ASA 无客户端 SSL VPN (WebVPN) 故障排除技 术说明

目录

简介 先决条件 要求 使用的组件 规则 故障排除 ASA 版本 7.1/7.2 无客户端 ASA 版本 8.0 无客户端 程序 将 ASA 添加为可信站点 启用 Cookie 清除浏览器缓存 清除 Java 缓存 启用 Java 小程序调试选项 启用 HTML 捕获工具 相关信息

<u>简介</u>

本文档列出了ASA版本7.1、7.2和8.0采用的无客户端SSL VPN(WebVPN)故障排除技术。这些版本 之间有显着的改进,需要采用各种故障排除技术。

<u>先决条件</u>

<u>要求</u>

本文档没有任何特定的要求。

<u>使用的组件</u>

本文档中的信息基于运行软件版本 7.1 或更高版本的 Cisco 5500 系列 ASA。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息,请参阅 Cisco 技术提示规则。

<u>故障排除</u>

在 ASA 上排除无客户端 SSL VPN 连接 (Webvpn) 故障的目的,是为了通过屏幕截图和 HTML 捕获 工具以了解客户端体验,然后将此体验与直接连接要访问的 URL/应用程序时的相同信息进行比较。

ASA 版本 7.1/7.2 无客户端

本部分介绍了适用于 ASA 版本 7.1/7.2 和所有过渡版本的故障排除技术,但不包括 8.0 版本。

在此版本中,如果无法使用复杂的 Java 或 Javascript 功能,可以考虑使用其他选项(例如应用程 序访问端口转发或使用代理旁路)。有关这些替代方案的详细信息,请参阅<u>配置应用程序访问和使</u> <u>用代理旁路。</u>

在多数情况下,如果 Internet Explorer 无法访问可以通过无客户端 SSL VPN 访问的 URL,则使用 其他浏览器也将无法访问。

为确保此行为与客户端 PC 或操作系统无关,请从其他位置使用另一个客户端进行访问。您还可以 测试 lpsec 或 SSL VPN 客户端的使用。

请确保按照"在浏览器中启用 WebVPN 的 Cookie"的说明将 ASA 包含到<u>浏览器可信区域中,并按照</u> <u>启用 Cookie</u> 的说明启用 Cookie。

如果此过程仍失败,请执行以下步骤以采集必要信息,然后打开 TAC 案例。

- 1. 按照清除浏览器缓存的说明清除浏览器缓存。
- 2. 按照<u>清除 Java 缓存</u>的说明清除 Java 缓存。
- 3. 按照<u>配置缓存</u>的说明在 ASA 上禁用 Webvpn 缓存。
- 如果存在 Java 小程序,请按照<u>启用 Java 小程序调试选项</u>的说明在小程序窗口中使用调试级 别 5。
- 5. 通过无客户端 SSL VPN 登录 ASA。
- 6. 在问题 URL 之前的 URL 上,按照<u>启用 HTML 捕获工具</u>的说明在浏览器中启用 HTML 捕获工 具。
- 7. 捕获从此点发往问题 URL 的序列。
- 8. 按键盘上的 Ctrl+Print Screen 以捕获屏幕截图。
- 9. 停止 HTML 捕获工具。
- 10. 当您使用 Ipsec 或 SSL VPN 会话通过 ASA 直接连接到 URL 时,请执行相同的第 1 步至第 9 步;或是直接连接相同 LAN 网段(如果可能),然后将数据发送到 TAC 以供分析。

ASA 版本 8.0 无客户端

本部分介绍用于 ASA 版本 8.0 和所有过渡版本的故障排除技术。

在此版本中,如果无法通过无客户端 SSL VPN 使用复杂的 URL 或应用程序,则可以考虑使用其他选项(例如使用智能隧道)。有关智能隧道的详细信息,请参阅<u>配置智能隧道访问。</u>

您也可以考虑使用应用程序访问端口转发或使用代理旁路。有关这些替代方案的详细信息,请参阅 <u>配置应用程序访问和使用代理旁路。</u> 在多数情况下,如果 Internet Explorer 无法访问可以通过无客户端 SSL VPN 访问的 URL,则使用 其他浏览器也将无法访问。

