di errore "peer non risponde più" quando il client Linux 3.5 tenta di stabilire una connessione IPsec a un PIX o a un concentratore VPN 3000. Cosa devo fare?

R. Il sintomo di questo problema è che il client Linux sembra tentare di connettersi, ma non riceve mai una risposta dal dispositivo gateway.

Il sistema operativo Linux ha un firewall incorporato (ipchains) che blocca i pacchetti UDP porta 500, UDP porta 1000 e Encapsulating Security Payload (ESP). Poiché il firewall è attivato per impostazione predefinita, è necessario disattivare il firewall o aprire le porte per la comunicazione IPsec per le connessioni in entrata e in uscita per risolvere il problema.

D. Quando cerco di eseguire Cisco VPN 5000 5.2.2 Client su Mac OS X 10.3 ricevo un errore di estensione del kernel. Cosa devo fare?

R. Come indicato nelle note di rilascio, il client Cisco VPN 5000 è supportato fino alla versione 10.1.x e, pertanto, non è supportato nella versione 10.3. È possibile fare in modo che il client VPN funzioni quando si reimpostano le autorizzazioni su due dei file installati dopo aver eseguito lo script di installazione. Di seguito è riportato un esempio:

Nota: questa configurazione *non* è supportata da Cisco.

```
sudo chown -R root:wheel /System/Library/Extensions/VPN5000.kext
sudo chmod -R go-w /System/Library/Extensions/VPN5000.kext
```

D. Non è possibile installare la nuova versione di Cisco VPN Client. Durante l'installazione viene visualizzato uno dei seguenti messaggi di errore: "**Errore di esecuzione DNEinst durante l'installazione di DNE, codice restituito -2146500093**" O "**Errore InstallDNE: Errore di esecuzione DNEinst durante l'installazione di DNE, codice restituito -2147024891.**" Questo problema si verifica quando viene installato Deterministic Network Enhancer.

R. Installare l'ultimo aggiornamento DNE da Deterministic Networks .

D. Quando effettuo una connessione, ricevo questi registri per il client VPN Cisco:

```
208    15:09:08.619  01/17/08  Sev=Debug/7CVPND/0x63400015
Value for ini parameter VAEnableAlt is 1.

209    15:09:08.619  01/17/08  Sev=Warning/2CVPND/0xE3400003
```

```
Function RegOpenKey failed with an error code of 0x00000002(WindowsVirtualAdapter:558)

210    15:09:08.619  01/17/08  Sev=Warning/3CVPND/0xE340000C
The Client was unable to enable the Virtual Adapter because it could not open the device.
```

R. Si tratta di un messaggio di errore piuttosto generico, che in genere richiede la disinstallazione manuale del client. Seguire le istruzioni in questo collegamento. Rimozione di una versione client VPN installata con MSI Installer.

Una volta completata la disinstallazione, riavviare il sistema. Quindi reinstallare il client. Verificare di aver eseguito l'accesso come utente con diritti di amministratore nel computer locale.

D. Quando cerco di connettere il client VPN Cisco su un Mac OS, ricevo questo messaggio di errore: `Errore 51- Impossibile comunicare con il sottosistema VPN.` Come risolvere il problema?

R. Il problema può essere risolto riavviando il servizio dopo aver chiuso il client VPN nel modo seguente:

Per interrompere:

```
sudo kextunload -b com.cisco.nke.ipsec
```

Per iniziare:

```
sudo kextload /System/Library/Extensions/CiscoVPN/CiscoVPN
```

Verificare inoltre che quanto segue sia in esecuzione sullo stesso computer in cui è installato il client VPN e disabilitarlo.

- Qualsiasi software virtuale (ad esempio, VMWare Fusions, Parallels, crossover).
- Qualsiasi software antivirus/firewall.
- Compatibilità del client VPN con il sistema operativo a 64 bit; fare riferimento alle note di rilascio di Cisco VPN Client.

