

ASA无客户端SSLVPN:RDP插件问题

目录

[简介](#)

[背景信息](#)

[Java插件](#)

[Active-X插件](#)

[RDP插件](#)

[RDP和RDP-2插件使用](#)

[ActiveX与Java客户端定位](#)

[RDP-ActiveX](#)

[RDP-Java](#)

[RDP书签格式](#)

[RDP插件和VPN负载均衡](#)

[常见问题](#)

[为什么某些键入的字符不显示在远程RDP会话中？](#)

[键盘映射的已知问题](#)

[Java RDP插件是否支持全屏RDP会话？](#)

[Java客户端能否使用AES-256进行加密通信？](#)

[排除RDP问题](#)

[已知问题说明](#)

[Microsoft安全更新问题](#)

[ActiveX客户端](#)

[Java客户端](#)

简介

本文档提供有关思科自适应安全设备(ASA)无客户端安全套接字层VPN(SSLVPN)用户可用的远程桌面协议(RDP)插件的一些常见问题的解答。

RDP插件仅是用户可用的插件之一，以及其他插件，如安全外壳(SSH)、虚拟网络计算(VNC)和Citrix。RDP插件是此集合中使用最频繁的插件之一。本文档提供有关此插件的部署和故障排除过程的详细信息。

注意：本文档不提供有关如何配置RDP插件的信息。有关其他信息，请参阅[Cisco ASA 5500 SSL VPN部署指南8.x版](#)。

背景信息

RDP插件已从纯基于Java的RDP插件发展为包括ActiveX RDP客户端(Internet Explorer)和Java客户端(非Internet Explorer浏览器)。

Java插件

Java RDP客户端使用适当的[Java RDP小](#)程序。然后，Java小程序将封装在允许在ASA无客户端门户中安装的插件中。

Active-X插件

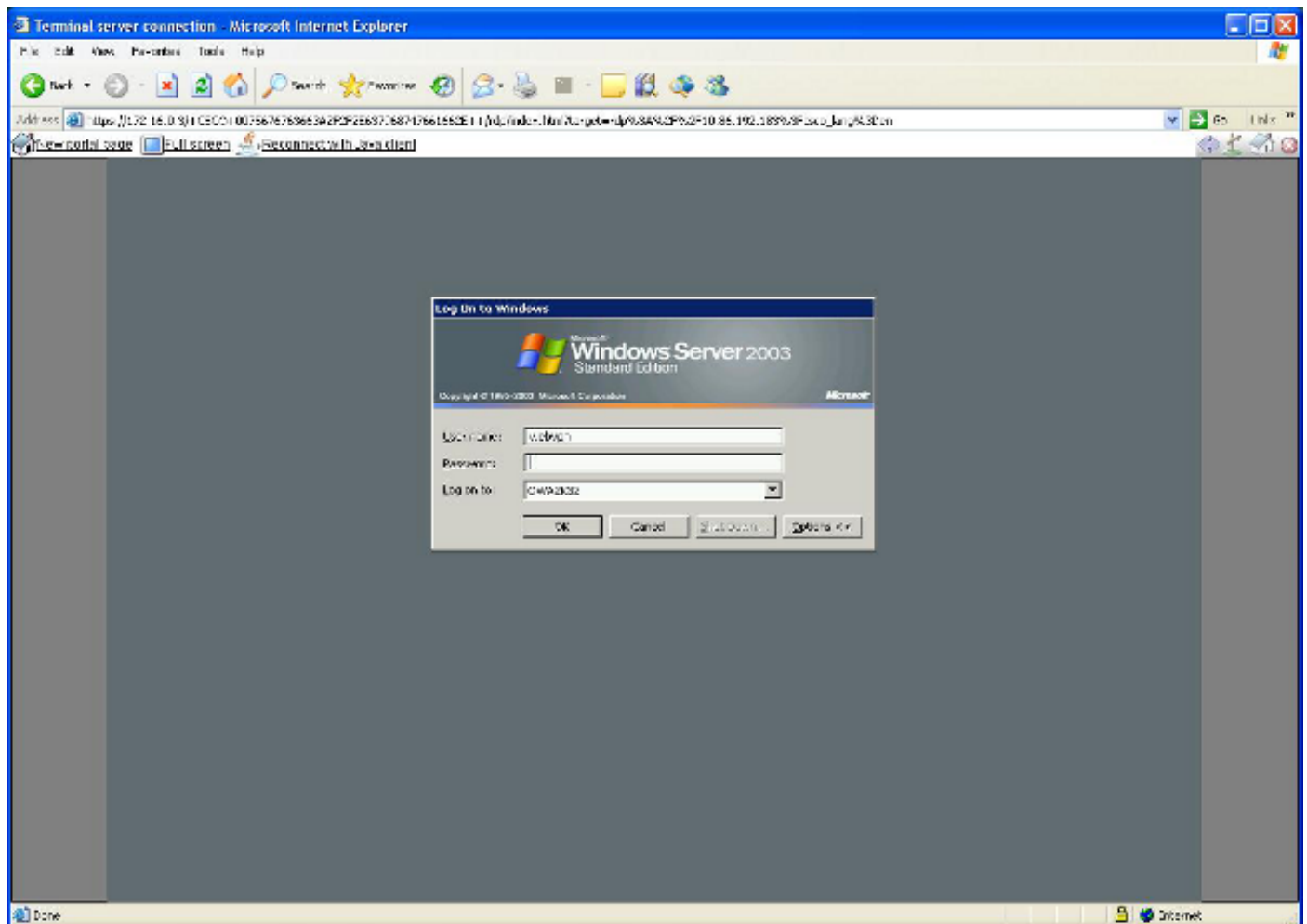
RDP插件还包括Microsoft ActiveX RDP客户端，该插件根据浏览器确定是使用Java还是ActiveX客户端。即：

