

Guía de solución de problemas de AnyConnect VPN Client: problemas comunes

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Proceso de Troubleshooting](#)

[Problemas de la Instalación y del Adaptador Virtual](#)

[Desconexión o Imposibilidad de Establecer la Conexión Inicial](#)

[Problemas con el Paso del Tráfico](#)

[Problemas por Crash de AnyConnect](#)

[Problemas con la Fragmentación o el Paso del Tráfico](#)

[Desinstalación Automática](#)

[Problema para completar el FQDN del clúster](#)

[Configuración de la lista de servidores de respaldo](#)

[AnyConnect: Problema en la Base de Datos del Driver Dañado](#)

[Reparación](#)

[Error en la reparación](#)

[Analizar la Base de Datos](#)

[Mensajes de error](#)

[Error: Unable to Update the Session Management Database](#)

[Solución 1](#)

[Solución 2](#)

[Error: "Module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register" \(No se pudo registrar el módulo c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll\)](#)

[Solución](#)

[Error: "An error was received from the secure gateway in response to the VPN negotiation request. Please contact your network administrator" \(El gateway seguro arrojó un error como respuesta a la solicitud de negociación de la VPN. Comuníquese con su administrador de redes\)](#)

[Solución](#)

[Error: Session could not be established. Session limit of 2 reached.](#)

[Solución 1](#)

[Solución 2](#)

[Error: AnyConnect no está habilitado en el servidor VPN al intentar conectar AnyConnect a ASA](#)

[Solución](#)

[Error:- %ASA-6-722036: IP x.x.x.x del xxxx del usuario del cliente-grupo del grupo que transmite el paquete grande 1220 \(umbral 1206\)](#)

[Solución](#)

[Error: El gateway seguro ha rechazado la solicitud de conexión o reconexión de VPN del agente.](#)

[Solución](#)

[Error: "Unable to update the session management database"](#)

Solución

Error: "The VPN client driver has encountered an error" (Error en el controlador del cliente VPN)

Solución

Error: "Unable to process response from xxx.xxx.xxx.xxx"

Solución

Error: "Login Denied , unauthorized connection mechanism , contact your administrator"

Solución

Error: "Anyconnect package unavailable or corrupted. Contact your system administrator" (Paquete de Anyconnect no disponible o dañado. Comuníquese con su administrador del sistema)

Solución

Error: "The AnyConnect package on the secure gateway could not be located"

Solución

Error: "Secure VPN via remote desktop is not supported"

Solución

Error: "The server certificate received or its chain does not comply with FIPS. A VPN connection will not be established"

Solución

Error: "Certificate Validation Failure"

Solución

Error: "VPN Agent Service has encountered a problem and needs to close. We are sorry for the inconvenience" (Ocurrió un error en el servicio del agente VPN y debe cerrarse. Lamentamos las molestias ocasionadas)

Solución

Error: "This installation package could not be opened. Verify that the package exists"

Solución

Error: "Error applying transforms. Verify that the specified transform paths are valid." (Error al aplicar transformaciones. Compruebe que las rutas de transformación especificadas son válidas).

Solución

Error: "The VPN client driver has encountered an error" (Error en el controlador del cliente VPN)

Solución

Error: "A VPN reconnect resulted in different configuration setting. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restored." (Una reconexión a la VPN provocó una configuración diferente. La configuración de la red VPN se está reiniciando. Es posible que deba restaurar las aplicaciones que usan la red privada)

Solución

Error al iniciar sesión con AnyConnect

Solución

La configuración del proxy de Internet Explorer no se restaura una vez que AnyConnect se desconecta en Windows 7

Solución

Error: AnyConnect Essentials cannot be enabled until all these sessions are closed. (AnyConnect Essentials no puede habilitarse hasta que se cierren todas estas sesiones)

Solución

Error: La ficha de conexión en la opción de Internet de Internet Explorer se oculta después de conectarse al cliente AnyConnect.

Solución

Error: Algunos usuarios reciben un mensaje de error de inicio de sesión, mientras que otros

[pueden conectarse correctamente mediante AnyConnect VPN](#)

[Solución](#)

[Error: The certificate you are viewing does not match with the name of the site you are trying to view. \(El certificado que está viendo no coincide con el nombre del sitio que intenta visualizar\)](#)

[Solución](#)

[No es posible iniciar AnyConnect desde CSD Vault en una máquina con Windows 7](#)

[Solución](#)

[El perfil de AnyConnect no se replica en reserva después de la conmutación por falla](#)

[Solución](#)

[El cliente de AnyConnect se bloquea si Internet Explorer se desconecta](#)

[Solución](#)

[Mensaje de error: TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER](#)

[Solución](#)

[Mensaje de error: "Connection attempt has failed due to invalid host entry"](#)

[Solución](#)

[Error: "Ensure your server certificates can pass strict mode if you configure always-on VPN"](#)

[Solución](#)

[Error: "Se ha producido un error interno en los servicios HTTP de Microsoft Windows"](#)

[Solución](#)

[Error: "El transporte SSL recibió una falla de Secure Channel. Puede ser el resultado de una configuración criptográfica no admitida en el gateway seguro".](#)

[Solución](#)

[Información Relacionada](#)

Introducción

Este documento describe un escenario de solución de problemas que se aplica a las aplicaciones que no funcionan con Cisco AnyConnect VPN Client.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento tiene como base un dispositivo Cisco Adaptive Security Appliance (ASA) que ejecuta la versión 8.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Proceso de Troubleshooting

Windows Vista:

```
\Users\
```

Si se trata de una actualización automática, este log se encuentra en el directorio temporal del sistema:

```
\Windows\Temp
```

El nombre del archivo está en este formato: **anyconnect-win-x.x.xxxx-k9-install-
yyyyyyyyyyyyyyyy.log**. Obtenga el archivo más reciente para la versión del cliente que desee instalar. Los cambios x.xxxx basados en la versión, como 2.0.0343, y yyyyyyyyyyyyyyy incluyen la fecha y hora de la instalación.

3. Obtenga el archivo de información del sistema de la PC:

Desde el Indicador del Comando/cuadro DOS, escriba lo siguiente:

Windows XP/Windows 2000:

```
winmsd /nfo c:\msinfo.nfo
```

Windows Vista:

```
msinfo32 /nfo c:\msinfo.nfo
```

Nota: Después de escribir, espere. El archivo puede tardar entre dos y cinco minutos en completarse.

