Clientless SSLVPN ASA: Problemas del enchufe RDP

Contenido

Introducción

Este documento proporciona las respuestas a algunas preguntas frecuentes sobre el enchufe del protocolo del Escritorio Remoto (RDP), disponible para los usuarios adaptantes de Secure Sockets Layer VPN (SSLVPN) del clientless del dispositivo de seguridad de Cisco (ASA).

El enchufe RDP es solamente uno de los enchufes disponibles para los usuarios, junto con otros tales como Secure Shell (SSH), Virtual Network Computing (VNC), y Citrix. El enchufe RDP es uno lo más frecuentemente de los enchufes usados en esta colección. Este documento proporciona más detalles sobre los procedimientos del despliegue y del Troubleshooting para este enchufe.

> Nota: Este documento no proporciona la información sobre cómo configurar el enchufe RDP. Para la información adicional, refiera a la guía del despliegue de VPN de Cisco ASA

5500 SSL, versión 8.x.

Antecedentes

El enchufe RDP se ha desarrollado de un enchufe puro de la Java basada RDP, para incluir ambo el cliente de ActiveX RDP (Internet Explorer), así como al cliente de las Javas (navegadores del explorador de NON-Internet).

Módulo Java

El cliente de las Javas RDP utiliza el applet apropiado de las Javas RDP. Los subprogramas java entonces se envuelven dentro de un enchufe que permita la instalación dentro del portal del clientless ASA.

Enchufe activo-x

El enchufe RDP también incluye al cliente de Microsoft ActiveX RDP, y el enchufe determina si utilizar las Javas o al cliente de ActiveX basado en el hojeador. Es decir:

- Si los usuarios del internet explorer (IE) intentan utilizar el RDP a través de un portal del clientless SSLVPN, y el marcador URL no contiene el argumento de **ForceJava=true**, después utilizan al cliente de ActiveX. Si ActiveX no puede ejecutar, el enchufe inicia al cliente de las Javas.
- Si los usuarios NON-IE intentan iniciar un marcador RDP o un URL, sólo inician al cliente de las Javas.

Para más información sobre los requisitos para los privilegios RDP ActiveX y del USUARIO, refiérase a los requisitos de Microsoft para el artículo de la conexión Web del Escritorio Remoto.

La imagen siguiente ilustra los tres links que se pueden seleccionar dentro de la ventana del buscador después de que se inicie el enchufe:

1. **Nueva página porta** - Este link abre la página porta en una nueva ventana del buscador.
2. **De plena pantalla** - Esto utiliza la ventana RDP en el modo de plena pantalla.
3. **Vuelva a conectar con las Javas** - Esto fuerza el enchufe para volver a conectar y para utilizar las Javas en vez de ActiveX.

Enchufe RDP

Uso del enchufe RDP y RDP-2

- **Enchufe RDP:** Éste es el enchufe original creado que contiene las Javas y al cliente de

ActiveX.

- **Enchufe RDP2:** Debido a los cambios dentro del protocolo RDP, el cliente apropiado de las Javas RDP era actualizado para soportar Microsoft Windows 2003 servidores terminales y los servidores terminales de Windows Vista.

  Consejo: El último enchufe RDP combina los protocolos RDP y RDP2. Como consecuencia el enchufe RDP2 es Obsoleto. Se recomienda para utilizar la versión más-reciente del enchufe RDP. Las nomenclaturas plugs-in RDP siguen esta estructura: **rdp-plugin.yymmdd.jar, donde está un** formato el **yy de dos dígitos del año**, milímetro es un formato del **two-digitmonth**, y la DD es un formato **two-digitday**.

Para descargar el enchufe, visite la página de la descarga de software de Cisco.

ActiveX contra la colocación del cliente de las Javas

RDP-ActiveX

- Aplicaciones IE solamente
- Proporciona el soporte para el sonido remitido

RDP-Javas

- Trabaja en todos los buscadores admitidos Java-se habiliten que.
- Inician al cliente de las Javas en el IE solamente si ActiveX no puede iniciar, o el argumento de **ForceJava=true** pasa en el marcador RDP.
- La implementación de las RDP-Javas se basa en el proyecto apropiado de las Javas RDP, una iniciativa de fuente abierta; el soporte de mejor esfuerzo se proporciona para la aplicación.

Formato del marcador RDP

Aquí está un ejemplo de formato de un marcador RDP:

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

Aquí están algunas NOTAS IMPORTANTES sobre el formato:

- **servidor** - Éste es el único atributo requerido. Ingrese el nombre del ordenador que recibe los servicios de terminal de Microsoft.
- **puerto** (opcional) - Ésta es la dirección virtual dentro de la computadora remota que recibe los servicios de terminal de Microsoft. El valor predeterminado, 3389, hace juego el número de puerto conocido para los servicios de terminal de Microsoft.
- **parámetros** - Ésta es una cadena de consulta opcional que consiste en los pares del Valor de

parámetro. Los demarks de un signo de interrogación el principio de la cadena del argumento, y cada par del Valor de parámetro es separados por un signo "&".