- 如果Internet Explorer(IE)用户尝试通过无客户端SSLVPN门户使用RDP，且书签URL不包含**ForceJava=true**参数，则使用ActiveX客户端。如果ActiveX无法执行，则插件将启动Java客户端。
- 如果非IE用户尝试启动RDP书签或URL，则仅启动Java客户端。

有关RDP ActiveX和USER权限要求的详细信息，请参阅Microsoft[远程桌面Web连接要求](#)文章。

下一张图显示了在启动插件后可在浏览器窗口中选择的三个链接：

1. **新门户页面** — 此链接在新浏览器窗口中打开门户页面。
2. **全屏** — 在全屏模式下使用RDP窗口。
3. **重新连接Java** — 这会强制插件重新连接并使用Java而不是ActiveX。



RDP插件

RDP和RDP-2插件使用

- RDP插件：这是创建的原始插件，包含Java和ActiveX客户端。
- RDP2插件：由于RDP协议中的更改，已更新正确的Java RDP客户端以支持Microsoft Windows 2003终端服务器和Windows Vista终端服务器。

提示：最新的RDP插件将RDP和RDP2协议结合在一起。因此，RDP2插件已过时。建议使用RDP插件的最新版本。RDP插件命名法遵循以下结构：**rdp-plugin.yymmdd.jar**，其中**yy**是两位数的年格式，**mm**是两位数的月格式，**dd**是两位数的日格式。

要下载插件，请访问思科[软件下载页](#)。

The screenshot shows the Cisco Software Download page for the Cisco ASA 5520 Adaptive Security Appliance. The breadcrumb navigation path is highlighted in red and labeled "Download Path": Downloads Home > Products > Security > Firewalls > Firewall Appliances > Cisco ASA 5500 Series Adaptive Security Appliances > Cisco ASA 5520 Adaptive Security Appliance > Remote Access Plugins for Adaptive Security Appliance (ASA)-1.1.1.

The main content area is titled "Cisco ASA 5520 Adaptive Security Appliance" and "Release 1.1.1". It displays a table of plugins with the following columns: File Information, Release Date, Size, and actions (Download, Add to cart, Publish). The first row is circled in red and labeled "Plugin".

