Preguntas frecuentes sobre VPN Client

Contenido

Introducción

Este documento responde las preguntas más frecuentes sobre Cisco VPN Client.

Nota: Aquí están las convenciones de nombres para los diversos clientes VPN:

- Cisco Secure VPN Client versiones 1.0 a 1.1a solamente
- Cisco VPN 3000 Client versión 2.x solamente
- Cisco VPN Client 3.x y posterior solamente

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Descargue el Software VPN Client

P. ¿Dónde puedo descargar el software Cisco VPN Client?

A. Debe iniciar sesión y poseer un contrato de servicio válido para acceder al software Cisco VPN Client. El software Cisco VPN Client se puede descargar de la página Download Software (sólo clientes registrados). **Si no tiene un contrato de servicio válido asociado a su perfil de Cisco.com, no puede iniciar sesión ni descargar el software de cliente VPN.**

Para obtener un contrato de servicio válido, puede:

- Póngase en contacto con su equipo de Cuenta de Cisco si tiene un acuerdo de compra directo.
- Póngase en contacto con un Socio o Revendedor de Cisco para adquirir un acuerdo de servicio.

- Use el Administrador de Perfil (clientes registrados solamente) para actualizar su perfil de Cisco.com y solicitar asociación a un acuerdo de servicio.

P. El área de descarga de Cisco VPN Client parece estar vacía. ¿Por qué?

A. Cuando alcanza el área de VPN Client del Centro de Software (clientes registrados solamente) asegúrese de seleccionar el área de descargas para su sistema operativo deseado en el centro de la página.

P. ¿Cómo puedo inhabilitar la Función Stateful Firewall durante la instalación de Cisco VPN Client?

A. Para las versiones de VPN Client anteriores a la 5.0:

Consulte la sección Cambios en la Documentación de VPN Client Rel 4.7 Release Notes para obtener información acerca de los dos temas "Cómo Usar MSI para Instalar VPN Client de Windows sin Stateful Firewall" y "Cómo Usar InstallShield para Instalar VPN Client de Windows sin Stateful Firewall".

Para las versiones de VPN Client posteriores a la 5.0:

A partir de Cisco VPN Client versión 5.0.3.0560, se agregó un indicador de instalación MSI para evitar la instalación de la hermandad en los archivos de firewall:

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

Refiérase a la sección Omitir la Instalación de Archivos de Firewall cuando No se Requiere Stateful Firewall para obtener más información sobre esto.

P. ¿Cómo desinstalo o actualizo Cisco VPN Client?

A. Consulte Remoción de una Versión de VPN Client Instalada con el Instalador MSI para obtener información sobre cómo desinstalar manualmente (InstallShield) y, a continuación, actualizar Cisco VPN Client versión 3.5 y posterior para Windows 2000 y Windows XP.

El software Cisco VPN Client para Windows 2000 y Windows XP puede descargar de forma segura actualizaciones y nuevas versiones automáticamente a través de un túnel desde un concentrador VPN 3000 u otro servidor VPN que pueda proporcionar notificaciones. El requisito previo mínimo para esto es que los usuarios remotos deben tener instalado VPN Client para Windows 4.6 o posterior en sus PC para utilizar la función de actualización automática.

Con esta función, llamada autoupdate, los usuarios no necesitan desinstalar una versión antigua del software, reiniciar, instalar la nueva versión y después reiniciar otra vez. En lugar de esto, un administrador realiza las actualizaciones y los perfiles disponibles en un servidor web y cuando un usuario remoto inicia VPN Client, el software detecta que está disponible una descarga y la obtiene automáticamente. Para obtener más información, consulte Administración de Actualizaciones Automáticas y Cómo Funciona la Actualización Automática.

Para obtener información sobre cómo configurar la actualización del cliente en un Cisco ASA Series 5500 Adaptive Security Appliance mediante ASDM, consulte Configuración de la Actualización del Software Cliente Usando ASDM.

P. Deseo personalizar los clientes VPN para Vista. Sé que, con la nueva versión de VPN Client para Vista, no existe el archivo oem.mst. ¿Cómo se pueden personalizar las nuevas versiones de VPN Client (5.x), o donde puedo encontrar este archivo?

A. El archivo MST ya no se proporciona con VPN Client, pero puede descargarlo desde la página Download Software (sólo clientes registrados):

Nombre de Archivo: Readme y MST para la instalación en la versión internacional de Windows.

Sistema operativo

P. ¿Cisco proporciona un VPN Client para Windows Vista?

A. La nueva versión Cisco VPN Client 5.0.07 admite Windows Vista en x86 (32 bits) y x64. Consulte 5.0.07.0240 Release Notes para obtener más información.

Nota: Cisco VPN Client se soporta solamente en Windows Vista clean install, lo que significa que una actualización de cualquier sistema operativo Windows a Windows Vista no se soporta con el software cliente VPN. Debe instalar nuevamente Windows Vista y a continuación instalar el software VPN Client para Vista.

Nota: Si no tiene un contrato de servicio válido asociado a su perfil de Cisco.com, no puede iniciar sesión ni descargar el software VPN Client. Consulte Cómo Descargar VPN Client para obtener más información.

