ASA無客戶端SSLVPN:RDP外掛問題

目錄

簡介

本文檔為思科自適應安全裝置(ASA)無客戶端安全套接字層VPN(SSLVPN)使用者可用的遠端案頭協定(RDP)外掛的一些常見問題提供了解答。

RDP外掛只是使用者可用的外掛之一，其他外掛還包括安全外殼(SSH)、虛擬網路計算(VNC)和Citrix。RDP外掛是此集合中最常用的外掛之一。本文檔提供有關此外掛的部署和故障排除過程的更多詳細資訊。

> **附註**：本文檔沒有提供有關如何配置RDP外掛的資訊。有關詳細資訊，請參閱Cisco ASA 5500 SSL VPN部署指南8.x版。

背景資訊

RDP外掛已經從純基於Java的RDP外掛發展到包括ActiveX RDP客戶端(Internet Explorer)和Java客戶端（非Internet Explorer瀏覽器）。

Java外掛

Java RDP客戶端使用正確的Java RDP小程式。然後，Java小程式包裝在外掛中，該外掛允許在ASA無客戶端門戶中進行安裝。

Active-X外掛

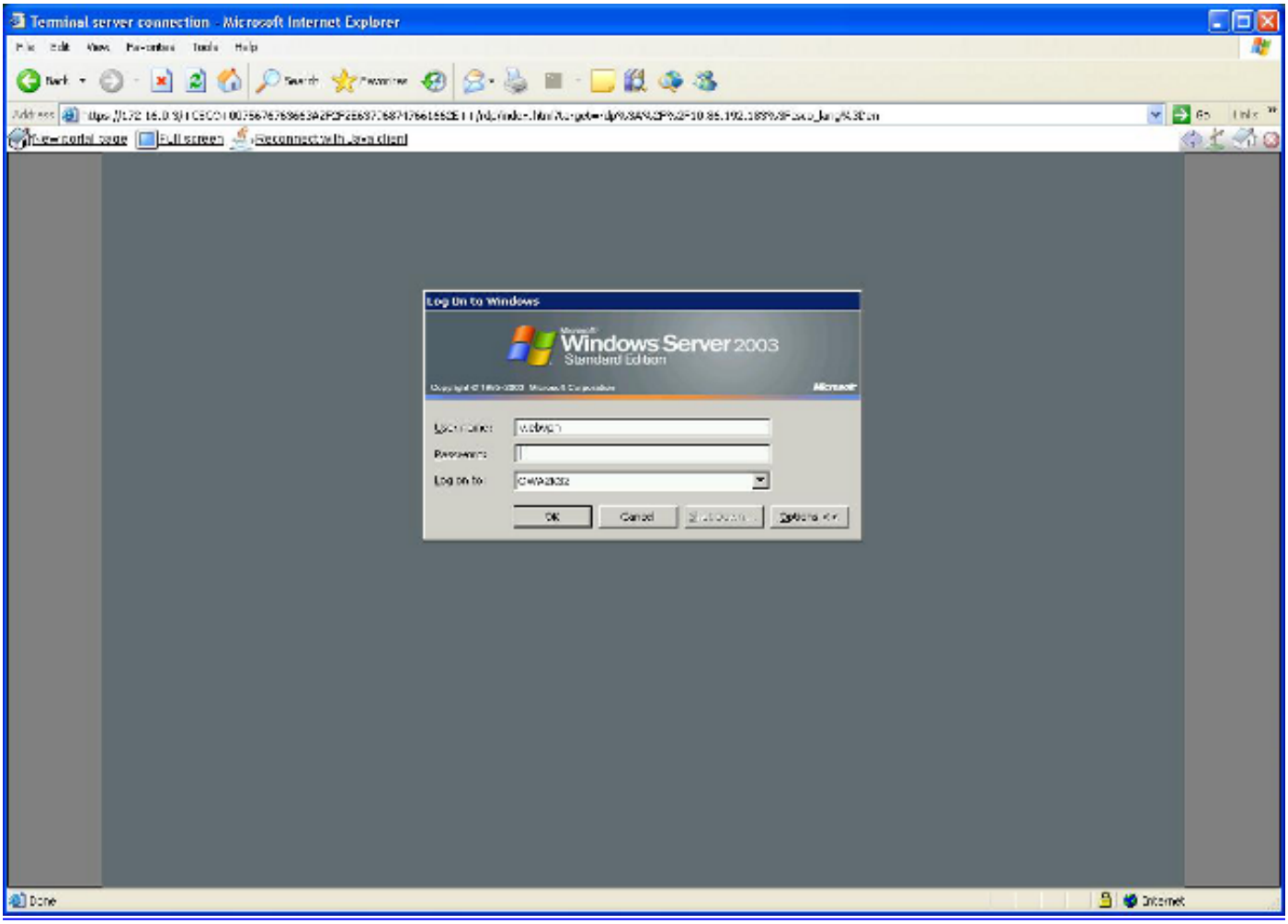
RDP外掛還包括Microsoft ActiveX RDP客戶端，外掛根據瀏覽器確定是否使用Java或ActiveX客戶端。即：