Aquí está una lista de parámetros disponibles:

geometría - Éste es el tamaño de la pantalla del cliente en los pixeles (W x H).**bpp** - Éste es el bit-por-pixel (intensidad del color), 8|16|24|32.**dominio** - Éste es el dominio del login.**nombre de usuario** - Éste es el nombre de usuario para el login.**contraseña** - Ésta es la contraseña de inicio de sesión. Utilice la contraseña con el cuidado, porque se utiliza en el client cara y puede ser observado.**consola** - Esto se utiliza para conectar con la sesión de consola en el servidor (sí/no).**ForceJava** - Fije este parámetro al **sí** para utilizar solamente al cliente de las Javas. La configuración predeterminada es **no.shell** - Fije este parámetro a la trayectoria del ejecutable/de la aplicación que se comienza automáticamente cuando usted conecta con RDP (**rdp://server/?shell=path**, por ejemplo).

Aquí está una lista de parámetros adicionales de ActiveX-solamente:

RedirectDrives - Fije este parámetro **para verdad** para asociar las unidades remotas localmente.**RedirectPrinters** - Fije este parámetro **para verdad** para asociar las impresoras remotas localmente.**De plena pantalla** - Fije este parámetro **para verdad** para iniciar en el modo de plena pantalla.**ForceJava** - Fije este parámetro al **sí** para forzar al cliente de las Javas.**el audio** este parámetro se utiliza para la expedición audio sobre la sesión RDP:

0 - Reorienta los sonidos remotos a la computadora cliente.**1** - Juega los sonidos en la computadora remota.**2** - Inhabilita el cambio de dirección sano; no juega los sonidos en el servidor remoto.

Enchufe RDP y balanceo de carga VPN

el balanceo de carga de la Multi-geografía se soporta con el uso del Domain Name Server (DNS) - Equilibrio de carga basado del servidor global. Debido al resultado DNS que ocultaba las diferencias, los enchufes pudieron actuar diferentemente a través de los sistemas operativos variados. El caché de Windows DNS permite que el enchufe resuelva la misma dirección IP cuando él los lauches los subprogramas java. En Macintosh (MAC) OS X, es posible que los subprogramas java resuelvan una diversa dirección IP. Como consecuencia, el enchufe no puede iniciar correctamente.

Un ejemplo del DNS circular es cuando usted tiene un solo 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 los registros de usuario en el portal del Clientless-WebVPN vía un navegador en ASA1, el initiaition del enchufe RDP es posible. Durante el lanzamiento del cliente de las Javas, los ordenadores de MAC OS X ejecutan una nueva petición de la resolución de DNS. Con una Configuración de DNS circular, hay una ocasión del 50% que esta segunda respuesta de la resolución vuelve el mismo sitio que fue elegido para la conexión WebVPN inicial. Si la respuesta del servidor DNS es 198.51.100.50 (ASA2) bastante que 192.0.2.10 (ASA1), el cliente de las Javas inicia una conexión al ASA incorrecto (ASA2). Pues la sesión del usuario no existe en el ASA2, se rechaza el pedido de conexión.

Esto pudo dar lugar a los mensajes de error de Java similares a esto:

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

Preguntas más Frecuentes

¿Por qué algunos caracteres tecleados no aparecen en la sesión del telecontrol RDP?

La computadora remota en la sesión RDP pudo tener una diversa configuración de la región del teclado que la computadora local. Debido a esta diferencia, la computadora remota no pudo visualizar los ciertos caracteres o caracteres incorrectos tecleados. Este comportamiento se considera con solamente con el módulo Java. Para resolver este problema, utilice el atributo del **keymap** para asociar el keymap local en la PC remota.

