WebVPN Capture Tool auf der Cisco Adaptive Security Appliance der Serie ASA 5500

Inhalt

Einführung

Die Cisco Adaptive Security Appliance der Serie ASA 5500 umfasst ein WebVPN-Erfassungstool, mit dem Sie Informationen über Websites protokollieren können, die über eine WebVPN-Verbindung nicht ordnungsgemäß angezeigt werden. Sie können das Erfassungstool über die Befehlszeilenschnittstelle (CLI) der Sicherheitsappliance aktivieren. Die von diesem Tool erfassten Daten können Ihrem Cisco Kundensupport-Mitarbeiter bei der Fehlerbehebung helfen.

Hinweis: Wenn Sie das WebVPN-Erfassungstool aktivieren, wirkt sich dies auf die Leistung der Sicherheits-Appliance aus. Deaktivieren Sie das Erfassungstool, nachdem Sie die Ausgabedateien generiert haben.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderung erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Verwenden Sie die CLI (Command Line Interface), um die Cisco Adaptive Security Appliance der Serie ASA 5500 zu konfigurieren.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Adaptive Security Appliance der Serie ASA 5500, die Version 7.0 ausführt.

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 Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Ausgabedateien des WebVPN Capture-Tools

Wenn das WebVPN-Erfassungstool aktiviert ist, speichert das Erfassungstool die Daten der ersten in diesen Dateien besuchten URL:

- original.000 - Enthält die Daten, die zwischen der Sicherheits-Appliance und dem Webserver ausgetauscht werden.
- mangled.000: Enthält die Daten, die zwischen der Sicherheits-Appliance und dem Browser ausgetauscht werden.

Für jede nachfolgende Erfassung generiert das Erfassungstool zusätzliche übereinstimmende Original-.<nn> und verwaltete.<nn> Dateien und inkrementiert die Dateierweiterungen. In diesem Beispiel zeigt die Ausgabe des Befehls **dir** drei Gruppen von Dateien aus drei URL-Erfassungen an:

```
hostname#dir
Directory of disk0:/
2952        -rw-        10931           10:38:32 Jan 19 2005 config
6           -rw-        5124096         19:43:32 Jan 01 2003 cdisk.bin
3397        -rw-        5157            08:30:56 Feb 14 2005 ORIGINAL.000
3398        -rw-        6396            08:30:56 Feb 14 2005 MANGLED.000
3399        -rw-        4928            08:32:51 Feb 14 2005 ORIGINAL.001
3400        -rw-        6167            08:32:51 Feb 14 2005 MANGLED.001
3401        -rw-        5264            08:35:23 Feb 14 2005 ORIGINAL.002
3402        -rw-        6503            08:35:23 Feb 14 2005 MANGLED.002
hostname#
```

Aktivieren des WebVPN Capture-Tools

Hinweis: Das Flash-Dateisystem hat Einschränkungen, wenn mehrere Dateien zum Schreiben geöffnet werden. Das WebVPN-Erfassungstool kann möglicherweise zu einer Beschädigung des Dateisystems führen, wenn mehrere Erfassungsdateien gleichzeitig aktualisiert werden. Sollte

dieser Fehler beim Erfassungstool auftreten, wenden Sie sich an das Cisco Technical Assistance Center (TAC).

Um das WebVPN-Erfassungstool zu aktivieren, verwenden Sie den Befehl **webvpn 67 im** privilegierten EXEC-Modus:

```
debug menu webvpn 67
```

Wo:

- **cmd** ist 0 oder 1. 0 deaktiviert die Erfassung. 1 ermöglicht die Erfassung.
- **user** ist der Benutzername, der für die Datenerfassung übereinstimmt.
- **url** ist das für die Datenerfassung geeignete URL-Präfix. Verwenden Sie eines der folgenden URL-Formate:Verwenden Sie /http, um alle Daten zu erfassen.Verwenden Sie /http/0/<server/path>, um HTTP-Datenverkehr zu dem von <server/path> identifizierten Server zu erfassen.Verwenden Sie /https/0/<server/path>, um HTTPS-Datenverkehr zu dem Server zu erfassen, der von <server/path> identifiziert wurde.

Verwenden Sie den Befehl **debug menu webvpn 67 0**, um die Erfassung zu deaktivieren.

In diesem Beispiel ist das WebVPN-Erfassungstool aktiviert, um HTTP-Datenverkehr für Benutzer2 zu erfassen, der die Website wwwin.abcd.com/hr/people besucht:

```
hostname#debug menu webvpn 67 1 user2 /http/0/wwwin.abcd.com/hr/people
Mangle Logging: ON
Name: "user2"
URL: "/http/0/wwwin.abcd.com/hr/people"
hostname#
```

In diesem Beispiel ist das WebVPN-Erfassungstool deaktiviert:

```
hostname#debug menu webvpn 67 0
Mangle Logging: OFF
Name: "user2"
URL: "/http/0/wwwin.abcd.com/hr/people"
hostname#
```

Suchen und Hochladen der Ausgabedateien des WebVPN Capture Tool

Suchen Sie mithilfe des Befehls **dir** die Ausgabedateien des WebVPN-Erfassungstools. In diesem Beispiel wird die Ausgabe des Befehls **dir** veranschaulicht und die erstellten Dateien ORIGINAL.000 und MANGLED.000 enthalten:

```
hostname#dir
Directory of disk0:/
2952        -rw-        10931           10:38:32 Jan 19 2005 config
6         -rw-        5124096         19:43:32 Jan 01 2003 cdisk.bin
3397        -rw-        5157            08:30:56 Feb 14 2005 ORIGINAL.000
```

```
3398        -rw-        6396            08:30:56 Feb 14 2005 MANGLED.000
hostname#
```

Sie können die Ausgabedateien des WebVPN-Erfassungstools mithilfe des Befehls **copy flash** auf einen anderen Computer hochladen. In diesem Beispiel werden die Dateien ORIGINAL.000 und MANGLED.000 hochgeladen:

```
hostname#copy flash:/original.000 tftp://10/86.194.191/original.000
Source filename [original.000]?
Address or name of remote host [10.86.194.191]?
Destination filename [original.000]?
!!!!!!
21601 bytes copied in 0.370 secs
hostname#copy flash:/mangled.000 tftp://10/86.194.191/mangled.000
Source filename [mangled.000]?
Address or name of remote host [10.86.194.191]?
Destination filename [mangled.000]?
!!!!!!
23526 bytes copied in 0.380 secs
hostname#
```

Hinweis: Um eine mögliche Beschädigung des Dateisystems zu vermeiden, lassen Sie nicht zu, dass die Originaldateien überschrieben werden.<nnn> und die Dateien aus früheren Aufnahmen überschrieben werden. Wenn Sie das Erfassungstool deaktivieren, löschen Sie die alten Dateien, um eine Beschädigung des Dateisystems zu verhindern.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Konfigurationsanleitungen für Cisco Adaptive Security Appliance der Serie ASA 5500
- Technischer Support und Dokumentation - Cisco Systems