ASA Clientless SSLVPN: Problemas de plug-in RDP

Contenido

Introducción

Este documento proporciona respuestas a algunas preguntas frecuentes sobre el plug-in de protocolo de escritorio remoto (RDP), disponible para los usuarios de Cisco Adaptive Security Appliance (ASA) Clientless Secure Sockets Layer VPN (SSLVPN).

El complemento RDP es sólo uno de los complementos disponibles para los usuarios, junto con otros como Secure Shell (SSH), Virtual Network Computing (VNC) y Citrix. El plug-in RDP es uno de los plug-in más utilizados en esta colección. Este documento proporciona más detalles sobre los procedimientos de implementación y solución de problemas para este plug-in.

> **Nota:** Este documento no proporciona información sobre cómo configurar el plug-in RDP. Para obtener más información, consulte la Guía de implementación de Cisco ASA 5500 SSL VPN, versión 8.x.

Antecedentes

El plug-in RDP ha evolucionado desde un plug-in RDP basado exclusivamente en Java, para incluir tanto el cliente RDP ActiveX (Internet Explorer) como el cliente Java (exploradores que no son de Internet Explorer).

Complemento Java

El cliente RDP de Java utiliza el applet RDP de Java adecuado. El subprograma Java se incluye luego en un plug-in que permite la instalación dentro del portal sin cliente ASA.

Complemento Active-X

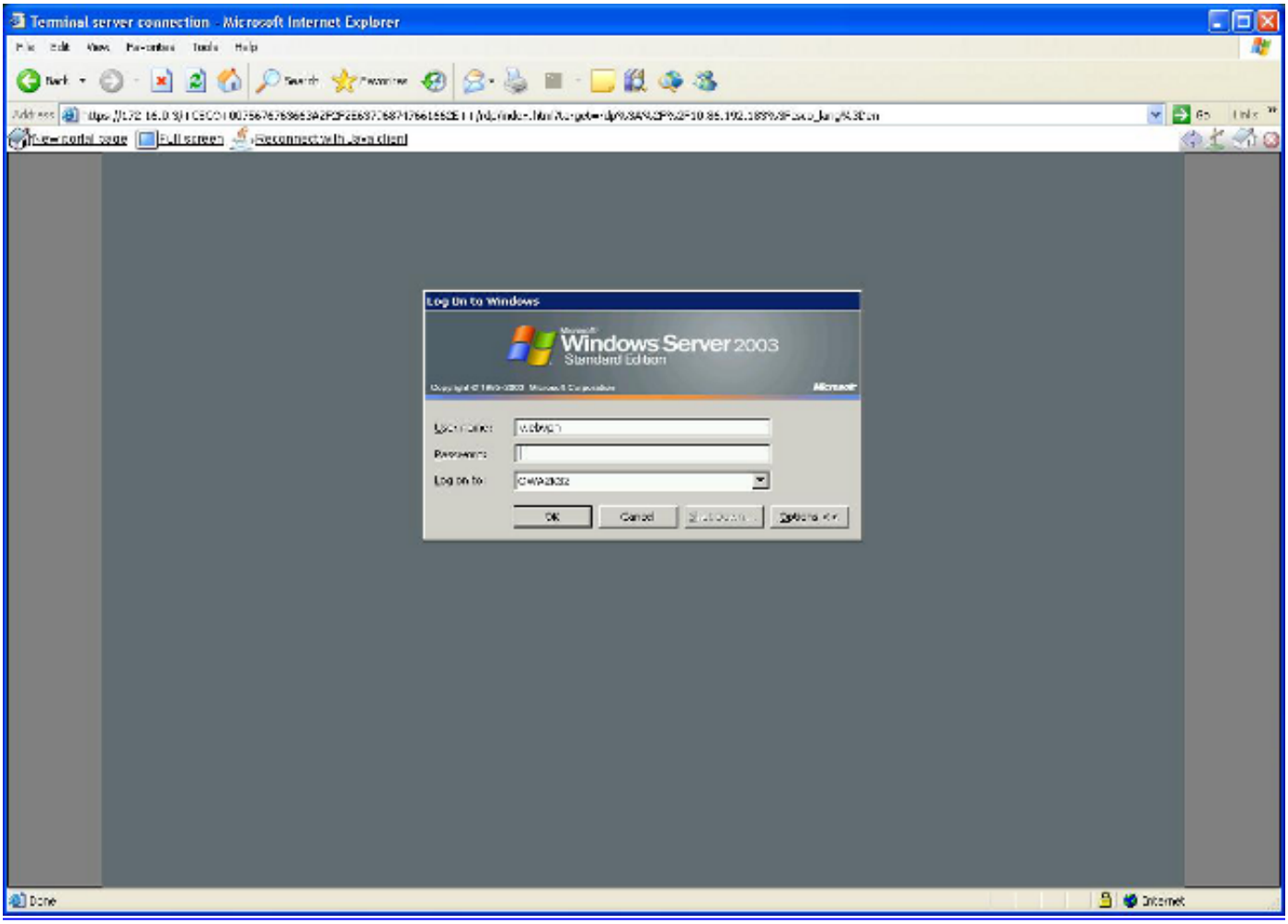
El plug-in RDP también incluye el cliente RDP de Microsoft ActiveX y el plug-in determina si se utiliza Java o el cliente ActiveX basado en el navegador. Es decir:

- Si los usuarios de Internet Explorer (IE) intentan utilizar RDP a través de un portal SSLVPN sin cliente y la URL de marcador no contiene el argumento **ForceJava=true**, se utiliza el cliente ActiveX. Si ActiveX no se puede ejecutar, el plug-in inicia el cliente Java.
- Si los usuarios que no son de IE intentan iniciar un marcador RDP o una URL, sólo se inicia el cliente de Java.

Para obtener más información sobre los requisitos para los privilegios de RDP ActiveX y USER, consulte el artículo Microsoft Requirements for Remote Desktop Web Connection.

La siguiente imagen ilustra los tres enlaces que se pueden seleccionar en la ventana del navegador después de iniciar el plug-in:

1. **Nueva página del portal**: este enlace abre la página del portal en una nueva ventana del navegador.
2. **Pantalla completa**: utiliza la ventana RDP en modo de pantalla completa.
3. **Reconnect with Java** - Esto fuerza al plug-in a volver a conectarse y utilizar Java en lugar de ActiveX.



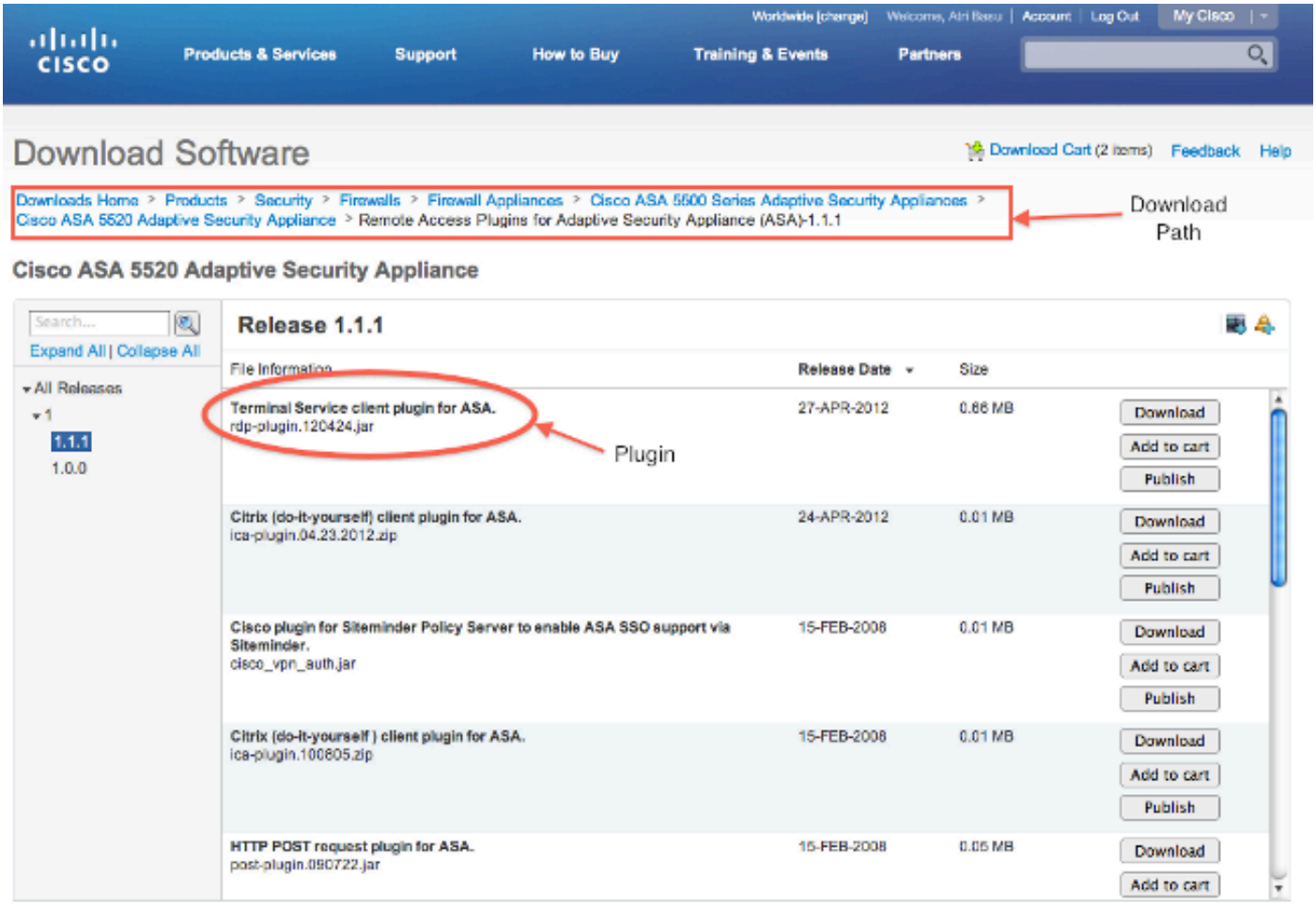
Complemento RDP

Uso de complementos RDP y RDP-2

- **plug-in RDP:** Éste es el complemento original creado que contiene tanto el cliente Java como el cliente ActiveX.
- **plug-in RDP2:** Debido a los cambios dentro del protocolo RDP, se actualizó el cliente RDP de Java adecuado para soportar los servidores de terminal de Microsoft Windows 2003 y los servidores de terminal de Windows Vista.

  Consejo: El último plug-in RDP combina tanto los protocolos RDP como RDP2. Como resultado, el plug-in RDP2 está obsoleto. Se recomienda utilizar la versión más reciente del plug-in RDP. La nomenclatura de complementos RDP sigue esta estructura: **rdp-plugin.yymmdd.jar**, donde **yy** es un formato de año de dos dígitos, **mm** es un formato de mes de dos dígitos y **dd** es un formato de día de dos dígitos.

Para descargar el plug-in, visite la página de descarga de software de Cisco.



Posicionamiento de clientes de ActiveX frente a Java

RDP-ActiveX

- Sólo utiliza IE
- Proporciona compatibilidad para el sonido reenviado

