ASA Clientless SSL VPN (WebVPN) Technische Hinweise zur Fehlerbehebung

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Fehlerbehebung ASA Version 7.1/7.2 Clientless ASA Version 8.0 - Clientless Verfahren Hinzufügen der ASA als vertrauenswürdiger Standort Cookies aktivieren Löschen des Browser-Cache Löschen des Java-Cache Java Applet Debugoptionen aktivieren Aktivieren der HTML-Erfassungstools Zugehörige Informationen

Einführung

In diesem Dokument werden die Techniken zur Clientless-SSL-VPN-Fehlerbehebung (WebVPN) aufgeführt, die für die ASA-Versionen 7.1, 7.2 und 8.0 verwendet wurden. Zwischen diesen Versionen gibt es bedeutende Fortschritte, für die unterschiedliche Fehlerbehebungsverfahren erforderlich sind.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Serie ASA 5500, auf der die Softwareversion 7.1 oder höher ausgeführt wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten

Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Fehlerbehebung

Voraussetzung für die Fehlerbehebung bei Clientless-SSL-VPN-Verbindungen (WebVPN) auf der ASA ist die Transparenz der Client-Umgebung über Screenshots und HTML-Erfassungstools. Diese Informationen können dann mit den gleichen Informationen verglichen werden, wenn eine Verbindung direkt mit der URL/Anwendung besteht, auf die zugegriffen wird.

ASA Version 7.1/7.2 Clientless

In diesem Abschnitt werden die Fehlerbehebungsverfahren für die ASA-Versionen 7.1/7.2 und alle Interims bis zur Version 8.0 beschrieben.

Wenn komplexe Java/Javascript-Funktionen Schwierigkeiten haben, können in dieser Version auch andere Optionen (wie z.B. die Weiterleitung von Anwendungs-Access-Ports oder die Verwendung von Proxy-Bypass) in Betracht gezogen werden. Weitere Informationen zu diesen Alternativen finden Sie unter Konfigurieren des Anwendungszugriffs und Verwenden des Proxyumgehens.

Wenn die URL, auf die über Clientless-SSL-VPN zugegriffen wird, in den meisten Szenarien für Internet Explorer fehlschlägt, schlägt sie auch für einen anderen Browser fehl.

Um sicherzustellen, dass dies nicht vom Client-PC oder Betriebssystem abhängig ist, verwenden Sie einen anderen Client von einem anderen Standort. Die Verwendung eines IPsec- oder SSL VPN-Clients kann ebenfalls getestet werden.

Stellen Sie sicher, dass die ASA im <u>Browser Trusted Zone</u> enthalten ist, wie unter <u>Aktivieren von</u> <u>Cookies in Browsern für WebVPN</u> beschrieben, und dass Cookies aktiviert sind, wie unter <u>Cookies</u> <u>aktivieren</u> beschrieben.

Wenn der Vorgang immer noch fehlschlägt, führen Sie diese Schritte aus, um die erforderlichen Informationen zu sammeln, und öffnen Sie dann ein TAC-Ticket.

- 1. Löschen Sie den Browser-Cache wie unter Löschen des Browser-Cache beschrieben.
- 2. Löschen Sie den Java-Cache wie unter Löschen des Java-Cache beschrieben.
- 3. Deaktivieren Sie den WebVPN-Cache auf der ASA, wie unter <u>Konfigurieren der</u> <u>Zwischenspeicherung</u> beschrieben.
- 4. Wenn ein Java-Applet vorhanden ist, verwenden Sie Debug Level 5 im Appletfenster, wie unter <u>Optionen zum Aktivieren von Java-Applet-Debugging</u> beschrieben.
- 5. Melden Sie sich über SSL VPN ohne Client bei der ASA an.
- 6. Aktivieren Sie bei der URL direkt vor der problematischen URL ein HTML-Erfassungstool im Browser, wie unter <u>Aktivieren der HTML-Erfassungstools</u> beschrieben.

- 7. Erfassen Sie die Sequenz von diesem Punkt bis zur problematischen URL.
- 8. Drücken Sie Strg+Druck auf Ihrer Tastatur, um einen Screenshot aufzunehmen.
- 9. Beenden Sie das HTML-Erfassungstool.
- 10. Führen Sie die gleichen Schritte 1 bis 9 durch, wenn Sie entweder über eine IPsec- oder SSL-VPN-Sitzung über die ASA eine direkte Verbindung mit der URL herstellen oder (wenn möglich) eine direkte Verbindung mit demselben LAN-Segment herstellen und die Daten zur Analyse an das TAC senden.