Consejo: Cisco AnyConnect VPN Client ahora está disponible para sistemas operativos Windows, que incluye Vista de 32 y 64 bits. El cliente AnyConnect soporta SSL y DTLS. No soporta IPsec en este momento. Además, AnyConnect está disponible solamente para el uso con Cisco Adaptive Security Appliance que ejecuta la versión 8.0(2) o posterior. El cliente también puede usarse en el modo weblaunch con los dispositivos IOS que ejecutan la versión 12.4(15)T. El VPN3000 no es compatible.

Cisco AnyConnect VPN Client y el ASA 8.0 se pueden obtener del Centro de Software (clientes registrados solamente). Consulte Release Notes de Cisco AnyConnect VPN Client para obtener más información sobre AnyConnect Client. Consulte Release Notes de Cisco ASA 5500 Series Adaptive Security Appliances para obtener más información sobre ASA 8.0.

Nota: Si no tiene un contrato de servicio válido asociado a su perfil de Cisco.com, no puede iniciar sesión ni descargar el software AnyConnect VPN Client o ASA. Consulte Cómo Descargar VPN Client para obtener más información.

P. ¿Cómo configuro una conexión PPTP desde una PC con Microsoft Windows?

A. La Configuración depende de la versión de Microsoft Windows que tenga. Debe contactar a Microsoft para información específica. A continuación se indican las instrucciones de configuración para algunas de las versiones de Windows comunes:

Windows 95

1. Instale Msdun13.exe.
2. Elija **Programs > Accessories > Dial Up Networking**.
3. Cree una nueva conexión denominada "PPTP".
4. Seleccione el **Adaptador VPN como dispositivo para la conexión.**
5. Ingrese la dirección IP de la interfaz pública del switch y haga clic en **Finish**.
6. Regrese a la conexión que acaba de crear, haga clic con el botón derecho y elija **Properties**.
7. En Allowed Network Protocols, como mínimo, desmarque **netbeui**.
8. Determine la configuración Opciones Avanzadas : Respete los ajustes predeterminados para permitir que el switch y el cliente negocien automáticamente el método de autenticación.Habilite **Contraseña cifrada Requerida para forzar la autenticación de Handshake Authentication Protocol (CHAP).**Active **Require Encrypted Password y Require Data Encryption para forzar la autenticación MS-CHAP.**

Windows 98

1. Siga estos pasos para instalar la función PPTP: Elija **Start > Settings > Control Panel > Add New Hardware** y haga clic en **Next**.Haga clic en **Select from List**, elija **Network Adapter** y haga clic en **Next**.Elija **Microsoft en el panel izquierdo y Microsoft VPN Adapter en el derecho.**
2. Siga estos pasos para configurar la función PPTP: Elija **Start > Programs > Accessories > Communications > Dial Up Networking**.Haga clic en **Make New Connection** y elija **Microsoft VPN Adapter en Select a device.** Dirección IP del servidor VPN = punto final del túnel 3000.
3. Siga estos pasos para que su PC también permita Password Authentication Protocol (PAP): **Nota:** La autenticación predeterminada de Windows 98 consiste en utilizar el cifrado de contraseña (CHAP o MS-CHAP).Elija **Properties > Server types**.Anule la selección de **Require encrypted password**. Puede configurar un cifrado de datos (Cifrado punto a punto de Microsoft [MPPE] o no) en esta área.

Windows 2000

1. Elija **Start > Programs > Accessories > Communications > Network y Dialup connections**.
2. Haga clic en **Make new connection** y luego en **Next**.
3. Elija **Connect to a private network through the Internet and Dial a connection prior (no seleccione esto si tiene una LAN) y haga clic en Next**.
4. Ingrese el nombre de host o la dirección IP del extremo del túnel (3000).
5. Si necesita cambiar el tipo de contraseña, elija **Properties > Security for the connection> Advanced**. El valor predeterminado es MS-CHAP y MS-CHAP v2 (no CHAP o PAP). Puede configurar un cifrado de datos (MPPE o no) en esta área.

Windows NT

Consulte Instalación, Configuración, y Uso PPTP con Clientes y Servidores Microsoft .

P. ¿Qué versiones de sistema operativo admite Cisco VPN Client?

A. Constantemente se agrega soporte para sistemas operativos adicionales para el cliente VPN. Consulte Requisitos del Sistema en las notas de versión de VPN Client 5.0.07 para determinarlo, o consulte Hardware y Clientes VPN de Cisco que Soportan IPsec/PPTP/L2TP.

Notas:

- VPN Client incluye soporte para estaciones de trabajo de procesador dual y de doble núcleo para Windows XP y Windows Vista.
- La versión 4.8.00.440 de Windows VPN Client era la versión final que soportaba oficialmente el sistema operativo Windows 98.
- Windows VPN Client Release 4.6.04.0043 fue la versión final que soportó oficialmente el sistema operativo Windows NT.
- Cisco VPN Client ver 5.0.07 soporta Windows Vista y Windows 7 en las ediciones x86 (de 32 bits) y x64 (de 64 bits).
- Cisco VPN Client solamente soporta Windows XP de 32 bits, pero no soporta Windows XP de 64 bits.**Nota:** La compatibilidad con Windows Vista de 32 bits estaba disponible en todas las versiones 5.x. Cisco VPN Client versión 5.0.07 agregó el soporte de 64 bits.