RDP-Java

- Funciona en todos los exploradores compatibles que estén habilitados para Java.
- Java Client se inicia en IE sólo si ActiveX no se inicia o el argumento **ForceJava=true** pasa en el marcador RDP.
- La implementación de RDP-Java se basa en el proyecto RDP de Java Adecuado, una iniciativa de código abierto; se proporciona soporte de mejor esfuerzo para la aplicación.

Formato de marcador RDP

Este es un formato de ejemplo de un marcador RDP:

```
rdp://server:port/?Parameter1=value&Parameter2=value&Parameter3=value
```

A continuación, algunas notas importantes sobre el formato:

- **server** - Este es el único atributo requerido. Introduzca el nombre del equipo que aloja Microsoft Terminal Services.
- **port** (opcional): dirección virtual del equipo remoto que aloja Microsoft Terminal Services. El valor predeterminado, 3389, coincide con el número de puerto conocido para Microsoft Terminal Services.
- **Parameters**: Se trata de una cadena de consulta opcional que consta de pares parámetro-valor. Un signo de interrogación demarca el principio de la cadena de argumento y cada par de valor de parámetro está separado por un signo de interrogación.

  A continuación se muestra una lista de los parámetros disponibles:

  geometría: tamaño de la pantalla del cliente en píxeles (An. x Al.).**bpp**: es el bit por píxel (profundidad de color), 8|16|24|32.**dominio**: este es el dominio de inicio de sesión.**username** - Este es el nombre de usuario para el login.**password** - Ésta es la contraseña de inicio de sesión. Utilice la contraseña con cuidado, porque se utiliza en el lado del cliente y se puede observar.**console** - Se utiliza para conectar a la sesión de consola en el servidor (yes/no).**ForceJava** - Establezca este parámetro en **yes** para utilizar solamente el cliente Java. El valor predeterminado es **no**.**shell**: establezca este parámetro en la ruta del ejecutable/aplicación que se inicia automáticamente cuando se conecta con RDP (**rdp://server/?shell=path**, por ejemplo).