- 如果Internet Explorer(IE)使用者嘗試通過無客戶端SSLVPN門戶使用RDP，並且書籤URL不包含**ForceJava=true**引數，則使用ActiveX客戶端。如果ActiveX無法執行，則外掛會啟動Java客戶端。
- 如果非IE使用者嘗試啟動RDP書籤或URL，則僅啟動Java客戶端。

有關RDP ActiveX和USER許可權要求的詳細資訊，請參閱Microsoft Requirements for Remote Desktop Web Connection文章。

下一張圖說明了啟動外掛後可在瀏覽器視窗中選擇的三個連結：

1. **新門戶頁面** — 此連結在新瀏覽器視窗中開啟門戶頁面。
2. **全屏** — 它在全屏模式下使用RDP視窗。
3. **重新連線**Java — 這將強制外掛重新連線並使用Java而不是ActiveX。



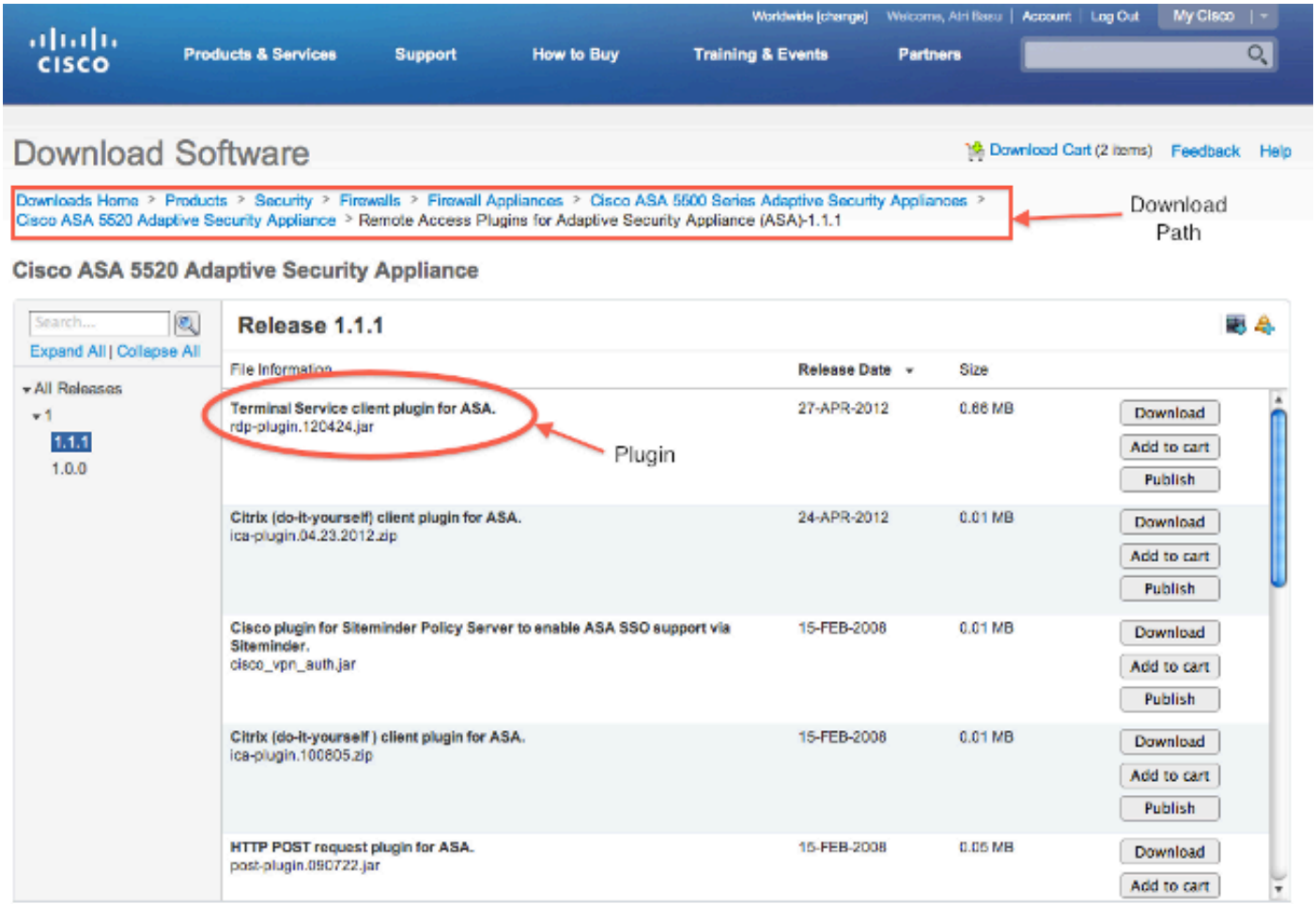
RDP外掛

RDP和RDP-2外掛使用情況

- **RDP外掛：這是**建立的原始外掛，它同時包含Java和ActiveX客戶端。
- **RDP2插**件：由於RDP協定中的更改，更新了正確的Java RDP客戶端，以支援Microsoft Windows 2003終端伺服器和Windows Vista終端伺服器。

提示：最新的RDP外掛結合了RDP和RDP2協定。因此，RDP2外掛已過時。建議使用最新版本的RDP外掛。RDP外掛名稱遵循以下結構： **rdp-plugin.yymmdd.jar**，其中**yy**是兩位數的年份格式， **mm**是兩位數的月份格式，**dd**是兩位數的日期格式。

若要下載該外掛，請訪問[思科軟體下載頁面](#)。



ActiveX與Java客戶端定位

RDP-ActiveX

- 僅使用IE
- 支援轉發的聲音

RDP-Java

- 可在所有支援Java的瀏覽器上運行。
- 僅當ActiveX無法啟動或RDP書籤中傳遞**ForceJava=true引數**時，才會在IE中啟動Java Client。
- RDP-Java實現基於Proper Java RDP專案，一個開源方案；為應用程式提供盡力支援。

RDP書籤格式

以下是RDP書籤的示例格式：

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

以下是有關格式的一些重要說明：

- **server** — 這是唯一必需的屬性。輸入託管Microsoft終端服務的電腦的名稱。