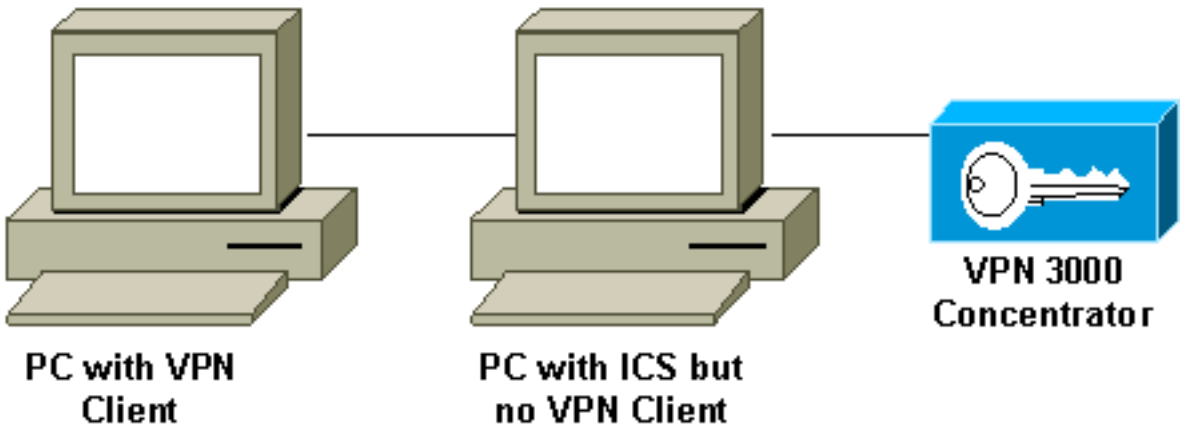
P. ¿Necesito ser administrador en equipos Windows NT/2000 para cargar el cliente VPN?

A. Sí, debe tener privilegios de administrador para instalar el cliente VPN en Windows NT y Windows 2000 porque estos sistemas operativos necesitan privilegios de administrador para unirse a los controladores de red existentes o para instalar nuevos controladores de red. El software VPN Client es un software de networking. Debe tener privilegios de administrador para instalarlo.

P. ¿Puede el cliente Cisco VPN funcionar con Microsoft Internet Connection Sharing (ISC) instalado en la misma máquina?

A. No, Cisco VPN 3000 Client no es compatible con Microsoft ICS en el mismo equipo. Debe desinstalar el ICS antes de instalar el cliente VPN. Consulte Cómo inhabilitar ICS al Preparar la Instalación o Actualización a Cisco VPN Client 3.5.x en Microsoft Windows XP para obtener más información.

Aunque tener el cliente VPN e ICS en la misma PC no funciona, esta disposición sí funciona.



P. Mi cliente VPN parece conectarse únicamente a ciertas direcciones. Tengo Windows XP. ¿Qué debo hacer?

A. Verifique que el firewall incorporado en Windows XP esté inhabilitado.

P. ¿Es compatible el cliente VPN Cisco con el firewall con estado de Windows XP?

A. Este problema ha sido resuelto. Consulte Cisco bug ID CSCdx15865 (sólo clientes registrados) en Bug Toolkit para obtener más información.

P. Al instalar el cliente VPN en Windows XP y Windows 2000, ¿se inhabilita la interfaz de usuarios múltiples?

A. La instalación inhabilita la pantalla de bienvenida y el switching deusuario rápido. Consulte Cisco bug ID CSCdu24073 (sólo clientes registrados) en Bug Toolkit para obtener más información.

P. ¿Cómo puedo hacer que el cliente VPN para Linux pase a un segundo plano después de la ejecución? Si inicio una conexión como vpnclient connect foo, puedo ingresar, pero el shell retorna.

A. Después de registrarse, escriba:

- ^Z
- bg

P. Cuando instalo Cisco VPN Client en Windows XP Home Edition, la barra de tareas no se ve. Cómo se deshace esto

A. Elija Control Panel > Network Connections > Remove Network Bridge para ajustar esta configuración.

P. Cuando intento instalar Linux VPN Client en RedHat 8.0, me salta un error que dice que el módulo no puede cargarse porque fue compilado con GCC 2 y el kernel fue compilado con GCC 3.2. ¿Qué debo hacer?

A. Esto se debe a que el nuevo RedHat posee una nueva versión del compilador GCC (3.2+), que hace que falle el cliente VPN de Cisco. Este problema ha sido resuelto y está disponible en Cisco VPN 3.6.2a. Consulte Cisco bug ID CSCdy49082 (sólo clientes registrados) en Bug Toolkit para obtener más detalles o paradescargar el software del Centro de VPN Software (sólo clientes registrados) .

P. ¿Por qué el software inhabilita el Fast User Switching cuando instalo VPN Client 3.1 en Windows XP?

A. Microsoft inhabilita automáticamente Fast User Switching en Windows XP cuando se especifica GINA.dll en el registro. Cisco VPN Client instala CSgina.dll a fin de implementar la característica “Start Before Login" (Comenzar antes del inicio sesión). Si necesita Fast User Switching, inhabilite la función "Comenzar Antes de Iniciar Sesión". Los usuarios registrados pueden obtener más información en Cisco bug ID CSCdu24073 (clientes registrados solamente) en Bug Toolkit.