File Information	Release Date	Size	Actions
Terminal Service client plugin for ASA. rdp-plugin.120424.jar	27-APR-2012	0.86 MB	Download, Add to cart, Publish
Citrix (do-it-yourself) client plugin for ASA. ica-plugin.04.23.2012.zip	24-APR-2012	0.01 MB	Download, Add to cart, Publish
Cisco plugin for Siteminder Policy Server to enable ASA SSO support via Siteminder. cisco_vpn_auth.jar	15-FEB-2008	0.01 MB	Download, Add to cart, Publish
Citrix (do-it-yourself) client plugin for ASA. ica-plugin.100805.zip	15-FEB-2008	0.01 MB	Download, Add to cart, Publish
HTTP POST request plugin for ASA. post-plugin.090722.jar	15-FEB-2008	0.05 MB	Download, Add to cart

ActiveX与Java客户端定位

RDP-ActiveX

- 仅使用IE
- 支持转发的声音

RDP-Java

- 在所有支持Java的浏览器上工作。
- 仅当ActiveX无法启动或ForceJava=true参数在RDP书签中传递时，才在IE中启动Java客户端。
- RDP-Java实现基于Proper Java RDP项目，这是一个开源计划；为应用提供尽力支持。

RDP书签格式

以下是RDP书签的示例格式：

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

以下是有关格式的一些重要说明：

- **server** — 这是唯一必需的属性。输入托管Microsoft终端服务的计算机的名称。
- **port** (可选) — 这是托管Microsoft终端服务的远程计算机中的虚拟地址。默认值3389与Microsoft终端服务的公认端口号匹配。
- **parameters** — 这是由参数 — 值对组成的可选查询字符串。问号用于标记参数字符串的开头，每个参数值对都用与号分隔。

以下是可用参数列表：

geometry — 这是客户端屏幕的大小(以像素 (宽x高) 为单位)。**bpp** — 这是每像素位 (颜色深度)，8|16|24|32。**domain** — 这是登录域。**username** — 这是登录的用户名。**password** — 这是登录密码。小心使用密码，因为密码在客户端使用，可以观察。**console** — 用于连接到服务器上的控制台会话 (是/否)。**ForceJava** — 将此参数设置为yes，以便仅使用Java客户端。默认设置为否。**shell** — 将此参数设置为在您连接RDP时自动启动的可执行/应用程序的路径(例如rdp://server/?shell=path)。

以下是其他仅ActiveX参数的列表：

RedirectDrives — 将此参数设置为true，以便在本地映射远程驱动器。**RedirectPrinters** — 将此参数设置为true，以便在本地映射远程打印机。**全屏** — 将此参数设置为true，以便在全屏模式下启动。**ForceJava** — 将此参数设置为yes以强制Java客户端。**audio** — 此参数用于通过RDP会话进行音频转发：

0 — 将远程声音重定向到客户端计算机。1 — 在远程计算机上播放声音。2 — 禁用声音重定向；不在远程服务器上播放声音。

RDP插件和VPN负载均衡

使用基于域名服务器(DNS)的全局服务器负载均衡可支持多地[地理位置负载均衡](#)。由于DNS结果缓存差异，插件在不同操作系统中的运行可能会有所不同。Windows DNS缓存允许插件在启动Java小程序时解析相同的IP地址。在Macintosh(MAC)OS X上，Java小程序可以解析不同的IP地址。因此，插件无法正确启动。

DNS轮询的一个示例是，当您有单个URL(<https://www.example.com>)时，**www.example.com**的DNS条目可以解析192.0.2.10(ASA1)或198.51.100.50(ASA2)。

在用户通过ASA1上的浏览器登录到无客户端WebVPN门户后，可以启动RDP插件。在启动Java客户端期间，MAC OS X计算机执行新的DNS解析请求。使用轮询DNS配置时，此第二个解析响应返回为初始WebVPN连接选择的同一站点的可能性为50%。如果DNS服务器响应是198.51.100.50(ASA2)，而不是192.0.2.10(ASA1)，则Java客户端会发起到错误ASA(ASA2)的连接。由于ASA2上不存在用户会话，因此连接请求被拒绝。