- **port**（可選） — 這是託管Microsoft終端服務的遠端電腦中的虛擬地址。預設值3389與Microsoft終端服務的公認埠號匹配。
- **parameters** — 這是一個可選的查詢字串，由引數 — 值對組成。問號將標籤引數字串的開頭，並且每個引數值對都用&號分隔。

  以下是可用引數的清單：

  幾何 — 這是客戶端螢幕的大小（畫素）(W x H)。**bpp** — 這是每畫素位數（顏色深度），8|16|24|32。**domain** — 這是登入域。**username** — 這是用於登入的使用者名稱。**password** — 這是登入密碼。請謹慎使用密碼，因為密碼在客戶端使用，可以觀察。**console** — 用於連線到伺服器上的控制**檯**會話(yes/no)。**ForceJava** — 將此引數設定為**yes**，以便只使用Java客戶端。預設設定為**no**。**shell** — 將此引數設定為與RDP連線時自動啟動的執行檔/應用程式的路徑(**rdp://server/?shell=path**)。

  以下是其他僅ActiveX引數的清單：

  RedirectDrives — 將此引數設定為**true**，以便在本地對映遠端驅動器。**RedirectPrinters** — 將此引數設定為**true**，以便在本地對映遠端印表機。**FullScreen** — 將此引數設定為**true**，以便在FullScreen模式下啟動。**ForceJava** — 將此引數設**置為**yes以強制Java客戶端。**audio** — 此引數用於通過RDP會話進行音訊轉發：

  0 — 將遠端聲音重定向到客戶端電腦。**1** — 在遠端電腦上播放聲音。**2** — 禁用聲音重定向；不在遠端伺服器上播放聲音。

RDP外掛和VPN負載平衡

使用基於域名伺服器(DNS)的全域性伺服器負載均衡支援多地[理負載均衡](#)。由於DNS結果快取差異，外掛可能在不同作業系統間運行不同。Windows DNS快取允許外掛在啟動Java小程式時解析相同的IP地址。在Macintosh(MAC)OS X上，Java小程式可以解析不同的IP地址。因此，外掛無法正確啟動。

DNS輪詢的範例是當您有單一的URL(https://www.example.com)時，**www.example.com**的DNS專案可以解析192.0.2.10(ASA1)或198.51.100.50(ASA2)。