Por ejemplo, para fijar una asignación alemana del teclado, uso:

```
rdp://<IP Address of the server>/?keymap=de

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 del teclado

- Id. de bug Cisco CSCth38454 - **Implemente el keymap húngaro para el enchufe RDP.**
- Id. de bug Cisco CSCsu77600 - **Las claves plugs-in de la ventana del WebVPN RDP son incorrectas. Desplace el .jar (dominante)**.
- Id. de bug Cisco CSCtt04614 - **WebVPN - Signos diacríticos del teclado ES manejados incorrectamente por el RDP plug-in.**
- Id. de bug Cisco CSCtb07767 - **ASA plug-in - Parámetros predeterminados de la configuración**.

  Consejo: Otra solución alternativa posible es utilizar un túnel elegante de la aplicación para **mstsc.exe. Esto** se configura bajo modo de la sub-configuración del WebVPN con este comando: **ventanas de la plataforma de RDP_List RDP mstsc.exe de la lista del Smart-túnel.**

¿Pueden las sesiones de plena pantalla del soporte plug-in RDP de las Javas RDP?

Actualmente, no hay soporte nativo para las sesiones de plena pantalla RDP. El pedido de mejora CSCto87451 fue clasificado para implementar esto. Si el parámetro de la **geometría** (**geometría =1024x768**, por ejemplo) se fija a la resolución del monitor del usuario, actúa en el modo de plena pantalla. Pues los tamaños de la pantalla del usuario varían, puede ser que sea necesario establecer las relaciones múltiples del marcador. El cliente de ActiveX soporta nativo

las sesiones de plena pantalla RDP.

¿Puede el cliente de las Javas comunicar con el uso del AES-256 para el cifrado?

Para permitir que el cliente de las Javas negocie el SSL correctamente, ajuste la orden del cifra-conjunto ASA SSL para hacer juego esto:

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

El cliente de las Javas pudo visualizar este error si la orden del cifra-conjunto es diferente:

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

Problemas del Troubleshooting RDP

Si usted experimenta otros problemas con el enchufe RDP, puede ser que sea útil recoger estos datos para resolver problemas los problemas RDP:

- **La tecnología de la demostración** hecha salir del ASA
- La salida **detallada plug-in del webvpn de la importación de la demostración del** ASA
- El sistema operativo y el corrección-nivel del ordenador del usuario
- El sistema operativo y el corrección-nivel de la computadora destino
- El cliente se utiliza que (ActiveX o las Javas) y versión JRE de las Javas
- Determine si el ASA está en un cluster del balance de la carga, basado en DNS, o ASA-basado

Advertencias conocidas

Problemas de la actualización de seguridad de Microsoft

1. KB2695962 - Security Advisory de Microsoft: Rollup de la actualización para los bits de la matanza de ActiveX: 8 de mayo, 2012.
2. KB2675157 - MS12-023: Actualización de seguridad acumulativa para Internet Explorer: De abril el 10 de 2012.
3. cisco-sa-20120314-asaclient - Vulnerabilidad remota de marzo el 14 de la ejecución de códigos del dispositivo de seguridad de las 5500 Series de Cisco ASA del control ActiveX adaptante del clientless VPN.
4. Id. de bug Cisco CSCtx68075 - WebVPN ASA que se rompe cuando la corrección KB2585542 de Windows es aplicada (8.2.5.29/8.4.3.9).
5. KB2585542 - MS12-006: Descripción de la actualización de seguridad para Webio, Winhttp, y el schannel en Windows: De enero el 10 de 2012.

Cliente de ActiveX

- Síntomas: El cliente de ActiveX no puede cargar de las versiones 6 a 9 IE después de una

actualización a la versión de OS 8.4.3 ASA.

Refiera al Id. de bug Cisco CSCtx58556. El arreglo está disponible para las versiones 8.4.3.4 y posterior.Solución alternativa: Fuerce el uso del cliente de las Javas.

- Síntomas: El cliente de ActiveX no puede cargar después de que la versión de OS ASA se retroceda a una versión antes de 8.4.3. Esto afecta a los usuarios que han utilizado al cliente de ActiveX en un ASA con el arreglo para el Id. de bug Cisco CSCtx58556, y conecta con este ASA con una versión antes de 8.4.3. Esto es debido a un nuevo enchufe de ActiveX RDP introducido en la Versión de ASA 8.4.3, que no es compatible con las versiones anteriores.

  Refiera al Id. de bug Cisco CSCtx57453.**¿**Quite todos los casos del registro de Windows de **b8e73359-3422-4384-8d27-4ea1b4c01232?** (ActiveX viejo CLSID).

  Nota: Se sugiere para realizar un respaldo del registro del sistema informático antes de ningunos edita.
- Síntomas: Las conexiones RDP a los dispositivos con la autenticación del nivel de red (NLA) habilitaron el fall.