P. ¿Admite el cliente VPN IPsec la función Start Before Logon (SBL) en Windows 7?

A. La función SBL no se soporta en los clientes VPN IPSec en Windows7. Es compatible con

AnyConnect VPN Client.

Mensajes de error

P. Cuando instalo Cisco VPN Client 4.x, recibo este mensaje de error: **Advertencia 201: The necessary VPN sub-system is not available. No puede conectatr con el servidor VPN remoto**

A. Este problema se puede producir por paquetes de firewall instalados en la computadora de su cliente de VPN. Para evitar este mensaje de error, asegúrese de que haya firewall o programas antivirus instalados o que se ejecuten en su PC al momento de la instalación.

P. Actualicé a Mac OS X 10.3 (conocido como "Panther"), pero ahora mi Cisco VPN Client 4.x muestra estos mensajes de error: **Secure VPN Connection terminated locally by the Client Reason: Unable to contact the security gateway**

A. Debe agregar UseLegacyIKEPort=0 al perfil (archivo .pcf) que se encuentra en el directorio /etc/CiscoSystemsVPNClient/Profiles/ para que Cisco VPN Client 4.x funcione con Mac OS X 10.3 ("Panther").

P. Cuando intento desinstalar el cliente VPN, recibo este mensaje de error: **Error msg: no se pudo encontrar el archivo de desinstalación...** ¿Qué significa este mensaje de error y cómo puedo completar con éxito la desinstalación?

A. Verifique Control Panel (Panel de control) de la red para asegurarse de que el Extensor NDIS determinante (DNE) no haya sido instalado. Además elija **Microsoft > Current Version > Uninstall para verificar la desinstalación del archivo.** Quite el archivo **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{5624C000-B109-11D4-9DB4-00E0290FCAC5} y vuelva a intentar la desinstalación.**

P. No puedo instalar el cliente VPN en Windows 2000 Professional. Recibo este error: **No se pudo instalar un archivo de soporte de instalación.** Falla Catastrófica. ¿Qué debo hacer?

A. Quite la clave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall . Luego reinicie la computadora y vuelva a instalar el cliente VPN.

Nota: Para encontrar la clave correcta para el software Cisco VPN Client bajo la trayectoria HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\<*clave a determinar*>, vaya a HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\ y haga clic en **VPN Client**. En la ventana derecha, vea la trayectoria de desinstalación (bajo el nombre de la columna). La columna de datos correspondiente muestra el valor de la clave del cliente VPN. Tome nota de esta clave, vaya a HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\, seleccione la clave determinada y elimínela.

ConsulteTroubleshooting de Error de Inicialización y consulte Cisco bug ID CSCdv15391 (clientes registrados solamente) en Bug Toolkit para obtener más información.

P. Cuando intento instalar Linux VPN Client en RedHat 8.0, recibo un error que dice que el módulo no puede cargarse porque fue compilado con GCC 2 y el kernel fue compilado con GCC 3.2. ¿Qué debo hacer?

A. Este problema se debe a que el nuevo RedHat posee una nueva versión del compilador GCC (3.2+), que hace que falle el Cisco VPN Client actual. Este problema ha sido resuelto y está disponible en Cisco VPN 3.6.2a. Consulte Cisco bug ID CSCdy49082 (sólo clientes registrados) en Bug Toolkit para obtener más detalles o paradescargar el software del Centro de VPN Software (sólo clientes registrados) .

P. Me salta el mensaje de error "peer no longer responding" cuando Linux Client 3.5 intenta establecer conexión IPSec con un PIX o un VPN 3000 Concentrator. ¿Qué debo hacer?

A. El síntoma de este problema es que el Linux Client parece intentar conectarse, pero nunca obtiene respuesta del dispositivo de gateway.

El sistema operativo de Linux cuenta con un firewall integrado (ipchains) que bloquea el puerto 500 de UDP, el puerto 1000 de UDP y los paquetes de carga de seguridad de encapsulamiento (ESP). Dado que el escudo de protección está activado de manera predeterminada, deberá desactivarlo; o bien, abrir los puertos para comunicación IPSec para las conexiones de entrada y de salida a fin de solucionar el problema.

P. Recibo un error de extensión kernel cuando intento ejecutar Cisco VPN 5000 5.2.2 en Mac OS X 10.3. ¿Qué debo hacer?

A. Como se indica en las release notes del producto, Cisco VPN 5000 Client es soportado hasta la versión 10.1.x y, por lo tanto, no es soportado en la versión 10.3. Es posible que el cliente VPN funcione cuando restablezca los permisos en dos de los archivos instalados después de ejecutar el script de instalación. Aquí tiene un ejemplo:

Nota: Esta configuración *no* es compatible con Cisco.

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

P. No puedo instalar la nueva versión de Cisco VPN Client. Cuando instalo, recibo uno de estos mensajes de error: "**Error DNEinst execution error while installing DNE, return code -2146500093" o "InstallDNE Error: Error de ejecución de DNEinst al instalar DNE, devuelve código -2147024891**". Este problema ocurre cuando instalé el Deterministic Network Enhancer.