使用者通過ASA1上的瀏覽器登入到無客戶端WebVPN門戶後，可以啟動RDP外掛。在Java客戶端啟動期間，MAC OS X電腦會執行新的DNS解析請求。使用循環DNS配置時，此第二個解析響應返回為初始WebVPN連線選擇的同一站點的可能性為50%。如果DNS伺服器響應為198.51.100.50(ASA2)而不是192.0.2.10(ASA1)，則Java客戶端發起到錯誤ASA(ASA2)的連線。 由於ASA2上不存在使用者會話，因此連線請求被拒絕。

這可能會導致類似以下內容的Java錯誤消息：

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

常見問題

為什麼某些鍵入的字元不會出現在遠端RDP會話上？

RDP會話中的遠端電腦的鍵盤區域設定可能與本地電腦不同。由於這種差異，遠端電腦可能不會顯示某些型別字元或不正確的字元。僅使用Java外掛時才會出現此行為。要解決此問題，請使用**keymap**屬性將本地金鑰對映對映到遠端PC。

例如，要設定德語鍵盤對映，請使用：

```
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
----------------------------------------------------------------------
```

鍵盤對映的已知問題

- 思科錯誤ID CSCth38454 — **實施適用於RDP外掛的匈牙利金鑰對映。**
- 思科錯誤ID CSCsu77600 - **WebVPN RDP外掛視窗金鑰不正確。Shift（鍵）。jar。**
- Cisco錯誤ID CSCtt04614 - **WebVPN - ES鍵盤數字由RDP外掛管理不正確。**
- 思科錯誤ID CSCtb07767 - **ASA外掛 — 配置預設引數。**

提示：另一種可能的解決方法是使用**mstsc.exe的應用程式智慧隧道。**在WebVPN子配置模式下使用以下命令進行配置：**smart-tunnel list RDP_List RDP mstsc.exe platform windows。**

Java RDP外掛是否支援全屏RDP會話？

目前，沒有針對全屏RDP會話的本機支援。增強請求CSCto87451已歸檔以便實現此功能。如果將**geometry**引數(例如，幾何**=1024x768**)設定為使用者監視器的解析度，則它在全屏模式下運行。由於使用者螢幕大小不同，可能需要建立多個書籤連結。ActiveX客戶端原生支援全屏RDP會話。

Java客戶端能否使用AES-256進行加密通訊？

為了允許Java客戶端正確協商SSL，請調整ASA SSL密碼集的順序以匹配以下內容：

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

如果密碼集順序不同，Java客戶端可能會顯示以下錯誤：

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

排除RDP故障

如果您遇到RDP外掛的其他問題，收集此資料以排除RDP問題可能會有幫助：

- ASA的**show tech**輸出
- **show import webvpn plug-in detailed**輸出來自ASA
- 使用者電腦作業系統和補丁級別
- 目標電腦的作業系統和修補程式級別
- 使用的客戶端（ActiveX或Java）和Java JRE版本
- 確定ASA是否位於負載平衡群集、基於DNS的群集或基於ASA的群集中

已知警告

Microsoft安全更新問題

1. KB2695962 - Microsoft安全建議：ActiveX終止位元的更新彙總：2012年5月8日。
2. KB2675157 - MS12-023:Internet Explorer累積安全更新：2012年4月10日。
3. cisco-sa-20120314-asaclient - Cisco ASA 5500系列自適應安全裝置無客戶端VPN ActiveX控制遠端代碼執行漏洞3月14日。
4. 思科錯誤ID CSCtx68075 — 應用Windows修補程式KB2585542時，ASA WebVPN中斷(8.2.5.29 / 8.4.3.9)。
5. KB2585542 - MS12-006:Windows中Webio、Winhttp和schannel的安全更新的說明：2012年1月10日。

ActiveX使用者端

- **症狀**:升級到ASA OS版本8.4.3後，ActiveX客戶端無法從IE版本6至9載入。

  請參閱Cisco錯誤ID CSCtx5856。8.4.3.4及更新版本提供此修復程式。因應措施：強制使用Java客戶端。

- **症狀**:將ASA OS版本降級到8.4.3之前的版本後，ActiveX客戶端無法載入。這會影響在ASA上使用具有思科錯誤ID CSCtx58556修復程式的ActiveX客戶端，並使用8.4.3之前的版本連線到此ASA的使用者。這是由於在ASA 8.4.3版中引入的新ActiveX RDP外掛與早期版本不相容。

  請參閱思科錯誤ID CSCtx57453。是否刪除所有Windows註**冊表例項b8e73359-3422-4384-8d27-4ea1b4c01232?**（舊的ActiveX CLSID）。