D. Viene visualizzato il messaggio "Reason 42: impossibile abilitare la scheda virtuale". Come risolvere l'errore?

A. Il `motivo 42: impossibile abilitare la scheda virtuale` viene visualizzato errore dopo che Vista ha segnalato che è stato rilevato un indirizzo IP duplicato. Le connessioni successive non riusciranno con lo stesso messaggio, ma Vista non segnala che è stato rilevato un indirizzo IP duplicato. Per ulteriori informazioni su come risolvere il problema, fare riferimento all'errore 442 relativo ai trigger degli indirizzi IP duplicati in Windows Vista.

D. Quando si installa il client VPN Cisco, viene visualizzato l'errore `Deterministic Network Enhancer Add Plugin Failed (Impossibile aggiungere plug-in).` Come viene risolto questo errore?

R. L'installazione dell'adattatore DNE potrebbe risolvere il problema. È preferibile utilizzare la versione di Installshield per l'installazione anziché MSI.

D. Errore: `Motivo 42: impossibile abilitare la scheda virtuale.` Come risolvere il problema?

R. Questo errore viene visualizzato dopo che Windows 7 e Windows Vista hanno rilevato un indirizzo IP duplicato. Le connessioni successive non riescono con lo stesso messaggio, ma il sistema operativo non segnala il rilevamento dell'indirizzo IP duplicato. Per ulteriori informazioni su come risolvere il problema, fare riferimento all'errore 442 relativo ai trigger degli indirizzi IP duplicati in Windows 7 e Vista.

D. Quando si prova ad avviare il client VPN 4.9 per MAC OS 10.6, viene visualizzato questo messaggio di errore: `Errore 51: Impossibile comunicare con il sottosistema VPN.` Come risolvere il problema?

R. Questo problema si verifica perché il supporto a 64 bit non è disponibile con il client VPN Cisco per MAC OS versione 4.9. Per risolvere il problema, è possibile avviare il sistema in modalità kernel a 32 bit. Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCth11092 (solo utenti registrati) e alle note di rilascio di Cisco VPN client per MAC OSX.

Compatibilità con prodotti di terze parti

D. Il client Nortel è compatibile con i concentratori Cisco VPN 3000?

R. No. Il client Nortel non può connettersi al concentratore Cisco VPN 3000.

D. Posso avere client VPN di altri fornitori, come Nortel Contivity VPN Client, installati contemporaneamente con Cisco VPN Client?

R. No. Quando sullo stesso PC sono installati più client VPN, si verificano problemi noti.

D. I client VPN Cisco sono supportati da concentratori VPN di terze parti?

R. I client VPN Cisco non sono supportati con concentratori VPN di terze parti.

Autenticazione

D. In che modo i client VPN Cisco versioni 1.1 e 3.x memorizzano internamente i certificati digitali (X.509v3)?

R. Cisco VPN Client 1.1 ha un proprio archivio certificati. Cisco VPN Client 3.x può archiviare i certificati nell'archivio Microsoft utilizzando Common-Application Programming Interface (CAPI) o in un archivio Cisco personalizzato (RSA Data Security).

D. Posso avere lo stesso nome di gruppo e lo stesso nome utente sul concentratore VPN?

R. No, il nome del gruppo e il nome utente non possono essere uguali. Questo è un problema noto, riscontrato nelle versioni software 2.5.2 e 3.0 e integrato nella versione 3.1.2. Per ulteriori informazioni, vedere l'ID bug Cisco CSCdw29034 (solo utenti registrati) in Bug Toolkit.

D. Le schede di verifica complete, ad esempio Defender, sono supportate sul client VPN da Cisco a PIX?

R. No, le schede di questo tipo non sono supportate.

Versione software client VPN

D. Dov'è l'opzione "Set MTU Utility" presente nelle versioni 2.5.2 e precedenti di Cisco VPN Client?

R. Il client VPN Cisco ora adatta le dimensioni della Maximum Transmission Unit (MTU). L'opzione Set MTU Utility non è più un passaggio di installazione obbligatorio. L'opzione Set MTU viene utilizzata principalmente per risolvere i problemi di connettività. Il percorso per selezionare l'opzione SetMTU per un computer Windows è **Start > Programmi > Cisco Systems VPN Client > SetMTU**. Per ulteriori informazioni sull'opzione SetMTU e l'impostazione di questa opzione in altri sistemi operativi, consultare il documento sulla modifica delle dimensioni della MTU tramite l'opzione SetMTU.