这可能会导致Java错误消息类似如下：

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

常见问题

为什么某些键入的字符不显示在远程RDP会话中？

RDP会话中的远程计算机可能具有与本地计算机不同的键盘区域设置。由于这种差异，远程计算机可能不显示某些键入的字符或不正确的字符。只有使用Java插件时，才会看到此行为。要解决此问题，请使用**keymap**属性将本地密钥映射映射到远程PC。

例如，要设置德语键盘映射，请使用：

```
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
-----
```

键盘映射的已知问题

- Cisco Bug ID CSCth38454 -为RDP插件实施匈牙利密钥映射。
- Cisco Bug ID CSCsu77600 - WebVPN RDP插件窗口密钥不正确。Shift (键)。jar。
- Cisco Bug ID CSCtt04614 - WebVPN - ES键盘符号被RDP插件错误管理。
- Cisco Bug ID CSCtb07767 - ASA插件 — 配置默认参数。

提示：另一个可能的解决方法是为mstsc.exe使用应用智能隧道。这是在WebVPN子配置模式下使用以下命令进行配置的：**smart-tunnel list RDP_List RDP mstsc.exe**平台窗口。

Java RDP插件是否支持全屏RDP会话？

目前，不支持全屏RDP会话。为了实施此功能，已提交增强请求CSCto87451。如果将几何参数(几何=1024x768，例如)设置为用户监视器的分辨率，则它在全屏模式下运行。由于用户屏幕大小不同，可能需要创建多个书签链接。ActiveX客户端本机支持全屏RDP会话。

Java客户端能否使用AES-256进行加密通信？

为了允许Java客户端正确协商SSL，请调整ASA SSL密码集的顺序以匹配以下项：

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

如果密码集顺序不同，Java客户端可能会显示此错误：

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

排除RDP问题

如果您遇到RDP插件的其他问题，收集此数据以排除RDP问题可能会很有用：

- ASA的show tech输出
- ASA的show import webvpn plug-in详细输出
- 用户计算机操作系统和补丁级别
- 目标计算机操作系统和补丁级别
- 使用的客户端 (ActiveX或Java) 和Java JRE版本
- 确定ASA是在负载均衡集群、基于DNS还是基于ASA

已知问题说明

Microsoft安全更新问题

1. [KB2695962](#) - Microsoft安全建议：ActiveX终止位的更新汇总：2012年5月8日。
2. [KB2675157](#) - MS12-023:Internet Explorer的累积安全更新：2012年4月10日。
3. [cisco-sa-20120314-asaclient](#) - Cisco ASA 5500系列自适应安全设备无客户端VPN ActiveX控制远程代码执行漏洞3月14日。
4. 思科漏洞ID CSCtx68075 — 应用Windows补丁KB2585542时ASA WebVPN中断(8.2.5.29 / 8.4.3.9)。
5. [KB2585542](#) - MS12-006:Windows中Webio、Winhttp和Schannel的安全更新说明：2012年1月10日。

ActiveX客户端

- **症状**：升级到ASA OS版本8.4.3后，ActiveX客户端无法从IE版本6到9加载。

请参阅Cisco Bug ID [CSCtx58556](#)。此修复程序适用于8.4.3.4及更高版本。解决方法：强制使用Java客户端。

- **症状**：ASA OS版本降级到8.4.3之前的版本后，ActiveX客户端无法加载。这影响在ASA上使用ActiveX客户端并修复思科Bug ID CSCtx58556，并使用8.4.3之前的版本连接到此ASA的用户。这是由于新的ActiveXASA 8.4.3版中引入的RDP插件，与早期版本不兼容。

请参阅Cisco Bug ID CSCtx57453 (仅限注册用户)。是否删除b8e73359-3422-4384-8d27-4ea1b4c01232的所有Windows注册表实例？(旧ActiveX CLSID)。