Obtenga un vaciado del archivo systeminfo de un Indicador de Comando:

Windows XP y Windows Vista:

```
systeminfo c:\sysinfo.txt
```

Consulte [AnyConnect: Problema en la Base de Datos del Driver Dañado para ejecutar un debug del problema del driver.](#)

Desconexión o Imposibilidad de Establecer la Conexión Inicial

Si experimenta problemas de conexión con el cliente AnyConnect, como desconexiones o la incapacidad para establecer una conexión inicial, obtenga estos archivos:

- El archivo de configuración de ASA para determinar si hay algo en la configuración que provoque la falla de conexión:

Desde la consola del ASA, escriba `write net x.x.x.x:ASA-Config.txt` donde `x.x.x.x` es la dirección IP de un servidor TFTP en la red.

O

Desde la consola de ASA, escriba `show running-config`. Deje que la configuración se complete en la pantalla; luego, corte y pegue el texto en un editor de texto para guardarlo.

- Los logs de eventos ASA:

Para habilitar el registro en ASA para eventos de autenticación, WebVPN, Secure Sockets Layer (SSL) y cliente SSL VPN (SVC), emita estos comandos de CLI:

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class svc console debugging
```

Origine una sesión de AnyConnect y asegúrese de poder reproducir el error. Capture la salida del registro de la consola en un editor de texto y guárdelo.

Para inhabilitar el registro, ejecute `no logging enable`.

- El log de Cisco AnyConnect VPN Client de Windows Event Viewer en el equipo cliente:

Elija **Start > Run**.

Escriba:

`eventvwr.msc /s`

Haga clic derecho en el registro de **Cisco AnyConnect VPN Client** y seleccione **Save Log File as AnyConnect.evt (Guardar archivo de registro como AnyConnect.evt)**.

Nota: Siempre guarde el archivo con el **formato de archivo .evt**.

Si el usuario no puede conectarse con AnyConnect VPN Client, es posible que el problema se relacione con una sesión de protocolo de escritorio remoto (RDP) ya establecida o con el cambio rápido de usuario habilitado en la computadora cliente. El usuario puede ver que las configuraciones del perfil de AnyConnect requieren un solo usuario local, pero varios usuarios locales actualmente tienen una sesión iniciada en su equipo. **No se establecerá la conexión VPN; aparece un mensaje de error en el equipo cliente.** Para resolver este problema, desconecte cualquier sesión establecida de RDP y deshabilite el cambio rápido de usuario. Este comportamiento es controlado por el atributo [Aplicación de inicio de sesión de Windows](#) en el perfil del cliente; sin embargo, actualmente no hay ninguna configuración que permita a un usuario establecer una conexión VPN mientras varios usuarios están conectados simultáneamente en la misma máquina. Solicitud de mejora [CSCsx15061](#) no se pudo abordar esta función.

Nota: Asegúrese de que el puerto 443 no esté bloqueado para que el cliente AnyConnect pueda conectarse con ASA.

Cuando un usuario no puede conectar AnyConnect VPN Client con ASA, el problema puede deberse a una incompatibilidad entre la versión del cliente AnyConnect y la versión de la imagen de software de ASA. En este caso, el usuario recibe este mensaje de error: **El instalador no pudo iniciar el cliente VPN Cisco y el acceso sin cliente no está disponible.**

Para resolver este problema, actualice la versión del cliente AnyConnect para que sea compatible con la imagen de software de ASA.

Cuando inicia sesión por primera vez en AnyConnect, el script de inicio de sesión no funciona. Si se desconecta y vuelve a iniciar sesión, el script de inicio de sesión se ejecuta correctamente. Ésta es la conducta esperada.

Cuando conecte el cliente AnyConnect VPN Client con ASA, es posible que aparezca este error: **User not authorized for AnyConnect Client access, contact your administrator** (Usuario no autorizado a acceder al cliente AnyConnect. Comuníquese con su administrador).

Este error aparece cuando la imagen de AnyConnect no está en ASA. Una vez que se carga la imagen en ASA, AnyConnect puede conectarse sin problemas a ASA.

Este error se puede resolver deshabilitando la seguridad de la capa de transporte de datagramas (DTLS). Vaya a **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles (Configuración > Acceso remoto a la VPN > Acceso a la red [cliente] > Perfiles de conexión de AnyConnect)** y desmarque la casilla de verificación **Enable DTLS (Permitir**

DTLS). Esto deshabilita la DTLS.

Este mensaje de error aparece en los archivos del paquete de la herramienta Diagnostic AnyConnect Reporting Tool (DART) cuando el usuario queda desconectado:

TUNNELPROTOCOLDPDMGR_ERROR_NO_DPD_RESPONSE:El gateway seguro no pudo responder a los paquetes de Detección de Peer Muerto. Este error significa que el canal de DTLS se vio afectado debido al error de detección de par muerto (DPD). Este error se resuelve si ajusta los keepalive de DPD y emite estos comandos:

```
webvpn
svc keepalive 30
svc dpd-interval client 80
svc dpd-interval gateway 80
```

A partir de la versión 8.4(1) de ASA, los comandos `svc keepalive` y `svc dpd-interval` se sustituyen por los comandos `anyconnect keepalive` y `anyconnect dpd-interval` (respectivamente), como se muestra a continuación:

```
webvpn
anyconnect ssl keepalive 15
anyconnect dpd-interval client 5
anyconnect dpd-interval gateway 5
```

Problemas con el Paso del Tráfico

Cuando se detectan problemas con el paso del tráfico a la red privada en una sesión de AnyConnect mediante ASA, complete estos pasos para recopilar datos:

1. Obtenga la salida del comando de ASA `show vpn-sessiondb detail svc filter name <username>` desde la consola. Si la salida muestra `Filter Name: XXXXX`, recopile el resultado para `show access-list XXXXX`. Verifique que la lista de acceso XXXXX no bloquee el flujo de tráfico deseado.
2. Exporte las estadísticas de AnyConnect desde AnyConnect VPN Client > Statistics > Details > Export (AnyConnect VPN Client > Estadísticas > Detalles > Exportar) (AnyConnect-ExportedStats.txt).
3. Verifique el archivo de configuración ASA para las **sentencias NAT**. Si la traducción de direcciones de red (NAT) está habilitada, estas deben exceptuar los datos que regresan al cliente como resultado de la NAT. Por ejemplo, para que NAT exceptúe (nat 0) las direcciones IP desde el grupo de AnyConnect, use esto en la CLI:

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

4. Determine si el gateway predeterminado tunelado debe habilitarse para la configuración. El gateway predeterminado tradicional es el gateway de último recurso para el tráfico no descifrado.

Ejemplo:

```
!--- Route outside 0 0 is an incorrect statement.
```

```
route outside 0 0 10.145.50.1  
route inside 0 0 10.0.4.2 tunneled
```

Por ejemplo, si el cliente VPN debe tener acceso a un recurso que no está en la tabla de routing del gateway VPN, el routing del paquete se realiza a través del gateway predeterminado estándar. El gateway de VPN no necesita la tabla de ruteo interno completa para resolver este problema. Se puede usar la palabra clave **tunneled en este caso**.

5. Compruebe si la política de inspección de ASA descarta el tráfico de AnyConnect. Puede exceptuar la aplicación específica que el cliente AnyConnect utiliza si implementa el marco de trabajo de política modular de Cisco ASA. Por ejemplo, podría eximir el protocolo delgado con estos comandos.