D. Quali lingue sono supportate sulle versioni GUI di Cisco VPN Client successive alla 4.0?

R. Le lingue supportate sulle versioni GUI di Cisco VPN Client successive alla 4.0 sono canadese, francese e giapponese.

D. Quali firewall personali sono supportati con Cisco VPN Client?

R. Per fornire un livello di sicurezza più elevato, il client VPN può applicare il funzionamento di un firewall supportato o ricevere un criterio firewall con stato push down per il traffico Internet.

Attualmente, VPN Client 5.0 supporta i seguenti firewall personali:

- BlackIce Defender
- Cisco Security Agent
- Sygate Personal Firewall
- Sygate Personal Firewall Pro
- Sygate Security Agent
- AllarmeZona
- ZonaAlarmPro

A partire dalla versione 3.1, viene aggiunta una nuova funzionalità a VPN 3000 Concentrator che rileva il software firewall personale installato dagli utenti remoti e impedisce agli utenti di connettersi in assenza del software appropriato. Scegliere **Configurazione > Gestione utente > Gruppi > FW client**, quindi fare clic sulla scheda del gruppo per configurare questa funzione

Per ulteriori informazioni sull'applicazione dei criteri firewall su un computer client VPN Cisco, fare riferimento agli scenari di configurazione del firewall.

D. Ci sono problemi di connettività quando si usa Cisco VPN Client 3.x con AOL 7.0?

R. Il client VPN Cisco non funziona con AOL 7.0 senza l'uso del tunneling suddiviso. Per ulteriori informazioni, vedere l'ID bug Cisco CSCdx04842 (solo utenti registrati) in Bug Toolkit.

Configurazione software VPN Client

D. Perché il client VPN Cisco si disconnette dopo 30 minuti? È possibile estendere questo periodo di tempo?

R. Se durante questo periodo di 30 minuti non è presente alcuna attività di comunicazione su una connessione utente, il sistema interrompe la connessione. L'impostazione predefinita del timeout di inattività è 30 minuti, con un valore minimo consentito di 1 minuto e un valore massimo consentito di 2.147.483.647 minuti (oltre 4.000 anni).

Scegliere **Configurazione > Gestione utente > Gruppi**, quindi scegliere il nome del gruppo appropriato per modificare l'impostazione del timeout di inattività. Scegliere **Modifica gruppo**, fare clic sulla scheda **Client hardware** e digitare il valore desiderato nel campo Timeout inattività utente. Digitare **0** per disabilitare il timeout e consentire un periodo di inattività illimitato.

D. È possibile implementare il client VPN Cisco con tutti i parametri preconfigurati?

R. Se il file vpnclient.ini viene fornito con il software VPN Client alla prima installazione, il client VPN viene configurato automaticamente durante l'installazione. Potete anche distribuire i file di profilo (un file .pcf per ciascuna voce di connessione) come profili di connessione preconfigurati per la configurazione automatica. Per distribuire copie preconfigurate del software VPN Client agli utenti per l'installazione, attenersi alla seguente procedura:

1. Copiare i file software VPN Client dal CD-ROM di distribuzione in ciascuna directory in cui è stato creato un file vpnclient.ini (globale) e profili di connessione separati per un gruppo di utenti.**Nota:** per la piattaforma Mac OS X, i file preconfigurati vengono inseriti nelle cartelle Profili e Risorse prima dell'installazione del client VPN. Il file vpnclient.ini viene inserito nella directory del programma di installazione. È necessario inserire i file vpnclient.ini personalizzati nella directory VPN Client Installer allo stesso livello delle cartelle Profili e Risorse. Per ulteriori informazioni, vedere il capitolo 2 della Guida dell'utente del client VPN per Mac OS X
2. Preparare e distribuire il software in dotazione. Distribuzione in rete o su CD-ROM. Accertarsi che il file vpnclient.ini e i file dei profili si trovino nella stessa directory con tutti i file immagine del CD-ROM. Gli utenti possono installare da questa directory tramite una connessione di rete; oppure copiare tutti i file su un nuovo CD-ROM per la distribuzione; in alternativa, è possibile creare un file ZIP autoestraente che contenga tutti i file di questa directory e che venga scaricato dagli utenti, quindi installare il software.
3. Fornire agli utenti tutte le informazioni e le istruzioni di configurazione necessarie. Vedere il Capitolo 2 della Guida dell'utente di VPN Client per la propria piattaforma.

D. Sembra che il client VPN Cisco sia in conflitto con la mia scheda NIC. Come risolvere il problema?

R. Accertarsi di eseguire i driver più recenti sulla scheda NIC. Questa operazione è sempre consigliata. Se possibile, verificare se il problema è specifico del sistema operativo, dell'hardware

del PC e di altre schede NIC.

D. Come posso automatizzare la connessione Cisco VPN Client da Connessione remota?

R. Scegliere **Opzioni > Proprietà > Connessioni** e fare in modo che il client VPN Cisco estragga una voce della rubrica di Connessione remota per automatizzare completamente la connessione remota alla connessione VPN.

D. Come configurare Cisco VPN 3000 Concentrator in modo da notificare agli utenti remoti gli aggiornamenti dei client VPN?

R. È possibile notificare agli utenti VPN Client quando è il momento di aggiornare il software VPN Client sui loro sistemi remoti. Per ulteriori informazioni, fare riferimento a Notifica di un aggiornamento client agli utenti remoti. Assicuratevi di digitare le informazioni sulla versione come "(Rel)", come indicato nel passo 7 del processo.

D. Cosa può causare un ritardo prima che venga visualizzato il client VPN Cisco, in particolare quando è abilitata l'opzione "Avvia prima dell'accesso"?

R. Il client VPN Cisco è in modalità *fallback*. Ciò contribuisce al ritardo. In modalità fallback, il client VPN funziona in modo diverso quando viene avviato prima che l'accesso sia in uso. In modalità fallback, il client VPN non verifica se i servizi Windows necessari sono stati avviati. Di conseguenza, la connessione VPN potrebbe non riuscire se avviata troppo rapidamente.Disinstallare Cisco VPN Client e rimuovere le applicazioni in conflitto per consentire l'avvio senza essere in modalità "fallback". Quindi reinstallare il client VPN Cisco. Per ulteriori informazioni sulla modalità di fallback, fare riferimento a Avvia prima di accedere.

per ulteriori informazioni, vedere gli ID dei bug Cisco CSCdt88922 (solo utenti registrati) e CSCdt5739 (solo utenti registrati) in Bug Toolkit.

D. È necessario comprendere la differenza tra ipsecdialer.exe e vpngui.exe. Perché vpngui.exe è installato in STARTUP in Windows XP, ma è comunque necessario avviare manualmente ipsecdialer per raggiungere le risorse aziendali? E (a parte la dimensione) questi programmi sembrano innescare la stessa cosa: un accesso VPN alla rete aziendale.

R. ipsecdialer.exe era il meccanismo di avvio originale per Cisco VPN Client versione 3.x. Quando la GUI è stata modificata nelle versioni 4.x, è stato creato un nuovo eseguibile denominato vpngui.exe. Il file ipsecdialer.exe è stato riportato in avanti solo per compatibilità con le versioni precedenti e avvia semplicemente vpngui.exe. Questo è il motivo per cui potete vedere la differenza nella dimensione del file.