注意：建议在进行任何编辑之前对计算机系统注册表执行备份。

- **症状**：与启用网络级身份验证(NLA)的设备的RDP连接失败。

有关请求将NLA纳入ActiveX RDP插件的增强功能，[请参阅Cisco Bug ID CSCtu63661 \(仅限注册用户 \)](#)。虽然Microsoft ActiveX客户端支持NLA，但不支持在ASA插件内使用该功能。解决方法：将RDP插件(mstsc.exe)配置为智能隧道。请参阅[Cisco ASA 5500 SSL VPN部署指南，版本8.x](#)。

- **症状**：ActiveX RDP无法加载，并显示空白页。

请参阅Cisco Bug ID [CSCsx49794](#)。当ASA SSL证书的证书链大于四个证书 (例如ROOT、SUBCA1、SUBCA2和ASA CERT) 时，会发生这种情况。解决方法：

请勿在ASA上安装大型证书链。已知Java RDP插件工作正常，而ActiveX插件不工作。当您使用智能隧道配置本地Windows mstsc.exe时，RDP也能正常工作。

- **症状**：使用ActiveX RDP客户端后，用户单击“注销”按钮，并收到HTTP 404 - Page Not Found错误。请参阅Cisco Bug ID CSCtz33266。此问题已通过插件版本rdp-plugin.120424.jar或更高版本得到解决。

- **症状**：用户在IE中打开两个选项卡 — 一个用于RDP会话，另一个用于空白或其他网页。关闭RDP选项卡后，IE无法正确运行。

请参阅Cisco Bug ID [CSCua69129](#)。解决方法：使用Java RDP插件(设置ForceJava=true)。

- **症状**：ActiveX插件导致IE的CPU使用率较高。请参阅Cisco Bug ID [CSCua16597](#)。

- **症状**：安装Windows更新KB2695962后,ActiveX RDP插件不加载。当打开新的RDP会话时，ActiveX客户端尝试安装Cisco SSL VPN端口转发器 (这并不总是发生) 并返回到无客户端门户页面，而不连接到远程计算机。这是由于漏洞CVE-2012-0358,Microsoft安全顾问(2695962)在[客户端解决了该漏洞](#)。

请参阅思科安全顾问[Cisco ASA 5500系列自适应安全设备无客户端VPN ActiveX控制远程代码执行漏洞](#)。请参阅Cisco Bug ID [CSCtr00165](#)。

Java客户端

注意: Cisco重新分发插件而不进行任何更改。由于GNU通用公共许可证, 思科不会更改或扩展插件应用。properJavaRDP 插件是一个开源应用程序, 任何与插件软件有关的问题都必须由项目所有者解决。

- **症状**: 当通过Java RDP客户端访问时, 处理器密集型应用程序在远程计算机上运行, 并且出现Java小程序崩溃。

此错误消息可能显示:**FATAL net.propero.rdp - javax.net.ssl.SSLException:连接已关闭**:在两个或多个CPU密集型应用之间快速切换时触发该行为。此问题已在插件版本 rdp.2012.6.4.jar及更高版本中解决。解决方法:

使用ActiveX客户端进行连接。请勿在应用程序之间快速切换。

- **症状**: Java RDP客户端生成以下错误消息: **net.propero.rdp.rdp - java.net.SocketException:套接字已关闭java.net.SocketException:套接字关闭**, 然后关闭。

此问题是由仅配置了FQDN(例如http://www.example.com)的group-url的隧道组引起的。请参阅Cisco Bug ID [CSCuh72888](#)。解决方法:

删除隧道组中没有"/"的group-URL条目。使用ActiveX客户端。

- **症状**: Java RDP客户端连接到Windows 8计算机时失败。

Java RDP客户端当前不支持此功能。请参阅Cisco Bug ID CSCuc79990解决方法:

使用ActiveX RDP客户端。智能隧道Windows本地RDP客户端(mstsc.exe)。

- **症状**: Java RDP客户端失败, 并显示以下错误消息: **ARSigningException:在资源中找到未签名的条目**
: https://10.105.130.91/+CSCO+3a75676763663A2F2F2E637968747661662E++/vnc/VncViewer.jar。

此问题是由ASA webVPN Java重写程序中的Bug引起的。请参阅Cisco Bug ID [CSCuj88114](#)。
解决方法: 降级到Java版本7u40。