```
ASA(config)# policy-map global_policy  
ASA(config-pmap)# class inspection_default  
ASA(config-pmap-c)# no inspect skinny
```

Problemas por Crash de AnyConnect

Complete estos pasos para recopilar datos:

1. Asegúrese de que esté habilitada la Utilidad de Microsoft Dr. Watson. Para hacerlo, seleccione Start > Run, y ejecute **Drwtsn32.exe**. Configure esto y haga clic en OK:

```
Number of Instructions      : 25  
Number of Errors To Save  : 25  
Crash Dump Type           : Mini  
Dump Symbol Table         : Checked  
Dump All Thread Contexts  : Checked  
Append To Existing Log File : Checked  
Visual Notification       : Checked  
Create Crash Dump File    : Checked
```

Cuando se produzca el crash, recopile los archivos .log y .dmp de **C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson**. Si estos archivos se están usando, utilice **ntbackup.exe**.

2. Obtenga el log del Cisco AnyConnect VPN Client del Visor de Eventos de Windows en el equipo cliente:

Elija **Start > Run**.

Escriba:

```
eventvwr.msc /s
```

Haga clic derecho en el registro de Cisco AnyConnect VPN Client y seleccione **Save Log File as AnyConnect.evt** (Guardar archivo de registro como AnyConnect.evt).

Nota: Siempre guarde el archivo con el formato de archivo **.evt**.

Problemas con la Fragmentación o el Paso del Tráfico

Algunas aplicaciones, como Microsoft Outlook, no funcionan. Sin embargo, el túnel deja pasar otro tráfico, como pequeños pings.

Esto puede proporcionar pistas en cuanto a un problema de fragmentación en la red. El rendimiento de los routers del consumidor es particularmente deficiente en cuanto a la fragmentación de paquetes y el re ensamblado.

Pruebe con un conjunto de pings de tamaño creciente para determinar si el error ocurre con un determinado tamaño. Por ejemplo, ping -l 500, ping -l 1000, ping -l 1500, ping -l 2000.

Se recomienda que configure un grupo especial para los usuarios que experimentan fragmentación y que defina la unidad máxima de transmisión (MTU) de SVC para este grupo en 1200. Esto le permite brindar una solución a los usuarios que experimentan este problema sin afectar la base de usuarios más amplia.

Problema

Las conexiones TCP dejan de responder después de conectarse con AnyConnect.

Solución

Para comprobar si el usuario tiene un problema de fragmentación, ajuste la MTU para clientes AnyConnect en ASA.

```
ASA(config)#group-policy <name> attributes
webvpn
svc mtu 1200
```

Desinstalación Automática

Problema

AnyConnect VPN Client se desinstala una vez que termina la conexión. Los logs del cliente muestran que la opción mantener instalado está inhabilitada.

Solución

AnyConnect se desinstala a pesar de que está seleccionada la opción **keep installed** (mantener

instalado) en Adaptive Security Device Manager (ASDM). Para resolver este problema, configure el comando `svc keep-installer installed` debajo de la política de grupo.

Problema para completar el FQDN del clúster

Problema: El cliente de AnyConnect se completa previamente con el nombre del host en lugar del nombre de dominio totalmente calificado (FQDN) del clúster.

Si tiene un clúster de equilibrio de carga configurado para SSL VPN y el cliente intenta conectarse al clúster, la solicitud se redirige a ASA en el nodo y el cliente inicia sesión correctamente. Después de algún tiempo, cuando el cliente intenta conectarse de nuevo al clúster, el FQDN del clúster no aparece en las entradas de **Connect to (Conectar a)**. En cambio, se ve la entrada de ASA en el nodo a la que se redirigió al cliente.

Solución

Esto ocurre porque el cliente de AnyConnect conserva el nombre del host al que se conectó por última vez. Se ha observado este comportamiento y se ha registrado el error. Para obtener información completa sobre el error, consulte la identificación de error de Cisco [CSCsz39019](#). La solución sugerida es actualizar Cisco AnyConnect a la versión 2.5.

Configuración de la lista de servidores de respaldo

Es necesario configurar una lista de servidores de respaldo en caso de que no sea posible tener acceso al servidor principal seleccionado por el usuario. Esto se define en el panel **Backup Server (Servidor de respaldo)** en el perfil de AnyConnect. Complete estos pasos:

1. Descargue el [editor de perfiles de AnyConnect \(solo para clientes registrados\)](#). El nombre del archivo es `AnyConnectProfileEditor2_4_1.jar`.
2. Cree un archivo XML con el editor de perfiles de AnyConnect.

Vaya a la ficha de la lista de servidores.

Haga clic en Add (Agregar).

Escriba el servidor principal en el campo **Hostname (Nombre del host)**.

Agregue el servidor de respaldo debajo de la lista de servidores de respaldo, en el campo **Host address (Dirección del host)**. Luego, haga clic en Add (Agregar).

3. Una vez que tenga el archivo XML, deberá asignarlo a la conexión que usa en ASA.

En ASDM, seleccione **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** (Configuración > Acceso remoto a la VPN > Acceso a la red [cliente] > Perfiles de conexión de AnyConnect).

Seleccione su perfil y haga clic en **Edit** (Editar).

Haga clic en **Manage (Administrar)** en la sección **Default Group Policy (Política de grupo predeterminada)**.

Seleccione su política de grupo y haga clic en **Edit (Editar)**.

Seleccione **Advanced (Avanzado)** y haga clic en **SSL VPN Client (Cliente SSL VPN)**.

Haga clic en **New**. Luego, deberá escribir un nombre para el perfil y asignar el archivo XML.

4. Conecte el cliente a la sesión para descargar el archivo XML.

AnyConnect: Problema en la Base de Datos del Driver Dañado

Esta entrada en el archivo SetupAPI.log sugiere que el sistema de catálogo está dañado:

Falta la lista de clase de firma del driver W239 "C:\WINDOWS\INF\certclas.inf" o no es válida.

Error 0xfffffde5: Unknown Error. (Error desconocido), suponiendo que todas las clases de dispositivos están sujetas a la política de firma de controlador.

También puede recibir este mensaje de error: **Error (3/17): Unable to start VA, setup shared queue, or VA gave up shared queue** (No es posible iniciar el adaptador virtual [VA]; hay una cola de configuración compartida o VA abandonó la cola compartida).

Puede recibir este registro en el cliente: **"The VPN client driver has encountered an error"** (Error en el controlador del cliente VPN).

Reparación

Este problema se debe a la identificación de error de Cisco [CSCsm54689](#). Para resolver este problema, asegúrese de que el Routing and Remote Access Service esté inhabilitado antes de iniciar AnyConnect. Si esto no resuelve el problema, siga estos pasos:

1. Abra un indicador de comando como Administrador en el equipo (indicador elevado en Vista).
2. Ejecute net stop CryptSvc.
3. Ejecute:

```
esentutl /p%systemroot%\System32\catroot2\  
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

4. Cuando se le pida, seleccione **OK (Aceptar)** para intentar la reparación.
5. Salga del indicador de comando.
6. Reiniciar.