ASA Version 8.0 - Clientless

In diesem Abschnitt werden die Fehlerbehebungsverfahren für ASA Version 8.0 und alle Interims beschrieben.

Wenn komplexe URLs oder Anwendungen durch clientloses SSL VPN Schwierigkeiten haben, sind in dieser Version andere Optionen (z. B. die Verwendung intelligenter Tunnel) eine leistungsstarke Alternative. Weitere Informationen zu Smart Tunnels finden Sie unter Konfigurieren des Smart Tunnel Access.

Sie können auch die Weiterleitung von Anwendungs-Access-Ports oder die Verwendung von Proxy-Bypass in Betracht ziehen. Weitere Informationen zu diesen Alternativen finden Sie unter Konfigurieren des Anwendungszugriffs und Verwenden des Proxyumgehens.

Wenn die URL, auf die über Clientless-SSL-VPN zugegriffen wird, in den meisten Szenarien für Internet Explorer fehlschlägt, schlägt sie auch für einen anderen Browser fehl.

Um sicherzustellen, dass dies nicht vom Client-PC oder Betriebssystem abhängig ist, verwenden Sie einen anderen Client von einem anderen Standort. Die Verwendung eines IPsec- oder SSL VPN-Clients kann ebenfalls getestet werden.

Stellen Sie sicher, dass die ASA im <u>Browser Trusted Zone</u> enthalten ist, wie unter <u>Aktivieren von</u> <u>Cookies in Browsern für WebVPN</u> beschrieben, und dass Cookies aktiviert sind, wie unter <u>Cookies</u> <u>aktivieren</u> beschrieben.

Wenn bei einer Anwendung ein Problem mit der clientlosen Content-Transformation-Engine (CTE/Rewriter) auftritt, können Sie das Lesezeichen für diese Anwendung ändern, um die Option Smart Tunnel zu aktivieren, wie in diesem Bild gezeigt:

Configuratio	Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks								
Configure	bookmark lists that the securit	ty appliance displays on the SSL VPN portal page.							
- bha 4 2	📝 Edit 🛱 Delete 💠								
-									
		Bookmarks							
Template									
Fdit	Bookmark List		X						
			~						
Bookm	hark List Name: Test_Sites								
	Name	URL Add							
Hotm Vabo	ail o Mail	http://www.hotmail.com							
		http://www.inaii.yarioo.com							
	dit Bookmark Entry								
	Bookmark Title: Hotmail								
	URL Value: http	:// www.hotmail.com	-						
	, .								
	Advance <mark>d</mark> Options	*							
	Subtitle:								
	Thumbnail:	None Manage							
	URL Method :	💿 Get 🔿 Post							
	Enable Favorite Option:	⊙ Yes ◯ No							
	Enable Smart Tunnel Option:	⊙ Yes C No							

Die Aktivierung dieser Option für ein Lesezeichen erfordert keine zusätzliche Konfiguration. Ähnlich wie bei der Port-Weiterleitung ist dies eine weitere praktische Option, um auf ein Lesezeichen zu klicken, um ein neues Fenster zu öffnen, das den Smart Tunnel verwendet, um Anwendungsdatenverkehr zu passieren und Probleme beim Umschreiben zu vermeiden.

Wenn Sie diese Funktion für TCP Winsock 32-Anwendungen (z. B. RDP) verwenden, muss der Administrator die Prozesse identifizieren, die über intelligente Tunnel verwendet werden sollen. RDP verwendet beispielsweise den Prozess mstsc.exe. Hierfür kann ein einfacher Smart Tunnel-Eintrag erstellt werden.

Komplexere Anwendungen können mehrere Prozesse auslösen. Wählen Sie auf der WebVPN-Portalseite den Bereich **Anwendungszugriff aus**. Sobald es geladen wird, kann die Liste der *zulässigen Anwendungen* mit der privaten Seite des Netzwerks verbunden werden.

Wenn der Vorgang immer noch fehlschlägt, führen Sie diese Schritte aus, um die erforderlichen Informationen zu sammeln, und öffnen Sie dann ein TAC-Ticket.