Pertanto, quando si esegue il downgrade dalla versione 4.x alla versione 3.x di Cisco VPN Client, è necessario il file ipsecdialer.exe per avviare questa operazione.

D. È possibile rimuovere in modo sicuro l'icona della VPN di avvio? Perché è necessario?

R. Il client VPN Cisco nella cartella di avvio supporta la funzione "Avvia prima di accedere". Se non si utilizza la funzione, non è necessario nella cartella di avvio.

D. Perché viene aggiunto "user_logon" e non il collegamento ipsecdialer.exe? Qual è lo scopo di "accesso utente"?

R. La funzione "Avvia prima dell'accesso" richiede "user_logon", ma non è necessaria per un normale avvio del client VPN Cisco da parte dell'utente.

Problemi NAT/PAT

D. Si verificano problemi con un solo client VPN (per le versioni 3.3 e precedenti) in grado di connettersi tramite un dispositivo PAT (Port Address Translation). Cosa posso fare per alleviare questo problema?

R. Si è verificato un bug in diverse implementazioni NAT (Network Address Translation)/PAT che ha impedito la traduzione delle porte inferiori a 1024. Sul client VPN Cisco 3.1, anche se la trasparenza NAT è abilitata, la sessione ISAKMP (Internet Security Association and Key Management Protocol) utilizza UDP 512. Il primo client VPN passa attraverso il dispositivo PAT e mantiene la porta di origine 512 all'esterno. Quando si connette il secondo client VPN, la porta 512 è già in uso. Il tentativo fallisce.

Sono disponibili tre soluzioni.

- Correggere il dispositivo PAT.
- Aggiornare i client VPN alla versione 3.4 e utilizzare l'incapsulamento TCP.
- Installare una VPN 3002 che sostituisca tutti i client VPN.

D. È possibile collegare due notebook al client VPN Cisco dalla stessa posizione?

R. Due client possono connettersi allo stesso headend dalla stessa posizione purché non si trovino entrambi dietro un dispositivo che esegue PAT, ad esempio un router/firewall SOHO. Molti dispositivi PAT possono mappare UNA connessione VPN a un client, ma non a due. Per consentire a due client VPN di connettersi dalla stessa posizione dietro un dispositivo PAT, abilitare una sorta di incapsulamento come NAT-T, IPSec over UDP o IPsec over TCP sull'headend. In genere, è necessario abilitare NAT-T o un altro incapsulamento se tra il client e l'headend è presente un dispositivo NAT.

Varie

D. Quando mi connetto alla rete in ufficio utilizzando il notebook e poi lo porto a casa, ho problemi a collegarmi a VPN 3000 Concentrator da casa. Qual è il problema?

R. È possibile che nel laptop siano memorizzate le informazioni di routing dalla connessione LAN. Per informazioni su come risolvere il problema, fare riferimento a Client VPN con problemi di routing Microsoft.

D. Come è possibile stabilire se un client VPN è connesso al concentratore VPN?

R. Controllare la chiave del Registro di sistema HKLM\Software\Cisco Systems\VPN Client\TunnelEstablished. Se è attivo un tunnel, il valore è 1. Se non è presente alcun tunnel, il valore è 0.

D. Si verificano problemi con la connessione NetMeeting da un PC dietro un concentratore VPN a un client VPN, ma la connessione funziona quando si esegue dal PC a un client VPN dietro un concentratore VPN. Come risolvere il problema?

R. Per controllare le impostazioni di connessione, procedere come segue:

- Sull'unità principale del PC, scegliere **Programmi > Cisco Systems > VPN Client > Profiles**. Fare clic con il pulsante destro del mouse sul profilo utilizzato e scegliere **Apri con** per aprire il profilo in un editor di testo, ad esempio Blocco note. Quando si sceglie il programma da utilizzare, assicurarsi di deselezionare la casella **Utilizza sempre questo programma per aprire i file**. Individuare il parametro di profilo per ForcekeepAlives e modificare il valore da 0 a **1**, quindi salvare il profilo.o
- Per il client VPN, scegliere **Opzioni > Proprietà > Generale**, quindi immettere un valore per "Timeout risposta peer", come mostrato in questa finestra di esempio. È possibile specificare una sensibilità di timeout compresa tra 30 secondi e 480 secondi.o
- Per il concentratore VPN, scegliere **Configurazione > Gestione utenti > Gruppi > *Modifica gruppo***. Nella scheda IPSec scegliere l'opzione relativa ai pacchetti keepalive IKE, come mostrato nella finestra di esempio.