Error en la reparación

Si la reparación falla, siga estos pasos:

1. Abra un indicador de comando como Administrador en el equipo (indicador elevado en Vista).
2. Ejecute net stop CryptSvc.
3. Cambie el nombre del directorio %WINDIR%\system32\catroot2 to catroot2_old.
4. Salga del indicador de comando.
5. Reiniciar.

Analizar la Base de Datos

Puede analizar la base de datos en cualquier momento para determinar si es válida.

1. Abra un indicador de comando como Administrador en el equipo.
2. Ejecute:

```
esentutl /g%systemroot%\System32\catroot2\  
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

Consulte [Integridad de la Base de Datos del Catálogo del Sistema para obtener más información.](#)

Mensajes de error

Error: Unable to Update the Session Management Database

Cuando la SSL VPN está conectada a través de un navegador web, aparece Unable to Update the Session Management Database como mensaje de error, y los logs de ASA muestran %ASA-3-211001: Memory allocation Error. The adaptive security appliance failed to allocate RAM system memory (Error de asignación de memoria. Adaptive Security Appliance no pudo asignar memoria RAM del sistema).

Solución 1

Este problema se debe a la identificación de error de Cisco [CSCsm51093](#). Para resolver este problema, recargue el ASA o actualice el software ASA a la versión provisoria mencionada en el bug. Consulte Cisco bug ID [CSCsm51093](#) para más información.

Solución 2

Este problema también puede resolverse si deshabilita la detección de amenazas en ASA (en caso de utilizarla).

Error: "Module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register" (No se pudo registrar el módulo c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll)

Cuando utiliza el cliente AnyConnect en computadoras portátiles o de escritorio, se produce un error durante la instalación:

```
"Module C:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register..."
```

Cuando se detecta este error, el instalador no puede avanzar y el cliente se elimina.

Solución

Estas son las posibles soluciones para este error:

- El cliente más reciente de AnyConnect ya no es oficialmente compatible con Microsoft Windows 2000. Es un problema de registro con la computadora que ejecuta Windows 2000.
- Elimine las aplicaciones de VMware. Una vez que se instala AnyConnect, es posible agregar las aplicaciones de VMware nuevamente a la computadora.
- Agregue ASA a los sitios de confianza.
- Copie estos archivos desde la carpeta **\ProgramFiles\Cisco\CiscoAnyconnect** a una carpeta nueva y ejecute **regsvr32 vpnapi.dll** en el símbolo del sistema:

```
vpnapi.dllvpncommon.dllvpncommoncrypt.dll
```

- Cree una nueva imagen del sistema operativo en la computadora portátil o de escritorio.

El mensaje del registro relacionado con este error en el cliente de AnyConnect es similar al siguiente:

```
DEBUG: Error 2911: Could not remove the folderC:\Program Files\Cisco\Cisco AnyConnect VPN Client\.
```

```
The installer has encountered an unexpected error installing this package. This may indicate a problem with this package. The error code is 2911. The arguments are:
```

```
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,
```

```
DEBUG: Error 2911: Could not remove the folder C:\Program Files\Cisco\Cisco AnyConnect VPN Client\.
```

```
The installer has encountered an unexpected error installing this package. This may indicate a problem with this package. The error code is 2911. The arguments are:
```

```
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,
```

```
Info 1721. There is a problem with this Windows Installer package. A program required for this install to complete could not be run. Contact your support personnel or package vendor. Action: InstallHelper.exe, location: C:\Program Files\Cisco\Cisco AnyConnect VPN Client\InstallHelper.exe, command: -acl "C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\\" -r
```

Error: "An error was received from the secure gateway in response to the VPN negotiation request. Please contact your network administrator" (El gateway seguro arrojó un error como respuesta a la solicitud de negociación de la VPN. Comuníquese con su administrador de redes)

Este error aparece cuando los clientes intentan conectarse a la VPN con Cisco AnyConnect VPN Client.

Este mensaje proviene del gateway seguro:

"Illegal address class" (Clase de dirección ilegal), "Host or network is 0" (El host o la red es 0) u "Other error" (Otro error).

Solución

El problema se produce debido al vaciado del grupo local de direcciones IP de ASA. Como se agota el recurso del grupo de la VPN, debe ampliarse el rango del grupo de direcciones IP.

Se registró la identificación de error de Cisco [CSCsl82188 para este problema](#). Este error suele producirse cuando se agota el grupo local para la asignación de direcciones, o si se usa una máscara de subred de 32 bits para el grupo de direcciones. La solución consiste en ampliar el grupo de direcciones y utilizar una máscara de subred de 24 bits para el grupo.

Error: Session could not be established. Session limit of 2 reached.

Al intentar conectar más de dos clientes con AnyConnect VPN Client, recibe el mensaje de error **Login Failed** (Error de inicio de sesión) en el cliente y un mensaje de advertencia en los registros de ASA que dice: **Session could not be established. Session limit of 2 reached**. Tengo la licencia **AnyConnect Essential** en ASA, que ejecuta la versión **8.0.4**.

Solución 1

Este error se produce porque la licencia **AnyConnect Essential** no es compatible con la versión **8.0.4 de ASA**. Necesita actualizar ASA a la versión 8.2.2. Esto resuelve el error.

Nota: Independientemente de la licencia utilizada, si se alcanza el límite de la sesión, el usuario recibirá el mensaje de error **Login failed** (Error al iniciar sesión).

Solución 2

Este error también puede producirse si se utiliza el comando `vpn-sessiondb max-anyconnect-premium-or-essentials-limit session-limit` para definir el límite de sesiones de VPN que se pueden establecer. Si el límite de sesión se define en dos, el usuario no puede establecer más de dos sesiones aun cuando la licencia instalada admita más sesiones. Defina el límite de sesiones con la cantidad necesaria de sesiones de VPN para evitar este mensaje de error.

Error: AnyConnect no está habilitado en el servidor VPN al intentar conectar AnyConnect a ASA

Recibe el mensaje de error `Anyconnect not enabled on VPN server` (Anyconnect no habilitado en el servidor VPN) cuando intenta conectar AnyConnect a ASA.

Solución

Este error se resuelve si habilita AnyConnect en la interfaz externa de ASA con ASDM. Para obtener más información sobre cómo habilitar AnyConnect en la interfaz exterior, consulte [Configuración de VPN SSL sin cliente \(WebVPN\) en el ASA](#).

Error:- %ASA-6-722036: IP x.x.x.x del xxxx del usuario del cliente-grupo del grupo que transmite el paquete grande 1220 (umbral 1206)

El %ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206) (Grupo < client-group > Usuario < xxxx > IP < x.x.x.x> transmitiendo paquete grande 1220 [umbral 1206]) aparece en los registros de ASA. ¿Qué significa este registro y cómo se resuelve?

Solución

Estados de este mensaje del registro que un paquete grande fue enviado al cliente. La fuente del paquete no es consciente del MTU del cliente. Esto puede también ser debido a la compresión de los datos incompresibles. La solución consiste en desactivar la compresión de SVC con el comando [svc compression none](#). Esto resuelve el problema.

Error: El gateway seguro ha rechazado la solicitud de conexión o reconexión de VPN del agente.

Al conectarse al cliente de AnyConnect, recibe este error: "The secure gateway has rejected the agent's vpn connect or reconnect request. A new connection requires re-authentication and must be started manually. Please contact your network administrator if this problem persists. The following message was received from the secure gateway: no assigned address" (El gateway seguro ha rechazado la solicitud de conexión o reconexión de VPN del agente. Una nueva conexión requiere una nueva autenticación y debe iniciarse manualmente. Comuníquese con su administrador de redes si el problema persiste. Se recibió el siguiente mensaje del gateway seguro: no hay una dirección asignada).

También se recibe este error al conectarse al cliente de AnyConnect: "The secure gateway has rejected the connection attempt. A new connection attempt to the same or another secure gateway is needed, which requires re-authentication. Se recibió el siguiente mensaje del gateway seguro: Host o red es 0".

También se recibe este error al conectarse al cliente de AnyConnect: "The secure gateway has rejected the agent's vpn connect or reconnect request. A new connection requires a re-authentication and must be started manually. Please contact the network administrator if the problem persists. The following message was received from the secure gateway: No License" (El gateway seguro ha rechazado la solicitud de conexión o reconexión de VPN del agente. Una nueva conexión requiere una nueva autenticación y debe iniciarse manualmente. Comuníquese con su administrador de redes si el problema persiste. Se recibió el siguiente mensaje del gateway seguro: no hay licencia).

Solución

El router no tenía una configuración de grupo después de volver a cargar. Debe volver a agregar la configuración correspondiente al router.