  A continuación se muestra una lista de parámetros adicionales de ActiveX únicamente:

  RedirectDrive - Establezca este parámetro en **true** para asignar unidades remotas localmente.**RedirectPrinters** - Establezca este parámetro en **true** para asignar impresoras remotas localmente.**FullScreen** - Establezca este parámetro en **true** para iniciar en modo FullScreen.**ForceJava** - Establezca este parámetro en **yes** para forzar el cliente Java.**audio** - Este parámetro se utiliza para el reenvío de audio sobre la sesión RDP:

  0: redirige los sonidos remotos al equipo cliente.**1** - Reproduce sonidos en el equipo remoto.**2** - Inhabilita la redirección de sonido; no reproduce sonidos en el servidor remoto.

Complemento RDP y Balanceo de Carga VPN

El balanceo de carga multigeográfico se admite con el uso de equilibrio de carga de servidor global basado en servidor de nombres de dominio (DNS). Debido a las diferencias en el almacenamiento en caché de resultados de DNS, los plug-ins podrían funcionar de forma diferente en diversos sistemas operativos. La caché de DNS de Windows permite que el plug-in resuelva la misma dirección IP cuando inicia el applet Java. En Macintosh (MAC) OS X, es posible que el applet Java resuelva una dirección IP diferente. Como resultado, el plug-in no se puede iniciar correctamente.

Un ejemplo de ordenamiento cíclico de DNS es cuando tiene una única URL (https://www.example.com) donde la entrada DNS para **www.example.com** puede resolver 192.0.2.10 (ASA1) o 198.51.100.50 (ASA2).

Después de que el usuario inicie sesión en el portal Clientless-WebVPN a través de un navegador

en ASA1, es posible iniciar el plug-in RDP. Durante el inicio del cliente Java, los ordenadores MAC OS X ejecutan una nueva solicitud de resolución DNS. Con una configuración DNS de ordenamiento cíclico, hay un 50% de probabilidades de que esta respuesta de segunda resolución devuelva el mismo sitio que se eligió para la conexión WebVPN inicial. Si la respuesta del servidor DNS es 198.51.100.50 (ASA2) en lugar de 192.0.2.10 (ASA1), el cliente Java inicia una conexión al ASA (ASA2) incorrecto. Como la sesión de usuario no existe en ASA2, se rechaza la solicitud de conexión.

Esto podría dar lugar a mensajes de error de Java similares a estos:

```
java.lang.ClassFormatError: Incompatible magic value 1008813135 in
 class file net/propero/rdp/applet/RdpApplet
```

Preguntas más Frecuentes

¿Por qué algunos caracteres con tipo no aparecen en la sesión RDP remota?

El equipo remoto de la sesión RDP puede tener una configuración de región de teclado diferente a la del equipo local. Debido a esta diferencia, es posible que el equipo remoto no muestre ciertos caracteres con tipo o caracteres incorrectos. Este comportamiento sólo se ve con el plug-in de Java. Para resolver este problema, utilice el atributo **keymap** para mapear el mapa de teclado local al equipo remoto.

Por ejemplo, para establecer una asignación de teclado en alemán, utilice:

```
rdp://
```

```
The following keymaps are available:
--------------------------------------------------------------------
ar    de    en-us fi    fr-be it    lt    mk    pl    pt-br sl    tk
da    en-gb es    fr    hr    ja    lv    no    pt    ru    sv    tr
--------------------------------------------------------------------
```

Problemas conocidos con las asignaciones de teclado

- Id. de bug Cisco CSCth38454 - **Implemente el mapa de teclado húngaro para el plug-in RDP.**
- ID de bug Cisco CSCsu77600 - **Las claves de ventana del complemento RDP de WebVPN son incorrectas. Mayús (tecla) .jar**.
- Id. de error de Cisco CSCtt04614 - **WebVPN - Diacrítica del teclado ES administrada incorrectamente por el complemento RDP.**
- Id. de bug Cisco CSCtb07767 - **Complemento ASA - Configurar parámetros predeterminados**.

Consejo: Otra solución alternativa posible es utilizar un túnel inteligente de aplicación para

mstsc.exe. Esto se configura en el modo de subconfiguración de WebVPN con este comando: **lista de túnel inteligente RDP_List RDP mstsc.exe plataformas windows**.

¿Puede el plug-in Java RDP soportar sesiones RDP de pantalla completa?