- 1. Löschen Sie den Browser-Cache wie unter Löschen des Browser-Cache beschrieben.
- 2. Löschen Sie den Java-Cache wie unter Löschen des Java-Cache beschrieben.
- 3. Deaktivieren Sie den WebVPN-Cache auf der ASA, wie unter <u>Konfigurieren der</u> <u>Zwischenspeicherung</u> beschrieben.
- 4. Wenn ein Java-Applet vorhanden ist, verwenden Sie Debug Level 5 im Appletfenster, wie unter Optionen zum Aktivieren von Java-Applet-Debugging beschrieben.
- 5. Melden Sie sich über SSL VPN ohne Client bei der ASA an.
- 6. Aktivieren Sie bei der URL direkt vor der problematischen URL ein HTML-Erfassungstool im Browser, wie unter <u>Aktivieren der HTML-Erfassungstools</u> beschrieben.
- 7. Erfassen Sie die Sequenz von diesem Punkt bis zur problematischen URL.
- 8. Drücken Sie **Strg+Druck** auf Ihrer Tastatur, um einen Screenshot aufzunehmen.
- 9. Beenden Sie das HTML-Erfassungstool.
- 10. Führen Sie die Schritte 1 bis 9 durch, wenn Sie entweder über eine IPsec- oder AnyConnect SSL-Sitzung über die ASA eine direkte Verbindung zur URL herstellen oder (wenn möglich) eine direkte Verbindung mit demselben LAN-Segment herstellen, diese Schritte aus und senden die Daten zur Analyse an das TAC

Verfahren

Hinzufügen der ASA als vertrauenswürdiger Standort

Wenn Sie in Internet Explorer auf die ASA zugreifen, erhalten Sie einen Zertifikatsfehler, wenn die Site nicht als vertrauenswürdige Site enthalten ist.



Gehen Sie wie folgt vor, um die ASA als vertrauenswürdigen Standort hinzuzufügen:

- 1. Wählen Sie im Internet Explorer Extras > Internetoptionen aus.
- 2. Klicken Sie auf die Registerkarte Sicherheit, und wählen Sie Vertrauenswürdige Sites



- 3. Klicken Sie auf Sites.
- 4. Fügen Sie die Adresse https:// der ASA hinzu, und klicken Sie auf

	Trusted sites
	You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
	Add this website to the zone:
	https://asa.com/
	Websites:
	Remove
	Require server verification (https:) for all sites in this zone
	Class
Hinzufügen.	Close

5. Nach dem Hinzufügen der Site wird in der Statusleiste von Internet Explorer das Symbol

Trusted sites

Trusted Sites (Vertrauenswürdige Sites) angezeigt.

Hinweis: <u>Detaillierte Informationen</u> zu diesem Verfahren finden Sie unter Arbeiten mit <u>Internet</u> <u>Explorer 6-Sicherheitseinstellungen</u>.

Cookies aktivieren

Gehen Sie wie folgt vor, um Cookies zu aktivieren:

- 1. Wählen Sie in Internet Explorer **Extras > Internetoptionen aus**.
- 2. Klicken Sie auf die Registerkarte Datenschutz und anschließend auf

	Internet Options 🔹 🔀								
	General Security Privacy Content Connections Programs Advanced								
	Settings								
	To set a standard privacy level instead of using custom settings, click the Default button.								
	Custom								
	- Advanced or imported settings								
	Sites Import Advanced Default								
	Pop-up Blocker								
	Prevent most pop-up windows from Settings appearing.								
	Turn on Pop-up Blocker								
Envoitort	OK Cancel Apply								

3. Aktivieren Sie im Dialogfeld Erweiterte Datenschutzeinstellungen das Kontrollkästchen Automatische Cookiebehandlung außer Kraft setzen, klicken Sie auf das Optionsfeld Akzeptieren, und klicken Sie auf

	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								
	Accept Accept								
	O Block O Block								
	O Prompt O Prompt								
	Always allow session cookies								
אר	OK Cancel								

Löschen des Browser-Cache

Gehen Sie wie folgt vor, um den Cache für Internet Explorer zu löschen:

1. Wählen Sie in Internet Explorer Extras > Internetoptionen

Internet Op	otions 🔹 💽 🔀						
General Se	ecurity Privacy Content Connections Programs Advanced						
Home page							
	To c <u>r</u> eate home page tabs, type each address on its own line.						
Desta exercised	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 Settings						
Search _							
$\left \right\rangle$	Change search defaults. Settings						
Tabs —							
	Change how webpages are displayed in Se <u>t</u> tings tabs.						
Appearan	ce						
	ors Languages Fo <u>n</u> ts Acc <u>e</u> ssibility						
	OK Cancel <u>A</u> pply						

2. Klicken Sie auf der Registerkarte Allgemein im Abschnitt Browserverlauf auf



- 3. Klicken Sie auf Alle löschen.
- 4. Aktivieren Sie das Kontrollkästchen Dateien und Einstellungen löschen, die von Add-ons gespeichert wurden, und klicken Sie auf Ja.
- 5. Wenn der Cache gelöscht ist, schließen Sie alle Instanzen des Browsers und starten Sie den Browser neu.