```
Router#show run | in pool
```

```
ip local pool SSLPOOL 192.168.30.2 192.168.30.254
```

```
svc address-pool SSLPOO
```

El error "The secure gateway has rejected the agent's vpn connect or reconnect request. A new connection requires a re-authentication and must be started manually. Please contact the network administrator if the problem persists. The following message was received from the secure gateway: No License" (El gateway seguro ha rechazado la solicitud de conexión o reconexión de VPN del agente. Una nueva conexión requiere una nueva autenticación y debe iniciarse manualmente. Comuníquese con su administrador de redes si el problema persiste. Se recibió el siguiente mensaje del gateway seguro: no hay licencia) se produce cuando falta la licencia de movilidad de AnyConnect. Una vez instalada la licencia, el problema se resuelve.

Error: "Unable to update the session management database"

Al intentar autenticarse en el portal web, recibe este mensaje de error: "Unable to update the session management database" (No se pudo actualizar la base de datos de administración de sesiones).

Solución

Este problema está relacionado con la asignación de memoria en ASA y aparece principalmente cuando la versión de ASA es 8.2.1. Originalmente, se necesitan 512 MB de RAM para obtener funcionalidad completa.

Actualice la memoria a 512 MB para solucionar este problema de manera permanente.

Como solución temporal, intente liberar memoria siguiendo estos pasos:

1. Deshabilite la detección de amenazas.
2. Deshabilite la compresión de SVC.
3. Vuelva a cargar ASA.

Error: "The VPN client driver has encountered an error" (Error en el controlador del cliente VPN)

Este es un mensaje de error de la máquina cliente al intentar conectarse a AnyConnect.

Solución

Para resolver este error, siga este procedimiento para ajustar manualmente el agente AnyConnect VPN a la opción de interacción:

1. Haga clic derecho en **My Computer > Manage > Services and Applications > Services (Mi**

PC > Administrar > Servicios y aplicaciones > Servicios) y seleccione el agente Cisco AnyConnect VPN.

2. Haga clic derecho en **Properties** (Propiedades), inicie sesión y seleccione **Allow service to interact with the desktop** (Permitir que el servicio interactúe con la computadora).

Esto establece el valor del tipo de registro DWORD en 110 (el valor predeterminado es 010) para HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vpnagent.

Nota: Si se debe utilizar esta opción, se recomienda usar la transformación de **.MST en esta instancia**. Esto se debe a que, si realiza esta configuración manual con estos métodos, será necesario que lo haga después de cada proceso de instalación o actualización. Por este motivo, es necesario identificar la aplicación que causa este problema.

Cuando está habilitado el servicio de routing y acceso remoto (RRAS) en la computadora con Windows, AnyConnect no funciona y arroja el error `The VPN client driver has encountered an error (Error en el controlador del cliente VPN)`. Para resolver este problema, asegúrese de que las opciones de routing y RRAS estén deshabilitadas antes de iniciar AnyConnect. Consulte la identificación de error de Cisco [CSCsm54689 para obtener más información](#).

Error: "Unable to process response from xxx.xxx.xxx.xxx"

Los clientes de AnyConnect no pueden conectarse a Cisco ASA. El error en la ventana de AnyConnect es "Unable to process response from xxx.xxx.xxx.xxx" (No es posible procesar la respuesta desde xxx.xxx.xxx.xxx).

Solución

Para resolver este error, pruebe estas soluciones:

- Elimine WebVPN del ASA y vuelva a habilitarlo.<
- Cambie el número actual de puerto (443) a 444 y vuelva a habilitarlo en 443.

Para obtener más información sobre cómo habilitar WebVPN y cambiar el puerto de WebVPN, consulte esta [solución](#).

Error: "Login Denied , unauthorized connection mechanism , contact your administrator"

Los clientes de AnyConnect no pueden conectarse a Cisco ASA. El error en la ventana de AnyConnect es "Login Denied , unauthorized connection mechanism , contact your administrator" (Se rechazó el inicio de sesión debido a un mecanismo de conexión no autorizado; comuníquese con su administrador).

Solución

Este mensaje de error se produce principalmente debido a problemas de configuración incorrecta

o incompleta. Verifique la configuración y asegúrese de que sea la necesaria para resolver el problema.

<

Error: "Anyconnect package unavailable or corrupted. Contact your system administrator" (Paquete de Anyconnect no disponible o dañado. Comuníquese con su administrador del sistema)

Este error se produce cuando intenta iniciar el software de AnyConnect desde un cliente Macintosh para conectarse a ASA.

Solución

Para resolverlo, siga estos pasos:

1. Cargue el paquete de AnyConnect para Macintosh a la memoria flash de ASA.
2. Modifique la configuración de WebVPN para especificar el paquete de AnyConnect que se utiliza.