为确保此行为与客户端 PC 或操作系统无关,请从其他位置使用另一个客户端进行访问。您还可以 测试 lpsec 或 SSL VPN 客户端的使用。

请确保按照"在浏览器中启用 WebVPN 的 Cookie"的说明将 ASA 包含到<u>浏览器可信区域中,并按照</u> <u>启用 Cookie</u> 的说明启用 Cookie。

如果应用程序遇到无客户端内容转换引擎 (CTE/rewriter) 的问题,您可以修改此应用程序的书签以 启用"智能隧道"选项,如下图所示:

Configuration	n > Remote Access VPN >	Clientless SSL VPN Access > Portal > B	ookmarks
Configure l	bookmark lists that the security	appliance displays on the SSL VPN portal page.	
🔂 Add	🗹 Edit 📋 Delete 🛛 🕂 In	nport 🗹 Export	
		Bookmarks	
Template		Doormano	
Test_Sites	5		
🔂 Edit	Bookmark List		x
Bookma	ark List Name: Test_Sites		
	Name	URL	Add
Hotma	il .	http://www.hotmail.com	Edit
Yahoo	Mail	http://www.mail.yahoo.com	EUIC
1	dit Bookmark Entry		×
В	ookmark Title: Hotmail		
- L	IRL Value: http	💌 :// www.hotmail.com	
	Advance <mark>d</mark> Options		*
	Subtitle:		
	Thumbnail:	None Manage	e
	URL Method :	⊙ Get C Post	
	Enable Favorite Option:	⊙ Yes C No	
	Enable Smart Tunnel Option:	⊙ Yes ○ No	

为书签启用此选项不需要其他额外的配置。与端口转发类似,您可以通过单击书签打开一个新窗口 ,以使用智能隧道传递应用程序流量并避免重写问题,这也是一种简单的办法。

当您对TCP Winsock 32应用程序(如RDP)使用此功能时,管理员需要确定要通过智能隧道使用的

进程。例如,RDP 使用 mstsc.exe 进程;您可以为此进程创建一个简单的智能隧道条目。

更复杂的应用程序可能产生多个进程。从 Webvpn 门户页中,选择 **Application Access 面板。**当它 装载时,*allowed applications 列表将连接到网络的专用部分。*

如果此过程仍失败,请执行以下步骤以采集必要信息,然后打开 TAC 案例。

- 1. 按照清除浏览器缓存的说明清除浏览器缓存。
- 2. 按照<u>清除 Java 缓存</u>的说明清除 Java 缓存。
- 3. 按照<u>配置缓存</u>的说明在 ASA 上禁用 Webvpn 缓存。
- 如果存在 Java 小程序,请按照<u>启用 Java 小程序调试选项</u>的说明在小程序窗口中使用调试级 别 5。
- 5. 通过无客户端 SSL VPN 登录 ASA。
- 6. 在问题 URL 之前的 URL 上,按照<u>启用 HTML 捕获工具</u>的说明在浏览器中启用 HTML 捕获工 具。
- 7. 捕获从此点发往问题 URL 的序列。
- 8. 按键盘上的 Ctrl+Print Screen 以捕获屏幕截图。
- 9. 停止 HTML 捕获工具。
- 10. 当您使用 Ipsec 或 Any Connect SSL 会话通过 ASA 直接连接到 URL 时,请执行相同的第 1 步至第 9 步;或是直接连接相同 LAN 网段(如果可能),执行以下步骤,然后将数据发送到 TAC 以供分析。

<u>程序</u>

将 ASA 添加为可信站点

当您在 Internet Explorer 中访问 ASA 时,如果此站点未包含在可信站点列表中,您将收到一条验证 错误。



执行以下步骤以将 ASA 添加为可信站点:

- 1. 在 Interent Explorer 中,选择工具 > Internet 选项。
- 2. 单击安全选项卡,然后选择"可信站点"。

Internet Options
General Security Privacy Content Connections Programs Advanced
Select a zone to view or change security settings.
🥥 🗐 🗸 🚫
Internet Local intranet Trusted sites Restricted sites
Trusted sites This zone contains websites that you trust not to damage your computer or your files.
Security level for this zone
Custom Custom settings. - To change the settings, click Custom level. - To use the recommended settings, click Default level.
Custom level Default level
Reset all zones to default level
OK Cancel Apply