Actualmente, no hay soporte nativo para sesiones RDP de pantalla completa. La solicitud de mejora CSCto87451 fue presentada para implementar esto. Si el parámetro **geometría** (**geometría =1024x768**, por ejemplo) se establece en la resolución del monitor de usuario, funciona en modo de pantalla completa. Debido a que los tamaños de pantalla del usuario varían, puede ser necesario crear varios enlaces de marcadores. El cliente ActiveX admite de forma nativa sesiones RDP de pantalla completa.

¿Puede el cliente Java comunicarse con el uso de AES-256 para el cifrado?

Para permitir que el cliente Java negocie el SSL correctamente, ajuste el orden del cifrado SSL de ASA para que coincida con esto:

```
Enabled cipher order: aes256-sha1 rc4-sha1 aes128-sha1 3des-sha1
Disabled ciphers: des-sha1 rc4-md5 null-sha1
```

El cliente Java podría mostrar este error si el orden del conjunto de cifras es diferente:

```
[Thread-12] INFO net.propero.rdp.Rdp - javax.net.ssl.SSLHandshakeException:
 Received fatal alert: handshake_failure
```

Solución de problemas de RDP

Si experimenta otros problemas con el plug-in RDP, podría ser útil recopilar estos datos para resolver problemas de RDP:

- La salida **show tech** del ASA
- El resultado **detallado de show import webvpn Plug-in** del ASA
- El sistema operativo del equipo del usuario y el nivel de parche
- El sistema operativo del equipo de destino y el nivel de parche
- El cliente que se utiliza (ActiveX o Java) y la versión Java JRE
- Determine si el ASA se encuentra en un clúster de equilibrio de carga, basado en DNS o basado en ASA

Advertencias conocidas

Problemas de actualización de seguridad de Microsoft

1. KB2695962 - Microsoft Security Advisory: Actualizar acumulación de bits de matar de ActiveX: 8 de may de 2012.

2. KB2675157 - MS12-023: Actualización de seguridad acumulada para Internet Explorer: 10 de abril de 2012.
3. cisco-sa-20120314-asaclient - Vulnerabilidad de ejecución de código remoto de control ActiveX de VPN sin cliente de Cisco ASA serie 5500 - 14 de marzo.
4. Id. de bug Cisco CSCtx68075 - Falla de WebVPN ASA cuando se aplica el parche KB258542 de Windows (8.2.5.29 / 8.4.3.9).
5. KB2585542 - MS12-006: Descripción de la actualización de seguridad para Webio, Winhttp y schannel en Windows: 10 de enero de 2012.

Cliente ActiveX

- **Síntomas:** El cliente ActiveX no puede cargar desde las versiones 6 a 9 de IE después de una actualización a la versión 8.4.3 del sistema operativo ASA.

  Consulte Cisco bug ID CSCtx58556. La corrección está disponible para las versiones 8.4.3.4 y posteriores.Solución alternativa: Forzar el uso del cliente Java.

- **Síntomas:** El cliente ActiveX no puede cargarse después de que la versión del sistema operativo ASA se haya degradado a una versión anterior a 8.4.3. Esto afecta a los usuarios que han utilizado el cliente ActiveX en un ASA con la corrección para el ID de bug Cisco CSCtx58556 y se conectan a este ASA con una versión anterior a 8.4.3. Esto se debe a un nuevo plug-in ActiveX RDP introducido en ASA versión 8.4.3, que no es compatible con las versiones anteriores.

  Consulte Cisco bug ID CSCtx57453.¿Eliminar todas las instancias del Registro de Windows de **b8e73359-3422-4384-8d27-4ea1b4c01232?** (antiguo CLSID de ActiveX).

  Nota: Se recomienda realizar una copia de seguridad del registro del sistema informático antes de realizar cualquier edición.
- **Síntomas:** Las conexiones RDP a los dispositivos con la autenticación de nivel de red (NLA) activada fallan.

  Consulte Cisco bug ID CSCtu63661 para ver la mejora que solicita que NLA se incorpore en el plug-in de RDP ActiveX.Aunque Microsoft ActiveX Client es compatible con NLA, el uso de esa función dentro del plug-in ASA no es compatible.Solución alternativa: configure el complemento RDP (**mstsc.exe**) para que se tunelice de forma inteligente. Consulte Guía de implementación de Cisco ASA 5500 SSL VPN, versión 8.x.

- **Síntomas:** El RDP de ActiveX no se puede cargar y muestra una página en blanco.