  Refiera al Id. de bug Cisco CSCtu63661 para la mejora que solicita NLA para ser incorporada dentro del enchufe de ActiveX RDP.Aunque los soportes de cliente NLA de Microsoft ActiveX, uso de esa característica dentro del enchufe ASA no se soporten.Solución alternativa: Configure el enchufe RDP (**mstsc.exe) Smart-**que se hará un túnel. Refiera a la guía del despliegue de VPN de Cisco ASA 5500 SSL, versión 8.x.

- Síntomas: ActiveX RDP no puede cargar, y muestra una página en blanco.

  Refiera al Id. de bug Cisco CSCsx49794.Esto ocurre cuando la Cadena de certificados para el certificado ASA SSL es mayor de cuatro Certificados (RAÍZ, SUBCA1, SUBCA2, y ASA CERT, por ejemplo).Solución alternativa:

  No instale la Cadena de certificados grande en el ASA.El enchufe de las Javas RDP se sabe para trabajar correctamente, en comparación con el enchufe de ActiveX.El RDP también trabaja correctamente cuando usted configura las ventanas nativas **mstsc.exe con los** túneles elegantes.

- Síntomas: Después de que utilicen al cliente de ActiveX RDP, un usuario hace clic el **botón Logout Button** y recibe un **HTTP 404 -** error **no encontrado de la página**. Refiera al Id. de bug Cisco CSCtz33266. Este problema tiene se resuelve con el Módulo, versión **rdp-plugin.120424.jar** o más adelante.

- Síntomas: Un usuario tiene dos lenguetas abiertas en el IE - uno para la sesión RDP y otro para el espacio en blanco o la otra página web. El IE no puede actuar correctamente después de que la lengueta RDP sea cerrada.

  Refiera al Id. de bug Cisco CSCua69129.Solución alternativa: Utilice el enchufe de las Javas RDP (fije **ForceJava=true**).

- Síntomas: El enchufe de ActiveX causa el uso de la CPU elevada con el IE. Refiera al Id. de bug Cisco CSCua16597.

- Síntomas: Después de la actualización **KB2695962 de la** instalación de Windows**, el** enchufe de ActiveX RDP no carga. Cuando se abre una nueva sesión RDP, el cliente de ActiveX intenta instalar el **promotor del puerto de Cisco SSL VPN** (éste no sucede siempre) y vuelve a la página porta del clientless sin la conexión con la computadora remota. Esto es debido a la vulnerabilidad **CVE-2012-0358,** que es resuelta en el client cara por el Security Advisory de Microsoft (2695962).

  Refiera a la vulnerabilidad remota de la ejecución de códigos del dispositivo de seguridad de las 5500 Series de Cisco ASA del Cisco Security Advisory del control ActiveX adaptante del clientless VPN.Refiera al Id. de bug Cisco CSCtr00165.

Cliente de las Javas

> Nota: Cisco redistribuye los enchufes sin ningunos cambios. Debido a la licencia GNU del público general, Cisco no altera ni amplía la aplicación plugin. El enchufe del **properJavaRDP** es una aplicación de fuente abierta, y cualquier problema con el software plug-in se debe abordar por el propietario del proyecto.

- Síntomas: Las aplicaciones uso intensivas del procesador se ejecutan en la computadora remota cuando están accedidas vía el cliente de las Javas RDP, y se experimenta una caída de la Java Applet.

  Este mensaje de error pudo visualizar: **Net.propero.rdp FATAL - javax.net.ssl.SSLException: La conexión ha sido apaga: .....**El comportamiento es triggerd al conmutar entre aplicaciones dos o más Uso intensivos de la CPU rápidamente.Este problema se repara en las versiones plugs-in rdp.2012.6.4.jar y posterior. Solución alternativa:

  Conecte con el uso del cliente de ActiveX.No conmute entre las aplicaciones rápidamente.

- Síntomas: El cliente de las Javas RDP genera este mensaje de error: **net.propero.rdp.Rdp - java.net.SocketException: El socket es java.net.SocketException cerrado: El socket es cerrado, y después se cierra.**

  El problema es causado por un grupo de túnel que tenga un grupo-URL configurado con solamente el FQDN (http://www.example.com, por ejemplo).Refiera al Id. de bug Cisco CSCuh72888.Solución alternativa:

  Quite la entrada grupo-URL sin “/” en el grupo de túnel.Utilice al cliente de ActiveX.

- Síntomas: El cliente de las Javas RDP falla cuando está conectado con un ordenador de Windows 8.

  El cliente de las Javas RDP no tiene actualmente soporte para esto.Refiera al Id. de bug

Cisco CSCuc79990Solución alternativa:

Utilice al cliente de ActiveX RDP.Túnel elegante el cliente nativo de Windows RDP (**mstsc.exe).**

- Síntomas: El cliente de las Javas RDP falla con este mensaje de error: **ARSigningException: Encontró la entrada sin signo en el recurso: https://10.105.130.91/+CSCO+3a75676763663A2F2F2E637968747661662E++/vnc/VncViewer.jar**.

  Este problema es causado por un bug en el rewriter de las Javas del webVPN ASA.Refiera al Id. de bug Cisco CSCuj88114.Solución alternativa: Downgrade a la versión de Java 7u40.