A. Instale la última versión de DNEsde Deterministic Networks .

P. Obtengo estos registros para Cisco VPN Client cuando hago una conexión:

```
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.
```

A. Es un mensaje de error bastante común, que en general requiere la desinstalación manual del cliente. Sigue las instrucciones de este link. Remoción de una Versión de VPN Client Instalada con el Instalador MSI.

Una vez que ha hecho la desinstalación, asegúrese de reiniciar el equipo. Vuelva a a instalar el cliente. Asegúrese de registrarse comousuario con derechos de administración en el equipo local.

P. Cuando intento conectar Cisco VPN Client en un Mac OS, recibo este mensaje de error: `Error 51- No se puede establecer comunicación con el subsistema VPN.` ¿Cómo puedo resolver este problema?

A. El problema puede resolverse si reinicia el servicio después de cerrar el cliente VPN de esta manera:

Para detener:

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

Para comenzar:

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

Verifique también que se ejecuta lo siguiente en la misma máquina en la que está instalado el cliente VPN y inhabilítelo.

- Cualquier software virtual (por ejemplo, VMWare Fusions, Parallels, crossovers).
- Cualquier software antivirus/de firewall.
- Compatibilidad del cliente VPN con el sistema operativo de 64 bits; consulte las Release Notes de Cisco VPN Client.

P. Recibo el error "Reason 442: failed to enable virtual adapter". ¿Cómo puedo resolver este error?

A. El error `Reason 442: failed to enable virtual adapter aparece después que Vista informa que se ha detectado una dirección IP duplicada.` Las conexiones subsiguientes fallan con el mismo mensaje, pero Vista no informa que se ha detectado una dirección IP duplicada. Consulte Una Dirección IP Duplicada Provoca el Error 442 en Windows Vista para obtener más información sobre cómo resolver este problema.

P. Cuando instalo Cisco VPN Client, se recibe el error `Deterministic Network Enhancer Add Plugin Failed.` ¿Cómo se resuelve este error?

A. Instalar el adaptador DNE podría resolver el problema. Es mejor utilizar la versión de Installshield para la instalación en vez del MSI.

P. He recibido este error: `Reason 442: no se pudo habilitar el adaptador virtual.` ¿Cómo

puedo resolver este problema?

A. Este error aparece después de que Windows 7 y Windows Vista informen de una dirección IP duplicada detectada. Las conexiones posteriores fallan con el mismo mensaje, pero el SO no informa que se ha detectado la dirección IP duplicada. Refiérase a Duplicate IP Address Triggers Error 442 en Windows 7 y Vista para obtener más información sobre cómo resolver este problema.

P. Cuando intento iniciar VPN Client 4.9 para MAC OS 10.6, recibo este error: `Error 51: No se puede comunicar con el subsistema vpn.` ¿Cómo se resuelve este problema?

A. Este problema ocurre porque el soporte de 64 bits no está disponible con el cliente VPN de Cisco para la versión 4.9 del sistema operativo MAC. Como solución alternativa, puede arrancar en modo kernel de 32 bits. Para obtener más información, refiérase al ID de bug de Cisco CSCth11092 (sólo clientes registrados) y el cliente Cisco VPN para las notas de versión de MAC OSX.

Compatibilidad de Terceros

P. ¿El cliente Nortel es compatible con los concentradores VPN 3000 de Cisco?

A. No. Nortel Client no puede conectarse al Cisco VPN 3000 Concentrator.

P. ¿Puedo tener clientes VPN de otros proveedores, como el Nortel Contivity VPN Client, instalados simultáneamente con Cisco VPN Client?

A. No. Hay problemas conocidos cuando se instalan varios clientes VPN en el mismo equipo.

P. ¿Se soportan Cisco VPN Clients con concentradores VPN de terceros?

A. No se soportan Cisco VPN Clients con concentradores VPN de terceros.

Autenticación

P. ¿Cómo almacenan internamente las versiones 1.1 y 3.x de Cisco VPN Clients los certificados digitales (X.509v3)?

A. Cisco VPN Client 1.1 tiene su propio almacén de certificados. Cisco VPN Client 3.x puede almacenar los certificados en el almacén de Interfaz de Microsoft de Programación de Aplicaciones Comunes (CAPI), o puede almacenarlos en el propio almacén de Cisco (Seguridad de Datos RSA).

P. ¿Puedo tener el mismo nombre de grupo y nombre de usuario en el concentrador VPN?

A. No, el nombre de grupo y el nombre de usuario no pueden ser iguales. Éste es un problema conocido que aparece en las versiones de software 2.5.2 y 3.0, e integradas en 3.1.2. Consulte

Cisco bug ID CSCdw29034 (sólo clientes registrados) en Bug Toolkit para obtener más información.

P. ¿Las tarjetas de autenticación completa como las Defender son compatibles con Cisco VPN Client para PIX?

A. No, las tarjetas de este tipo no están admitidas.

Versión de Software de VPN Client

P. ¿Qué pasó con la opción "Set MTU Utility" que estaba presente en las versiones 2.5.2 y anteriores de Cisco VPN Client?