  Consulte Cisco bug ID CSCsx49794.Esto ocurre cuando la cadena de certificados para el certificado SSL ASA es mayor que cuatro certificados (ROOT, SUBCA1, SUBCA2 y ASA CERT, por ejemplo).Solución alternativa:

  No instale la cadena de certificados grande en el ASA.Se sabe que el plug-in de Java RDP funciona correctamente, a diferencia del plug-in ActiveX.RDP también funciona correctamente cuando se configura Windows **mstsc.exe nativo** con túneles inteligentes.

- **Síntomas:** Después de utilizar el cliente RDP ActiveX, un usuario hace clic en el botón **Cerrar sesión** y recibe un **error HTTP 404 - Página no encontrada**. Consulte Cisco bug ID CSCtz33266. Este problema se ha resuelto con la versión plug-in **rdp-plugin.120424.jar** o posterior.

- **Síntomas:** Un usuario tiene dos fichas abiertas en IE: una para la sesión RDP y otra para una página web en blanco u otra. El IE no funciona correctamente después de cerrar la ficha RDP.

  Consulte Cisco bug ID CSCua69129.Solución alternativa: Utilice el plug-in de Java RDP (Set **ForceJava=true**).

- **Síntomas:** El plug-in ActiveX causa un uso elevado de la CPU con IE. Consulte Cisco bug ID CSCua16597.

- **Síntomas:** Después de la instalación de la actualización de Windows **KB2695962,** el plug-in RDP ActiveX no se carga. Cuando se abre una nueva sesión RDP, el cliente ActiveX intenta instalar el **Cisco SSL VPN Port Forwarder** (esto no siempre sucede) y vuelve a la página del portal sin cliente sin conectarse al equipo remoto. Esto se debe a la vulnerabilidad **CVE-2012-0358,** que se resuelve en el lado del cliente mediante Microsoft Security Advisory (2695962).

  Refiérase a Vulnerabilidad de Ejecución de Código Remoto de Control ActiveX de Cisco ASA 5500 Series Adaptive Security Appliance Clientless VPN.Consulte Cisco Bug ID CSCtr00165.

Cliente Java

> **Nota**: Cisco redistribuye los plug-ins sin ningún cambio. Debido a la Licencia Pública General de GNU, Cisco no modifica ni amplía la aplicación plug-in. El plug-in **JavaRDP adecuado** es una aplicación de código abierto, y cualquier problema con el software plug-in debe ser resuelto por el propietario del proyecto.

- **Síntomas:** Las aplicaciones con uso intensivo del procesador se ejecutan en el equipo remoto cuando se accede a través del cliente RDP de Java, y se produce una caída del Applet de Java.

  Este mensaje de error podría mostrar: **FATAL net.propero.rdp - javax.net.ssl.SSLException: Se ha apagado la conexión: .....**El comportamiento se activa cuando se cambia rápidamente entre dos o más aplicaciones que hacen un uso intensivo de la CPU.Este problema se soluciona en las versiones de plug-in rdp.2012.6.4.jar y posteriores. Solución alternativa:

  Conéctese con el cliente ActiveX.No cambie entre aplicaciones rápidamente.

- **Síntomas:** El cliente Java RDP genera este mensaje de error: **net.propero.rdp.Rdp - java.net.SocketException: Socket está cerrado java.net.SocketException: El socket está cerrado** y, a continuación, se cierra.

El problema es causado por un grupo de túnel que tiene una url de grupo configurada sólo con el FQDN (http://www.example.com, por ejemplo).Consulte Cisco bug ID CSCuh72888.Solución alternativa:

Quite la entrada group-URL sin un "/" en el grupo de túnel.Utilice el cliente ActiveX.

- **Síntomas:** Java RDP Client falla cuando se conecta a un equipo con Windows 8.

  El cliente RDP de Java actualmente no tiene soporte para esto.Consulte Cisco bug ID CSCuc79990Solución alternativa:

  Utilice el cliente RDP ActiveX.Túnel inteligente del cliente RDP nativo de Windows (**mstsc.exe**).

- **Síntomas:** El cliente RDP de Java falla con este mensaje de error: **Excepción ARSigningException: Entrada no firmada encontrada en el recurso: https://10.105.130.91/+CSCO+3a75676763663A2F2F2E637968747661662E++/vnc/VncViewer.jar**.

  Este problema es causado por un error de funcionamiento en ASA webVPN Java rewriter.Consulte Cisco bug ID CSCuj88114.Solución alternativa: Reversión a Java versión 7u40.