```
webvpn
svc image disk0:/anyconnect-macosx-i386-2.3.2016-k9.pkg 2
svc image disk0:/anyconnect-macosx-powerpc-2.3.2016-k9.pkg 3
```

El comando `svc image` se sustituye por el comando `anyconnect image` a partir de la versión de ASA 8.4(1), como se detalla a continuación:

```
hostname(config)#webvpn

hostname(config-webvpn)#anyconnect image disk0:/
anyconnect-win-3.0.0527-k9.pkg 1

hostname(config-webvpn)#anyconnect image disk0:/
anyconnect-macosx-i386-3.0.0414-k9.pkg 2
```

Error: "The AnyConnect package on the secure gateway could not be located"

Este error ocurre en la máquina Linux del usuario cuando intenta conectarse a ASA iniciando AnyConnect. A continuación, el mensaje de error completo:

```
"The AnyConnect package on the secure gateway could not be located. You may
be experiencing network connectivity issues. Please try connecting again."
```

Solución

Para resolver este mensaje de error, compruebe que el cliente de AnyConnect sea compatible con el sistema operativo (SO) que se utiliza en la máquina cliente.

Si es compatible con el SO, compruebe si el paquete de AnyConnect se especifica en la configuración de WebVPN o no. Consulte la sección [Paquete de Anyconnect no disponible o dañado de este documento para obtener más información.](#)

Error: "Secure VPN via remote desktop is not supported"

Los usuarios no pueden ejecutar un acceso para escritorio remoto. Aparece el mensaje de error `Secure VPN via remote desktop is not supported (No se admite la VPN segura mediante escritorio remoto)`.

Solución

Este problema se debe a estas identificaciones de error de Cisco: [CSCsu22088](#) y [CSCso42825](#). Si actualiza AnyConnect VPN Client, puede resolver el problema. Consulte estos errores para obtener más información.

Error: "The server certificate received or its chain does not comply with FIPS. A VPN connection will not be established"

Al intentar realizar una conexión VPN a ASA 5505, aparece el mensaje de error `The server certificate received or its chain does not comply with FIPS. A VPN connection will not be established (El certificado de servidor recibido o su cadena no cumplen con los FIPS. No se establecerá una conexión VPN)`.

Solución

Para resolver este error, debe deshabilitar los Estándares federales de procesamiento de la información de los Estados Unidos (FIPS) en el archivo **AnyConnect Local Policy**. Este archivo suele encontrarse en `C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\AnyConnectLocalPolicy.xml`. Si este archivo no se encuentra en esta ruta, busque el archivo en un directorio diferente con una ruta COMO `C:\Documents and Settings\All Users\Application Data\Cisco AnyConnectVPNClient\AnyConnectLocalPolicy.xml`. Una vez que encuentre el archivo xml, realice los cambios que figuran a continuación:

Cambie la frase:

```
<FipsMode>true</FipsMode>
```

A:

```
<FipsMode>>false</FipsMode>
```

Luego, reinicie la computadora. Los usuarios deben tener permisos de administrador para modificar este archivo.

Error: "Certificate Validation Failure"

Los usuarios no pueden iniciar AnyConnect y reciben el mensaje `certificate Validation Failure (Error al validar el certificado)`.

Solución

La autenticación de certificados funciona de manera distinta en AnyConnect y en el cliente IPsec. Para que la autenticación de certificados funcione, debe importar el certificado del cliente a su navegador y cambiar el perfil de conexión para que utilice la autenticación de certificados. También es necesario habilitar este comando en ASA para permitir que se utilicen los certificados de cliente SSL en la interfaz externa:

```
ssl certificate-authentication interface outside port 443
```

Error: "VPN Agent Service has encountered a problem and needs to close. We are sorry for the inconvenience" (Ocurrió un error en el servicio del agente VPN y debe cerrarse. Lamentamos las molestias ocasionadas)

Cuando se instala la versión 2.4.0202 de AnyConnect en una computadora con Windows XP, el proceso se detiene al actualizar los archivos de localización y aparece un mensaje de error que indica una falla en el archivo `vpnagent.exe`.

Solución

Este comportamiento está registrado con la identificación de error de Cisco [CSCsq49102](#). La solución sugerida es deshabilitar el cliente Citrix.

Error: "This installation package could not be opened. Verify that the package exists"

Al descargar AnyConnect, aparece este mensaje de error:

"Contact your system administrator. The installer failed with the following error: This installation package could not be opened. Verify that the package exists and that you can access it, or contact the application vendor to verify that this is a valid Windows Installer package." (Comuníquese con su administrador del sistema. No se pudo ejecutar el instalador debido al siguiente error: Este paquete de instalación no se pudo abrir. Verifique si el paquete existe y si puede tener acceso a él, o comuníquese con el proveedor de la aplicación para comprobar que se trata de un paquete válido del programa de instalación de Windows).

Solución

Complete estos pasos para solucionar este problema:

1. Elimine cualquier software antivirus.
2. Deshabilite el firewall de Windows.
3. Si el paso 1 o el 2 no resuelven el problema, formatee la máquina y realice la instalación.
4. Si el problema persiste, abra un [caso de TAC](#).

Error: "Error applying transforms. Verify that the specified transform paths are valid." (Error al aplicar transformaciones. Compruebe que las rutas de transformación especificadas son válidas).

Se recibe este mensaje de error durante la descarga automática de AnyConnect desde ASA:

**"Contact your system administrator. The installer failed with the following error:
Error applying transforms. Verify that the specified transform paths are valid."**

Este es el mensaje de error recibido cuando se conecta a AnyConnect para MacOS:

"The AnyConnect package on the secure gateway could not be located. You may be experiencing network connectivity issues. Please try connecting again."

Solución

Siga alguna de estas soluciones para resolver el problema:

1. La causa raíz de este error podría deberse a un archivo de traducción de MST dañado (por ejemplo, importado). Siga estos pasos para resolverlo:

Elimine la tabla de traducción de MST.

Configure la imagen de AnyConnect para MacOS en ASA.

2. Desde ASDM, siga la ruta **Network (Client) Access > AnyConnect Custom > Installs (Acceso a la red [cliente] > Personalizar AnyConnect > Instalaciones)** y elimine el archivo del paquete de AnyConnect. Asegúrese de que el paquete permanezca en **Network (Client) Access > Advanced > SSL VPN > Client Setting (Acceso a la red [cliente] > Avanzado > VPN con SSL > Configuración de cliente)**.

Si ninguna de estas soluciones resuelve el problema, comuníquese con el [soporte técnico de Cisco](#).

Error: "The VPN client driver has encountered an error" (Error en el controlador del cliente VPN)

Se recibe este error:

The VPN client driver has encountered an error when connecting through Cisco AnyConnect Client.

Solución

Este problema puede resolverse desinstalando el cliente AnyConnect y, luego, eliminando el software antivirus. Después de esto, vuelva a instalar el cliente AnyConnect. Si esta solución no funciona, vuelva a formatear la computadora para arreglar el problema.

Error: "A VPN reconnect resulted in different configuration setting. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restored." (Una reconexión a la VPN provocó una configuración diferente. La configuración de la red VPN se está reiniciando. Es posible que deba restaurar las aplicaciones que usan la red privada)

Este error aparece al intentar iniciar AnyConnect:

"A VPN reconnect resulted in different configuration setting. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restarted."

Solución

Para resolver este error, utilice lo siguiente:

```
group-policy <Name> attributes
webvpn
svc mtu 1200
```

El comando **svc mtu** se sustituye por el comando **anyconnect mtu** a partir de la versión de ASA 8.4(1), como se detalla a continuación:

```
hostname (config) #group-policy
```

```
hostname (config-group-policy) #webvpn
```

```
hostname (config-group-webvpn) #anyconnect mtu 500
```

Error al iniciar sesión con AnyConnect

Problema

AnyConnect recibe este error cuando se conecta al cliente:

The VPN connection is not allowed via a local proxy. This can be changed through AnyConnect profile settings.

Solución

El problema puede resolverse si realiza estos cambios en el perfil de AnyConnect:

Agregue esta línea al perfil de AnyConnect:

```
<ProxySettings>IgnoreProxy</ProxySettings><
AllowLocalProxyConnections>
false</AllowLocalProxyConnections>
```

La configuración del proxy de Internet Explorer no se restaura una vez que AnyConnect se desconecta en Windows 7

Problema

En Windows 7, si se configura el proxy de Internet Explorer para Detectar la configuración automáticamente y AnyConnect impone una nueva configuración de proxy, no se restaura el

proxy de Internet Explorer al valor Detectar la configuración automáticamente después de que el usuario termina la sesión de AnyConnect. Esto provoca problemas de la red LAN para usuarios que necesitan que su proxy para esté configurado como Detectar la configuración automáticamente.

Solución

Este comportamiento está registrado con la identificación de error de Cisco [CSCtj51376](#). La solución sugerida es actualizar a [AnyConnect 3.0](#).

Error: AnyConnect Essentials cannot be enabled until all these sessions are closed. (AnyConnect Essentials no puede habilitarse hasta que se cierren todas estas sesiones)

Este mensaje de error aparece en Cisco ASDM cuando intenta habilitar la licencia de AnyConnect Essentials:

```
There are currently 2 clientless SSL VPN sessions in progress. AnyConnect Essentials can not be enabled until all these sessions are closed.
```

Solución

Este es el comportamiento normal de ASA. AnyConnect Essentials es un cliente SSL VPN que tiene una licencia independiente. Se configura completamente en ASA y proporciona toda la funcionalidad de AnyConnect, salvo lo siguiente:

- Cisco Secure Desktop no está disponible (CSD) (esto incluye HostScan/Vault/Cache Cleaner)
- SSL VPN sin cliente no está disponible
- Compatibilidad opcional con Windows Mobile

Esta licencia no puede utilizarse al mismo tiempo que la licencia prémium compartida de SSL VPN. Cuando necesite usar una licencia, deberá deshabilitar la otra.

Error: La ficha de conexión en la opción de Internet de Internet Explorer se oculta después de conectarse al cliente AnyConnect.

La ficha de conexión en la opción de Internet de Internet Explorer se oculta después de conectarse al cliente AnyConnect.

Solución

Esto se debe a la función msie-proxy lockdown. Si la habilita, oculta la ficha de conexiones en Microsoft Internet Explorer durante la sesión de AnyConnect VPN. Si la deshabilita, no se modifica la ficha de conexiones en la pantalla.

Error: Algunos usuarios reciben un mensaje de error de inicio de sesión, mientras que otros pueden conectarse correctamente mediante AnyConnect VPN

Algunos usuarios reciben el mensaje de error de inicio de sesión, mientras que otros pueden conectarse correctamente mediante AnyConnect VPN.

Solución

Este problema puede resolverse si se asegura de que la casilla de verificación **do not require pre-authentication (no exigir preautenticación)** esté marcada para los usuarios.

Error: The certificate you are viewing does not match with the name of the site you are trying to view. (El certificado que está viendo no coincide con el nombre del sitio que intenta visualizar)

Durante la actualización del perfil de AnyConnect, aparece un error que indica que el certificado no es válido. Esto ocurre solo en Windows y en la fase de actualización del perfil. A continuación, se muestra el mensaje de error:

```
The certificate you are viewing does not match with the name of the site
you are trying to view.
```

Solución

Esto puede resolverse si se modifica la lista de servidores del perfil de AnyConnect para utilizar el FQDN del certificado.

Este es un ejemplo del perfil XML:

```
<ServerList>
<HostEntry>
<HostName>vpn1.ccsd.net</HostName>
</HostEntry>
</ServerList>
```

Nota: Si hay una entrada existente para la dirección IP pública del servidor, como `<HostAddress>`, elimínela y conserve únicamente el FQDN del servidor (por ejemplo, `<HostName>`, pero no `<Host Address>`).

No es posible iniciar AnyConnect desde CSD Vault en una máquina con Windows 7

Cuando se inicia AnyConnect desde CSD Vault, no funciona. Esto ocurre en máquinas con Windows 7.

Solución

En la actualidad, esto no es posible porque no es compatible.

El perfil de AnyConnect no se replica en reserva después de la conmutación por

falla

El cliente AnyConnect 3.0 VPN con la versión 8.4.1 de ASA funciona bien. Sin embargo, después de la conmutación por falla, no se replica la configuración relacionada con el perfil de AnyConnect.

Solución

Este problema se observó y registró con la identificación de error de Cisco [CSCtn71662](#). La solución temporal consiste en copiar manualmente los archivos a la unidad en reserva.

El cliente de AnyConnect se bloquea si Internet Explorer se desconecta

Cuando esto ocurre, el registro de eventos de AnyConnect contiene entradas similares a estas:

```
Description : Function:
CAdapterNetworkStateIfc::SetConnectedStateToConnected
File: .\AdapterNetworkStateIfc.cpp
Line: 147
Invoked Function: InternetSetOption
Return Code: 12010 (0x00002EEA)
Description: The length is incorrect for the option type
```

```
Description : Function: CTransportWinHttp::InitTransport
File: .\CTransportWinHttp.cpp
Line: 252
Invoked Function: CConnectedStateIfc::SetConnectedStateToConnected
Return Code: -25362420 (0xFE7D000C)
Description: CADAPTERNETWORKSTATEIFC_ERROR_SET_OPTION
```

Solución

Este comportamiento se observó y registró con la identificación de error de Cisco [CSCtx28970](#). Para resolver esto, salga de la aplicación de AnyConnect y vuelva a iniciarla. Las entradas de conexión reaparecen después del reinicio.

Mensaje de error: TLS_PROTOCOL_ERROR_INSUFFICIENT_BUFFER

El cliente de AnyConnect no se conecta y aparece el mensaje de error `Unable to establish a connection (No es posible establecer una conexión)`. En el registro de eventos de AnyConnect, se encuentra el mensaje `TLS_PROTOCOL_ERROR_INSUFFICIENT_BUFFER`.

Solución

Esto ocurre cuando la cabecera está configurada para túnel dividido con una lista muy extensa de túneles divididos (aproximadamente de 180 a 200 entradas) y hay uno o más atributos del cliente configurados en la política de grupo, como `dnd-server`.

Complete estos pasos para resolver el problema:

1. Reduzca la cantidad de entradas en la lista de túneles divididos.

2. Utilice esta configuración para deshabilitar DTLS:

```
group-policy groupName attributes
webvpn
svc dtls none
```

Para obtener más información, consulte la identificación de error de Cisco [CSCtc41770](#).

Mensaje de error: "Connection attempt has failed due to invalid host entry"

Aparece el mensaje de error `connection attempt has failed due to invalid host entry` (Error al intentar la conexión debido a una entrada de host no válida) mientras se realiza la autenticación de AnyConnect mediante un certificado.

Solución

Para resolver este problema, pruebe cualquiera de estas soluciones posibles:

- Actualice AnyConnect a la versión 3.0.
- Deshabilite Cisco Secure Desktop en su computadora.

Para obtener más información, consulte la identificación de error de Cisco [CSCti73316](#).

Error: "Ensure your server certificates can pass strict mode if you configure always-on VPN"

Al habilitar la función Always-On (Siempre activa) de AnyConnect, aparecerá el mensaje de error `Ensure your server certificates can pass strict mode if you configure always-on VPN` (Asegúrese de que sus certificados de servidor puedan superar el modo estricto si configura una VPN siempre activa).

Solución

Este mensaje de error implica que, si desea utilizar la función Always-On, necesita un certificado de servidor válido configurado en la cabecera. Sin un certificado de servidor válido, no funcionará. Strict Cert Mode (Modo estricto de certificado) es una opción que se configura en el archivo de política local de AnyConnect para asegurar que las conexiones usen un certificado válido. Si habilita esta opción en el archivo de política y se conecta con un certificado ficticio, ocurre un error de conexión.

Error: "Se ha producido un error interno en los servicios HTTP de Microsoft Windows"

La herramienta Diagnostic AnyConnect Reporting Tool (DART) muestra un intento fallido:

```
*****
Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnu

Description : Function: CTransportWinHttp::SendRequest
```

File: .\CTransportWinHttp.cpp
Line: 1170
Invoked Function: HttpSendRequest
Return Code: 12004 (0x00002EE4)
Description: **An internal error occurred in the Microsoft Windows HTTP Services**

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: ConnectIfc::connect
File: .\ConnectIfc.cpp
Line: 472

Invoked Function: ConnectIfc::sendRequest
Return Code: -30015443 (0xFE36002D)
Description: CTRANSPORT_ERROR_CONN_UNKNOWN

Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui

Description : Function: ConnectIfc::TranslateStatusCode
File: .\ConnectIfc.cpp
Line: 2999

Invoked Function: ConnectIfc::TranslateStatusCode
Return Code: -30015443 (0xFE36002D)
Description: CTRANSPORT_ERROR_CONN_UNKNOWN
Connection attempt failed. Please try again.

Consulte también los registros del visor de eventos en la máquina que ejecuta Windows.

Solución

Esto podría deberse a una conexión Winsock dañada. Use el siguiente comando para restablecer la conexión desde el símbolo del sistema y reinicie su máquina que ejecuta Windows:

netsh winsock reset

Para obtener más información, consulte el artículo de la base de conocimientos [Cómo determinar si Winsock2 se ha dañado en Windows Server 2003, Windows XP y Windows Vista y la forma de recuperarlo.](#)

Error: "El transporte SSL recibió una falla de Secure Channel. Puede ser el resultado de una configuración criptográfica no admitida en el gateway seguro".

La herramienta Diagnostic AnyConnect Reporting Tool (DART) muestra un intento fallido:

Date : 10/27/2014
Time : 16:29:09
Type : Error
Source : acvpnui

Description : Function: CTransportWinHttp::handleRequestError
File: .\CTransportWinHttp.cpp
Line: 854
The SSL transport received a Secure Channel Failure. May be a result of a unsupported crypto configuration on the Secure Gateway.

Date : 10/27/2014
Time : 16:29:09
Type : Error
Source : acvpnuui

Description : Function: CTransportWinHttp::SendRequest
File: .\CTransportWinHttp.cpp
Line: 1199
Invoked Function: CTransportWinHttp::handleRequestError
Return Code: -30015418 (0xFE360046)
Description: CTRANSPORT_ERROR_SECURE_CHANNEL_FAILURE

Date : 10/27/2014
Time : 16:29:09
Type : Error
Source : acvpnuui

Description : Function: ConnectIfc::TranslateStatusCode
File: .\ConnectIfc.cpp
Line: 3026
Invoked Function: ConnectIfc::TranslateStatusCode
Return Code: -30015418 (0xFE360046)
Description: CTRANSPORT_ERROR_SECURE_CHANNEL_FAILURE
Connection attempt failed. Please try again.

Solución

Windows 8.1 no admite RC4 según la siguiente actualización de KB:

<http://support2.microsoft.com/kb/2868725>

Configure los cifrados DES/3DES para SSL VPN en el ASA usando el comando "ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1" O edite el archivo del Registro de Windows en el equipo cliente como se menciona a continuación:

<https://technet.microsoft.com/en-us/library/dn303404.aspx>

Información Relacionada

- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Preguntas Más Frecuentes sobre AnyConnect VPN Client](#)
- [Preguntas Frecuentes sobre Cisco Secure Desktop \(CSD\)](#)
- [Cisco AnyConnect VPN Client](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)