A. Ahora, Cisco VPN Client ajusta el tamaño de la Unidad de Transmisión Máxima (MTU). La opción Set MTU Utility ya no es un paso de instalación necesario. La opción Set MTU se utiliza sobre todo para troubleshooting de problemas de conectividad. La trayectoria para seleccionar la opción SetMTU para una máquina Windows es **Start > Programs > Cisco Systems VPN Client > SetMTU**. Para obtener más información sobre la opción SetMTU y cómo configurar esta opción en otros sistemas operativos, consulte Cambio del Tamaño de la MTU mediante la Opción SetMTU.

P. ¿Cuáles son los idiomas soportados en las versiones de la GUI de Cisco VPN Client posteriores a la 4.0?

A. Los idiomas soportados en las versiones de la GUI de Cisco VPN Client posteriores a la 4.0 son francés canadiense y japonés.

P. ¿Qué tipos de firewall personales son compatibles con el Cisco VPN Client?

A. Para proporcionar un mayor nivel de seguridad, VPN Client puede hacer cumplir la operación de un firewall soportado o recibir una política de firewall con estado transferida para el tráfico dirigido a Internet.

Actualmente, VPN Client 5.0 soporta los siguientes firewalls personales:

- BlackIce Defender
- Cisco Security Agent
- Sygate Personal Firewall
- Sygate Personal Firewall Pro
- Sygate Security Agent
- ZoneAlarm
- ZoneAlarmPro

A partir de la versión 3.1, se agrega una nueva función al VPN 3000 Concentrator que detecta qué usuarios remotos de software de firewall personal se han instalado y evita que los usuarios se conecten en ausencia de software adecuado. Elija **Configuration > User Management > Groups > Client FW**, y haga clic en la pestaña del grupo para configurar esta función

Para obtener más información sobre la aplicación de la política del firewall en una máquina con Cisco VPN Client, consulte los Escenarios de Configuración del Firewall.

P. ¿Hay problemas de conectividad al usar Cisco VPN Client 3.x con AOL 7.0?

A. Cisco VPN Client no funciona con AOL 7.0 sin el uso de tunelización dividida. Consulte Cisco bug ID CSCdx04842 (sólo clientes registrados) en Bug Toolkit para obtener más información.

Configuración del Software VPN Client

P. ¿Por qué Cisco VPN Client se desconecta a los 30 minutos? ¿Puedo prolongar este período de tiempo?

A. Si no hay actividad de comunicación en una conexión de usuario durante este período de 30 minuto9s, el sistema termina la conexión. La configuración predeterminada de tiempo de espera inactivo es 30 minutos, con un valor mínimo permitido de 1 minuto y un valor máximo permitido de 2,147,483,647 minutos (más de 4,000 años).

Elija **Configuration > User Management > Groups** y elija el nombre de grupo adecuado para modificar la configuración de tiempo de espera inactivo. Elija **Modify Group**, haga clic en la pestaña **HW Client y escriba el valor que desee en el campo User Idle Timeout.** Escriba **0 para inhabilitar el tiempo de espera y permitir un período inactivo ilimitado.**

P. ¿Es posible implementar el cliente VPN de Cisco con todos los parámetros preconfigurados?

A. Si el archivo vpnclient.ini se incluye con el software VPN Client cuando se instala por primera vez, VPN Client se configura automáticamente durante la instalación. También puede distribuir los archivos de perfil (un archivo .pcf para cada entrada de conexión) como perfiles de conexión preconfigurados para la configuración automática. Para distribuir a los usuarios copias preconfiguradas de instalación del software VPN Client, siga estos pasos:

1. Copie los archivos del software VPN Client del CD-ROM de distribución en cada directorio en el que creó un archivo vpnclient.ini (global) y perfiles de conexión independientes para un conjunto de usuarios.**Nota:** Para la plataforma Mac OS X, los archivos preconfigurados se colocan en las carpetas Profiles and Resources antes de que se instale VPN Client. El archivo vpnclient.ini se coloca en el directorio del instalador. Debe poner los archivos vpnclient.ini personalizados en el directorio del instalador de VPN Client en el mismo nivel que las carpetas Profiles y Resources. Consulte el capítulo 2 de la Guía del Usuario de VPN Client para Mac OS X para obtener más información
2. Prepare y distribuya el software incluido. CD-ROM o distribución de red. Asegúrese de que el archivo vpnclient.ini y los archivos de perfil están en el mismo directorio que todos los archivos de imagen del CD-ROM. Puede dejar que los usuarios instalen desde este directorio a través de una conexión de red; o puede copiar todos los archivos en un nuevo CD-ROM para su distribución; o puede crear un archivo zip autoextraíble que contenga todos los archivos de este directorio, y dejar que los usuarios lo descarguen e instalen después el software.
3. Proporcione a los usuarios cualquier otra información e instrucciones de configuración necesarias. Consulte el Capítulo 2 de la Guía del Usuario de VPN Client de su plataforma.

P. Parece que Cisco VPN Client tiene un conflicto con mi tarjeta NIC. ¿Cómo puedo

solucionar este problema?

