Cisco ASA 5500系列自適應安全裝置上的WebVPN捕獲工具

目錄

簡介

Cisco ASA 5500系列自適應安全裝置包括一個WebVPN捕獲工具，通過該工具可以記錄有關無法通過WebVPN連線正確顯示的網站的資訊。您可以從安全裝置的命令列介面(CLI)啟用捕獲工具。此工具記錄的資料可幫助您的思科客戶支援代表排除故障。

注意：啟用WebVPN捕獲工具時，會對安全裝置的效能產生影響。請確保在生成輸出檔案後禁用捕獲工具。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 使用命令列介面(CLI)配置Cisco ASA 5500系列自適應安全裝置。

採用元件

本文檔中的資訊基於運行版本7.0的Cisco ASA 5500系列自適應安全裝置。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

WebVPN捕獲工具輸出檔案

啟用WebVPN捕獲工具後，該捕獲工具會在以下檔案中儲存來自第一個URL的資料：

- original.000 — 包含安全裝置與Web伺服器之間交換的資料。
- mangled.000 — 包含安全裝置和瀏覽器之間交換的資料。

對於每個後續捕獲，捕獲工具將生成其他匹配的原始。<nnn>和已損壞。<nnn>檔案並增加副檔名。在本例中， **dir**命令的輸出顯示了三個URL捕獲中的三組檔案：

```
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#
```

啟用WebVPN捕獲工具

注意：當開啟多個要寫入的檔案時，快閃記憶體檔案系統有限制。同時更新多個捕獲檔案時，WebVPN捕獲工具可能會導致檔案系統損壞。如果擷取工具發生此故障，請聯絡思科技術協助中心(TAC)。

若要啟用WebVPN捕獲工具，請在特權EXEC模式下使用**debug menu webvpn 67**命令：

```
debug menu webvpn 67
```

其中：

- **cmd**為0或1。0禁用捕獲。1啟用捕獲。
- **user**是資料捕獲要匹配的使用者名稱。
- **url**是資料捕獲要匹配的URL字首。使用以下URL格式之一：使用/http捕獲所有資料。使用

/http/0/<server/path>捕獲到<server/path>所標識伺服器的HTTP流量。使用/https/0/<server/path>捕獲到<server/path>所標識伺服器的HTTPS流量。

使用**debug menu webvpn 67 0**命令禁用捕獲。

在本示例中，啟用WebVPN捕獲工具可捕獲user2訪問網站wwwin.abcd.com/hr/people的HTTP流量：

```
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#
```

在此示例中，禁用WebVPN捕獲工具：

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

查詢並上傳WebVPN捕獲工具輸出檔案

使用**dir**命令可查詢WebVPN捕獲工具輸出檔案。此範例顯示**dir**命令的輸出，並包括所生成的ORIGINAL.000和MANGLED.000檔案：

```
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#
```

您可以使用**copy flash**命令將WebVPN捕獲工具輸出檔案上傳到另一台電腦。在此範例中，系統會上傳ORIGINAL.000和MANGLED.000檔案：

```
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#
```

注意：為了避免可能的檔案系統損壞，請不要覆蓋原始。<nnn>和損壞的。<nnn>以前捕獲中的檔案。禁用捕獲工具時，請刪除舊檔案以防止檔案系統損壞。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- Cisco ASA 5500系列自適應安全裝置配置指南
- 技術支援與文件 - Cisco Systems