3. 单击**站点**。

4. 添加 ASA 的 https:// 地址,然后单击**添加**。

Trusted sites		-	×
You can add a this zone will u	nd remove websites from this zo se the zone's security settings.	ne. All websites ir	1
Add this website to the	zone:		
https://asa.com/		Add)
Websites:			
		Remove	
Require server verif	ication (https:) for all sites in thi	s zone	
		Close)
			 Trusted sites
添加站点后,"可信站点	"图标将显示在 Internet Explor	rer 状态栏中。	5

注意:有关此过<u>程的详细信息,请参</u>阅使用Internet Explorer 6安全设置。

<u> 启用 Cookie</u>

执行以下步骤以启用 Cookie:

- 1. 在 Interent Explorer 中,选择**工具 > Internet 选项**。
- 2. 单击隐私选项卡,然后单击"高级"。

Internet Options					2 🛛
General Security	Privacy	Content	Connections	Programs	Advanced
Settings					
To set setting	a standar Is, click the	d privacy k e Default b	evel instead of utton.	using custo	m
Cust	om				
- Ac	lvanced o	r imported	settings		
and the second sec					
Sites	Imp	oort	Advanced	De	fault
Pop-up Blocker – Prever Appear	nt most po ring.	p-up windo	ows from	Set	tings
Tur	- n on Pop-I	up Blocker			
		Ok	: Ca	ancel	Apply

3. 在"高级隐私设置"对话框中,选中替代自动 cookie 处理复选框,单击"接受"单选按钮,然后单

	Advanced Privacy Settings
	You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.
	Cookies Override automatic cookie handling
	First-party Cookies Third-party Cookies O Accept O Accept O Block O Block
	Prompt Prompt Always allow session cookies
击"确定"。	OK Cancel

<u>清除浏览器缓存</u>

执行以下步骤以清除 Internet Explorer 的缓存:

1. 在 Interent Explorer 中,选择**工具 > Internet 选项**。

Internet Options
General Security Privacy Content Connections Programs Advanced
Home page
To create home page tabs, type each address on its own line.
Use <u>c</u> urrent Use de <u>f</u> ault Use <u>b</u> lank
Browsing history
Delete temporary files, history, cookies, saved passwords, and web form information.
Delete Search
Change search defaults. Settings
Tabs
Change how webpages are displayed in <u>Settings</u> tabs.
Appearance
Colors Languages Fonts Accessibility
OK Cancel <u>Apply</u>

2. 在"常规"选项卡中,单击"浏览历史记录"部分中的删除。

Delete Brows	ing History	
Temporary Copies of wel are saved for	Internet Files bpages, images, and media that Delete files r faster viewing.	
Cookies Files stored o save preferer	n your computer by websites to Delete cookies	
History List of websit	es you have visited. Delete history	
Form data Saved inform forms.	ation that you have typed into Delete forms	
Passwords Passwords th you log on to visited. About deletin	at are automatically filled in when Delete passwords a website you've previously Delete all Close	
	Delate Resuring History	×
	Are you sure you want to delete all Internet Explorer browsing history?	
_ 击 全部删除 。		

- 4. 选中同时删除加载项存储的文件和设置复选框,然后单击"是"。
- 5. 清除缓存后,关闭所有浏览器实例,然后重新启动浏览器。
- **注意:**要清除其他浏览器的缓存,请参阅<u>如何清除浏览器的缓存(以提高其性能)?</u>

<u>清除 Java 缓存</u>

3.

执行以下步骤以清除 Java 缓存:

- 1. 从 Windows"开始"菜单中选择控制面板。
- 2. 双击 **Java**。

🛓 Java Control Panel 🔄 🗖 🔀
General Update Java Security Advanced
About View version information about Java Control Panel.
About
Network Settings
Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.
Network Settings
Temporary Internet Files
Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.
Settings View
OK Cancel Apply

- 3. 单击**设置**。
- 4. 单击**删除文件**。

Select the locati	on where temporary files a	ire kept:	
ettings\rdavies\	Application Data\Sun\Java	\Deployment\cache	Change
Select the comp Set the amount	ression level for JAR files; of disk space for storing te	None mporary files:	000
		1	000 拿