  附註：建議在進行任何編輯之前對電腦系統登錄檔進行備份。
- **症狀**:到已啟用網路層級驗證(NLA)的裝置的RDP連線失敗。

  請參閱Cisco錯誤ID CSCtu6361，瞭解請求將NLA合併到ActiveX RDP外掛的增強功能。儘管Microsoft ActiveX Client支援NLA，但不支援在ASA外掛內使用該功能。解決方法：將RDP外掛(**mstsc.exe**)配置為智慧隧道。請參閱Cisco ASA 5500 SSL VPN部署指南8.x版。

- **症狀**:ActiveX RDP無法載入，並顯示空白頁面。

  請參閱Cisco錯誤ID CSCsx49794。當ASA SSL證書的證書鏈大於四個證書（例如ROOT、SUBCA1、SUBCA2和ASA CERT）時，會發生這種情況。因應措施：

  請勿在ASA上安裝大型證書鏈。已知Java RDP外掛可正常工作，而不是ActiveX外掛。使用智慧隧道配置本地Windows **mstsc.exe**時，RDP也可以正常工作。

- **症狀**:使用ActiveX RDP客戶端後，使用者按一下**Logout**按鈕並收到**HTTP 404 - Page Not found**錯誤。請參閱Cisco錯誤ID CSCtz33266。此問題已通過外掛版本**rdp-plugin.120424.jar**或更高版本解決。

- **症狀**:使用者在IE中開啟兩個頁籤，一個用於RDP會話，另一個用於空白或其他網頁。關閉RDP頁籤後，IE無法正常運行。

  請參閱Cisco錯誤ID CSCua69129。因應措施：使用Java RDP外掛(Set **ForceJava=true**)。

- **症狀**:ActiveX外掛導致IE使用高CPU。請參閱Cisco錯誤ID CSCua16597。

- **症狀**:安裝Windows更新**KB2695962後**,ActiveX RDP外掛不載入。開啟新的RDP會話時，ActiveX客戶端會嘗試安裝**Cisco SSL VPN埠轉發器**（並非總是發生這種情況），並返回到無客戶端門戶頁面而不連線到遠端電腦。這是由於漏洞**CVE-2012-0358**，此漏洞在客戶端由Microsoft Security Advisory(2695962)解決。

  請參閱思科安全建議Cisco ASA 5500系列自適應安全裝置無客戶端VPN ActiveX控制遠端代碼執行漏洞。請參閱Cisco錯誤ID CSCtr00165。

Java使用者端

注意:思科重新分發外掛，不做任何更改。由於GNU通用公共許可證，思科不會更改或擴展外掛應用程式。**properJavaRDP外掛是一個開源應用程式，該外掛軟體的任何問題必須由專案所有者解決。**

- **症狀**:通過Java RDP客戶端訪問時，處理器密集型應用程式會在遠端電腦上運行，並且會遇到Java Applet崩潰。

  可能會顯示以下錯誤消息： **FATAL net.propero.rdp - javax.net.ssl.SSLException:連線已關閉：.....**當在兩個或更多佔用大量CPU的應用程式之間快速切換時，觸發此行為。此問題已在外掛版本rdp.2012.6.4.jar及更高版本中修復。 因應措施：

  使用ActiveX客戶端進行連線。請勿在應用程式之間快速切換。

- **症狀**:Java RDP客戶端生成以下錯誤消息： **net.propero.rdp.Rdp - java.net.SocketException:套接字已關閉java.net.SocketException:Socket關閉**，然後關閉。

  此問題是由隧道組引起的，該隧道組的組URL僅配置了FQDN(例如http://www.example.com)。請參閱Cisco錯誤ID CSCuh72888。因應措施：

  刪除tunnel-group中沒有「/」的group-URL條目。使用ActiveX客戶端。

- **症狀**:Java RDP客戶端連線到Windows 8電腦時失敗。

  Java RDP客戶端當前不支援此功能。請參閱思科錯誤ID CSCuc79990因應措施：

  使用ActiveX RDP客戶端。Windows本地RDP客戶端(**mstsc.exe**)的智慧隧道。

- **症狀**:Java RDP客戶端失敗，並顯示以下錯誤消息：**ARSigningException:在資源中找到未簽名的條目：https://10.105.130.91/+CSCO+3a75676763663A2F2F2E637968747661662E++/vnc/VncViewer.jar**。

  此問題由ASA webVPN Java重寫程式中的錯誤引起。請參閱思科錯誤ID CSCuj88114。因應措施：降級到Java 7u40版。