A. Asegúrese de ejecutar los últimosdrivers en la tarjeta NIC. Esto se recomienda siempre. Si es posible, pruebe si el problema es específico al sistema operativo, hardware de la PC, y a otras tarjetas NIC.

P. ¿Cómo automatizo la conexión de Cisco VPN Client a partir del networking de marcación manual?

A. Elija **Options > Properties > Connections**, y haga que Cisco VPN Client despliegue una entrada de la agenda telefónica de networking de marcación manual para automatizar totalmente la marcación manual en la conexión VPN.

P. ¿Cómo configuro el Concentrador Cisco VPN 3000 para notificar a los usuarios remotos la actualización del cliente VPN?

A. Puede notificar a los usuarios de VPN Client cuándo es el momento de actualizar el software VPN Client en sus sistemas remotos. Consulte Notificación a los Usuarios Remotos de una Actualización del Cliente para un método paso a paso. Asegúrese de que escribe la información sobre la versión como "(Rel)", como se indica en el paso 7 del proceso.

P. ¿Qué puede causar una demora antes de que aparezca Cisco VPN Client, particularmente cuando la opción "Start Before Logon" está habilitada?

A. Cisco VPN Client está en el *modo de repliegue.* Esto provoca un retraso. En el modo de repliegue, VPN Client funciona de forma diferente cuando se abre antes de que se haya iniciado una sesión. Cuando funciona en el modo de repliegue, VPN Client no verifica si se han iniciado los servicios de Windows necesarios. Como resultado, la conexión VPN podría fallar si se inicia demasiado rápido.Desinstale Cisco VPN Client y elimine las aplicaciones infractoras para permitir el inicio sin estar en el modo "de retorno". A continuación reinstale Cisco VPN Client. Para obtener más información sobre el modo de repliegue, consulte Inicio antes del Inicio de Sesión.

Consulte Cisco bug IDs CSCdt88922 (sólo clientes registrados) y CSCdt55739 (sólo clientes registrados) en Bug Toolkit para obtener más información.

P. Necesito comprender la diferencia entre ipsecdialer.exe y vpngui.exe. ¿Por qué vpngui.exe se instala en la INICIALIZACIÓN en mi Windows XP, pero todavía debo iniciar manualmente ipsecdialer para alcanzar los recursos de mis compañías? Y (aparte del tamaño) estos programas parecen accionar lo mismo: un inicio de sesión VPN a la red de mi compañía.

A. El archivo ipsecdialer.exe era el mecanismo de inicio original de Cisco VPN Client versión 3.x. Cuando se modificó la GUI en las versiones 4.x, se creó un nuevo archivo ejecutable llamado vpngui.exe. Se transfirió el archivo ipsecdialer.exe (el nombre) sólo para la compatibilidad descendente y sólo lanza el vpngui.exe. Es por ello que puede ver la diferencia en el tamaño del archivo.

Así que si retrocede de la versión 4.x a la versión 3.x de Cisco VPN Client, necesita el archivo ipsecdialer.exe para iniciar esto.

P. ¿Puedo quitar con seguridad el icono de inicialización VPN? ¿Por qué se necesita?

A. Cisco VPN Client en la carpeta de inicialización soporta la función "Start Before Logon". Si no utiliza la función, no la necesita en la carpeta de inicialización.

P. ¿Por qué se agrega “user_logon” y no en el acceso directo ipsecdialer.exe? ¿Cuál es el propósito del “inicio de sesión de usuario”?

A. La función "Start Before Logon" requiere "user_logon", sin embargo, un inicio normal de Cisco VPN Client por parte del usuario no la necesita.

Problemas NAT/PAT

P. Estoy teniendo problemas para que uno de los clientes VPN (para versiones 3.3 y anteriores) se conecte a través de un dispositivo de traducción de dirección de puerto (PAT). ¿Qué puedo hacer para aligerar este problema?

A. Hubo un error de funcionamiento en varias implementaciones de la Traducción de direcciones de red (NAT)/PAT que causaron que los puertos menores a 1024 no se tradujeran. En Cisco VPN Client 3.1, incluso con la Transparencia NAT habilitada, Internet Security Association y la sesión de Key Management Protocol (ISAKMP) usa UDP 512. El primer cliente VPN atraviesa el dispositivo PAT y mantiene el puerto de origen 512 en el exterior. Cuando se conecta el segundo cliente VPN, el puerto 512 ya está funcionando. El intento falla.

Existen tres soluciones alternativas posibles.

- Arregle el dispositivo PAT.
- Actualice los clientes VPN a 3.4 y utilice la encapsulación TCP.
- Instale un VPN 3002 que reemplace a todos los clientes VPN.

P. ¿Se pueden conectar dos equipos portátiles con Cisco VPN Client desde la misma ubicación?

A. Dos clientes pueden conectarse con el mismo centro distribuidor de la misma ubicación siempre que los clientes no se encuentren detrás de un dispositivo que ejecute PAT como un router/firewall SOHO. Muchos dispositivos PAT pueden mapear UNA conexión VPN a un cliente detrás de ella, pero no dos. Para permitir que dos clientes VPN se conecten desde la misma ubicación detrás de un dispositivo PAT, habilite algún tipo de encapsulación como NAT-T, IPSec sobre el UDP, o IPSec sobre el TCP en el centro distribuidor. Generalmente, la NAT-T u otra encapsulación debe estar habilitado si CUALQUIER dispositivo NAT se encuentra entre el cliente y el centro distribuidor.