注意:请参<u>阅如何清除Java缓存?</u>。

<u>启用 Java 小程序调试选项</u>

执行以下步骤以启用 Java 小程序调试选项:

1. 确保启用 Java 1.4 或更高版本:从 Windows"开始"菜单中选择**控制面板。**双击 **Java**。单击**关 于**,然后检查版本号。

🛃 Java Control Panel 🔄 🗖 🔀
General Update Java Security Advanced
About View version information about Java Control Panel.
About
Network Settings
Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.
Network Settings
Temporary Internet Files
Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.
Settings View
OK Cancel Apply

About Java			
	Java [™] Platform, Standard Edition 6	Java ⁻	
Version 6 Update Copyright 2008 9 All rights reserve For more inform applications, visit	5 (build 1.6.0_05-b13) Sun Microsystems, Inc. d. Use is subject to license terms. ation about Java technology and to explore gr t <u>http://www.java.com</u>	eat Java	
Sun.		Close	
		Ciose	注音・您可以以

http://java.com/en/下载Java<u>更新</u>。

2. 确保将 Java 配置为启用追踪、显示控制台并将 Microsoft Internet Explorer 设置为默认浏览器

a Java Control Panel
General Update Java Security Advanced
Settings
Enable tracing
Enable logging
Show applet lifecycle exceptions
🚊 - Java console
Show console
O Hide console
🛄 🔘 Do not start console
🖨 - Default Java for browsers
Microsoft Internet Explorer
加玉 図 元 テ・ Mozilla family
MF図/N小 . L

- 3. 确保按照<u>清除 Java 缓存</u>的说明清除 Java 缓存。
- 4. 在 Internet Explorer 中,选择**工具 > JAVA 控制台以打开 Java 调试窗口。**

🖆 Java Console	
Java Plug-in 1.6.0_05 Using JRE version 1.6.0_05 Java HotSpot(TM) Client VM User home directory = C:\Documents and Settings\rdavies network: Loading user-defined proxy configuration network: Done. network: Loading proxy configuration from Internet Explorer network: Done. network: Loading direct proxy configuration network: Done. network: Done. network: Proxy Configuration: No proxy	
 c: clear console window f: finalize objects on finalization queue g: garbage collect h: display this help message l: dump classloader list m: print memory usage o: trigger logging p: reload proxy configuration q: hide console r: reload policy configuration s: dump system and deployment properties t: dump thread list v: dump thread stack x: clear classloader cache 0-5: set trace level to <n></n> 	
<u>Clear</u> Copy Clos <u>e</u>	

- 5. 打开 JAVA 控制台调试窗口后,按 **5 以设置跟踪级别**当访问包含 Java 小程序的 URL 时,在 此窗口中将会捕获此活动。
- 6. 单击复制以复制信息。

<u> 启用 HTML 捕获工具</u>

有多种 HTML 捕获工具可用于收集数据,其中一些工具已在此处列出。在客户端 PC 上安装以下一种 HTML 捕获工具以用于练习收集数据:

- HttpWatch
- IE Inspector
- Debug Proxy

注意:此过程使用HTTPWatch应用。

安装此应用程序后,请执行以下步骤:

1. 按 Shift+P+F+2 或单击浏览器窗口中的图标以启用 HTTPWatch。

🙆 MSN.com - Microsoft Internet Explorer		_ 🗖 🗖 🔀
😋 🕤 👻 http://www.msn.com/	Google	P -
😪 🛠 📢 MSN.com	• 🖶 • 🔂 Page • 🍈 Tools • 🔞 • 😰 🦃 🎎	8 🏢 🧇

2. 启用此应用程序后,浏览器窗口底部将会出现一个嵌入式窗口,如下图所示

×	Record	🔜 Stop	Clear	🔚 View 🔹 🎯 Summary	🔍 Find	- 🔻 Filte	er ▼	Save -	😗 Help 👻
	Started 4	- Ti	me Chart		1	Time	Sent	Received	Method

3. 单击记录以记录数据;单击停止以停止记录。

注意:建议使用HttpWatch 7.x来记录数据。

相关信息

- ASA 上的无客户端 SSL VPN (WebVPN) 配置示例
- <u>Cisco ASA 5500 系列自适应安全设备</u>
- <u>技术支持和文档 Cisco Systems</u>