L'intervallo DPD (Dead Peer Detection) varia in base all'impostazione della sensibilità. Una risposta non ricevuta passa a una modalità più aggressiva e invia pacchetti ogni cinque secondi fino a raggiungere la soglia di risposta del peer. In quel momento, la connessione è interrotta. È possibile disattivare i pacchetti keepalive, ma se la connessione si interrompe effettivamente, è necessario attendere il timeout. Cisco consiglia di impostare inizialmente un valore di sensibilità molto basso.

D. Il client VPN Cisco supporta la doppia autenticazione?

R. No. L'autenticazione doppia non è supportata sul client VPN Cisco.

D. Come configurare il client VPN Cisco per la connessione in modalità principale anziché in modalità aggressiva?

R. Per consentire la connessione del client VPN Cisco in modalità principale, è necessario utilizzare le firme digitali (certificati). A tale scopo, è possibile procedere in due modi:

1. Ottenere i certificati CA dal provider di certificati di terze parti (ad esempio Verisign o Entrust) sul router e su tutti i client VPN Cisco. Registrare i certificati di identità dallo stesso server CA e utilizzare le firme digitali per autenticarsi tra il client VPN di Cisco e il router. Per ulteriori informazioni su questa configurazione, consultare il documento sulla configurazione di IPSec tra i router Cisco IOS e il client VPN Cisco con certificati Entrust.
2. La seconda opzione consiste nel configurare il router come server CA e l'headend della VPN ad accesso remoto. L'installazione dei certificati (e di tutto il resto) rimarrà come descritto nel

collegamento precedente, con la differenza che il router si comporterà come un server CA. Per ulteriori informazioni, fare riferimento all'esempio di VPN da LAN a LAN dinamica tra i router Cisco IOS che utilizzano la CA IOS sull'hub.

D. Come fare per rendere di sola lettura i parametri richiesti nel file di accesso client VPN?

R. Aggiungere un punto esclamativo (!) davanti a ciascun parametro nel file .pcf per ciascun utente in modo da rendere il parametro di sola lettura.

I valori dei parametri che iniziano con un punto esclamativo (!) non possono essere modificati dall'utente nel client VPN. I campi di questi valori nella GUI sono disattivati (sola lettura).

Di seguito è riportato un esempio di configurazione:

File .pcf originale

```
[main]

Description=connection to TechPubs server

Host=10.10.99.30

AuthType=1

GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C85
              1ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=

ISPCommand=

Username=alice
```

File .pcf modificato

```
[main]

!Description=connection to TechPubs server

!Host=10.10.99.30

AuthType=1

!GroupName=docusers

GroupPwd=

enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C
```

```
          851ECF2DCC8BD488857EFA FDE1397A95E01910CABECCE4E040B7A77BF

EnableISPConnect=0

ISPConnectType=0

ISPConnect=

ISPCommand=

!Username=alice
```

In questo esempio, l'utente non è in grado di modificare i valori *Description*, *Host*, *GroupName* e *Username*.

D. È possibile limitare/limitare l'accesso per i client VPN in base agli indirizzi MAC?

R. No. Non è possibile limitare/limitare l'accesso per i client VPN in base agli indirizzi MAC.

Informazioni correlate

- Pagina di supporto per i client Cisco VPN 3000
- Pagina di supporto per Cisco VPN Client
- Soluzioni per la risoluzione dei problemi più comuni di VPN IPSec di L2L e ad accesso remoto
- Documentazione e supporto tecnico – Cisco Systems