Miscelánea

P. Cuando me conecto a la red en la oficina utilizando mi computadora portátil y la llevo a mi casa, tengo problemas para conectarme al concentrador VPN 3000 desde allí. ¿Cuál es el problema?

A. El equipo portátil posiblemente conserve información de routing de la conexión LAN. Consulte Clientes VPN con Problemas de Microsoft Routing para obtener información sobre cómo resolver este problema.

P. ¿Cómo se puede determinar si un cliente VPN se encuentra conectado al concentrador VPN?

A. Verifique la clave de registro denominada HKLM\Software\Cisco Systems\VPN Client\TunnelEstablished. Si un túnel es activo, el valor es 1. Si no hay ningún túnel presente, el valor es 0.

P. Tengo problemas con la conexión de NetMeeting entre una PC detrás de un concentrador VPN y un cliente VPN, pero la conexión funciona cuando ejecuto desde la PC a un cliente VPN detrás de un concentrador VPN. ¿Cómo puedo solucionar esto?

A. Siga los pasos correspondientes enumerados a continuación para controlar la configuración de la conexión:

- En la unidad principal de la PC, elija el **Program Files > Cisco Systems > VPN Client > Profiles**. Haga clic con el botón derecho en el perfil que utilice y elija **Open With para abrir el perfil en un editor de textos (por ejemplo Notepad).** (Cuando elige el programa que desea utilizar, asegúrese de desmarcar el cuadro que dice **Utilizar siempre este programa para abrir estos archivos**.) Localice el parámetro del perfil de ForcekeepAlives y cambie el valor de 0 a **1**, a continuación guarde el perfil.or
- Para el cliente VPN, elija **Options > Properties > General** e ingrese un valor para "Peer response timeout", como se muestra en esta ventana de ejemplo. Puede especificar una sensibilidad de tiempo de espera de 30 a 480 segundos.or
- Para el VPN Concentrator, elija **Configuration > User Management > Groups > modify group.** En la pestaña IPsec, elija la opción de Keepalives IKE, como se muestra en esta ventana de ejemplo.

El intervalo del Detección de Peer Inactivo (DPD) varía según la configuración de sensibilidad. Si no se recibe la respuesta, se traslada a un modo más agresivo, y envía los paquetes cada cinco segundos hasta que se alcanza el umbral de respuesta de par. En ese momento, la conexión se desactiva. Usted puede inhabilitar las keepalives, pero si su conexión cae realmente, debe esperar el tiempo de espera inactivo. Cisco recomienda que establezca un valor de sensibilidad inicial muy bajo.

P. ¿Cisco VPN Client soporta la autenticación doble?

A. No. La autenticación doble no se soporta en Cisco VPN Client.

P. ¿Cómo puedo configurar Cisco VPN Client para conectar en el modo principal, en vez del modo agresivo?

A. Debe utilizar firmas digitales (certificados) para permitir que Cisco VPN Client se conecte en el modo principal. Hay 2 métodos para lograr esto:

1. Obtenga los certificados de CA del proveedor de certificados de terceros (por ejemplo, Verisign o Entrust) en el router y todos los Cisco VPN Clients. Suscriba los certificados de identidad del mismo servidor de CA y utilice firmas digitales como una manera de autenticar entre Cisco VPN Client y el router. Para obtener más información sobre esta configuración, consulte Configuración de IPSec entre Routers Cisco IOS y Cisco VPN Client mediante Certificados Entrust.
2. La segunda opción es configurar el router como el servidor de CA junto con el centro distribuidor al VPN de acceso remoto. La instalación de los certificados (y todo lo demás) permanecerá según se describe en el link anterior, salvo que el router se comportará como un servidor de CA. Para obtener más información, consulte VPN de LAN a LAN Dinámico entre Routers Cisco IOS Usando CA de IOS en el Ejemplo de Configuración del Hub.

P. ¿Cómo convierto los parámetros necesarios en solo lectura en el archivo de acceso del cliente VPN?

A. Agregue un signo de exclamación (!) en frente de cada parámetro en el archivo .pcf para cada usuario a fin de convertir el parámetro en solo lectura.

Los valores de los parámetros que comienzan con un signo de exclamación (!) no los puede cambiar el usuario en el cliente VPN. Los campos de estos valores dentro de la GUI se atenuarán (solo lectura).

A continuación se incluye una configuración de ejemplo:

Archivo .pcf original

```
[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
```

Archivo .pcf cambiado

```
[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
```

En este ejemplo, el usuario no puede cambiar los valores de *Description*, *Host*, *GroupName* y *Username.*

P. ¿Es posible limitar/restringir el acceso de los clientes VPN según las direcciones MAC?

A. No. No es posible limitar/restringir el acceso de los clientes VPN según las direcciones MAC.

Información Relacionada

- Página de soporte del VPN 3000 Client de Cisco
- Página de soporte para cliente Cisco VPN
- Soluciones a los Problemas más frecuentes de IPSec VPN L2L y de Acceso Remoto
- Soporte Técnico y Documentación - Cisco Systems