Hinweis: Informationen zum Löschen des Cache für andere Browser finden Sie unter <u>Wie lösche</u> ich den Cache meines Browsers (um die Leistung zu verbessern)?

Löschen des Java-Cache

Führen Sie die folgenden Schritte aus, um den Java-Cache zu löschen:

- 1. Wählen Sie Systemsteuerung im Windows-Startmenü aus.
- 2. Doppelklicken Sie auf

🛓 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 def will use the network settings in your web browser. Only advanced use modify these settings.	ault, Java ers should
Network Set	tings
Temporary Internet Files	
Files you use in Java applications are stored in a special folder for quid later. Only advanced users should delete files or modify these setting	k execution Is.
Settings V	'iew
OK Cancel	Apply

- 3. Klicken Sie auf Einstellungen.
- 4. Klicken Sie auf **Dateien** löschen.



Hinweis: Weitere Informationen finden Sie unter <u>Wie lösche ich meinen Java-Cache?</u> für weitere Informationen über dieses Verfahren.

Java Applet Debugoptionen aktivieren

Gehen Sie wie folgt vor, um die Debugoption für Java-Applets zu aktivieren:

Versionsnummer.

🛃 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 All rights reserve For more inform applications, vis	e 5 (build 1.6.0_05-b13) Sun Microsystems, Inc. ed. Use is subject to license terms. nation about Java technology and to explore grea t <u>http://www.java.com</u>	it Java
Num.		
		Close

Hinweis: Sie

können Java-Updates von http://java.com/en/ herunterladen.

2. Stellen Sie sicher, dass Java so konfiguriert ist, dass die Ablaufverfolgung aktiviert, die Konsole angezeigt und Microsoft Internet Explorer als Standardbrowser festgelegt wird, wie

2 Java Control Panel
Seneral Update Java Security Advanced
Settings
Enable tracing
Enable logging
Show applet lifecycle exceptions
Show console
Mide console
O not start console
Default Java for browsers
Microsoft Internet Explorer
Mozilla family

in diesem Bild gezeigt:

- 3. Stellen Sie sicher, dass der Java-Cache wie unter <u>Löschen des Java-Cache</u> beschrieben gelöscht wird.
- 4. Wählen Sie in Internet Explorer Extras > Java Console, um das Fenster Java-Debuggen zu

🕌 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> 	
Trace level set to 5: all completed.	
<u>C</u> lear Cop <u>y</u> Clos <u>e</u>	

- 5. Wenn das Debugfenster der Java Console geöffnet ist, drücken Sie 5, um die Ablaufverfolgungsebene festzulegen. Wenn auf eine URL zugegriffen wird, die ein Java-Applet enthält, wird die Aktivität in diesem Fenster erfasst.
- 6. Klicken Sie auf **Kopieren**, um die Informationen zu kopieren.

Aktivieren der HTML-Erfassungstools

Zum Erfassen von Daten stehen verschiedene HTML-Erfassungstools zur Verfügung, von denen einige hier aufgelistet sind. Installieren Sie eines dieser HTML-Erfassungstools auf dem Client-PC, der für die Datenerhebung verwendet wird:

- HTTPWatch
- IE-Inspektor
- <u>Debugproxy</u>

Hinweis: Bei dieser Prozedur wird die HTTPWatch-Anwendung verwendet.

Führen Sie nach der Installation der Anwendung die folgenden Schritte aus:

1. Drücken Sie Umschalttaste+P+F+2, oder klicken Sie im Browserfenster auf das Symbol, um HTTPWatch zu



2. Sobald die Anwendung aktiviert ist, wird am unteren Rand des Browserfensters ein Fenster eingebettet, das diesem Bild

ähnelt:

×	Record	🔙 Stop	Clear	🔁 View 👻	🮯 Summary	🔍 Find	•	۲ P	Filter	Ŧ	ave 🔚	😗 🍞 Help 👻
	Started -	≜ Ті	me Chart			- I	Tir	me	Ser	nt	Received	Method

3. Klicken Sie auf **Datensatz**, um Daten aufzuzeichnen. klicken Sie auf **Beenden**, um die Aufzeichnung zu beenden.

Hinweis: Es wird empfohlen, HttpWatch 7.x zum Aufzeichnen der Daten zu verwenden.

Zugehörige Informationen

- Clientless-SSL-VPN (WebVPN) auf ASA-Konfigurationsbeispiel
- <u>Cisco Adaptive Security Appliances der Serie ASA 5500</u>
- <u>Technischer Support und Dokumentation Cisco Systems</u>