WebVPN捕获工具在Cisco ASA5500系列适配器上的安全工具

目录

简介

Cisco ASA 5500系列可适应安全工具包括让您关于网站的日志信息不在WebVPN连接适当地显示的WebVPN捕获工具。您能启用从安全工具的命令行界面(CLI)的捕获工具。此工具记录的数据可帮助您的Cisco用户支持代表排除故障问题。

注意： 当您启用WebVPN捕获工具时，有在安全工具的性能的一影响。在您生成输出文件后，请务必禁用捕获工具。

先决条件

要求

在尝试进行此配置之前，请确保满足以下要求：

- 请使用命令行界面(CLI)为了配置Cisco ASA 5500系列可适应安全工具。

使用的组件

本文档中的信息根据运行版本7.0的Cisco ASA 5500系列可适应安全工具。

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。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

WebVPN捕获工具输出文件

当WebVPN捕获工具启用时，在这些文件存储从第一个URL的数据访问的捕获工具：

- original.000 —包含数据交换在安全工具和Web服务器之间。
- mangled.000 —包含数据交换在安全工具和浏览器之间。

对于每个随后的捕获，捕获工具生成另外的匹配的original.<nnn>和mangled.<nnn>文件并且增加文件扩展。在本例中，**dir命令**显示的输出三套从三个URL捕获的文件：

```
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#
```

激活WebVPN捕获工具

注意： 当多个文件为文字时，打开闪存文件系统有限制。当多次捕获文件同时时，更新WebVPN捕获工具能可能导致文件系统损坏。如果此失败应该发生在捕获工具，请与Cisco技术支持中心(TAC)联系。

为了激活WebVPN捕获工具，请使用**debug menu webvpn 67命令**从特权EXEC模式：

```
debug menu webvpn 67 <cmd> <user> <url>
```

Where:

- **cmd**是0个或1. 0个功能失效捕获。1个enable (event)捕获。
- **用户**是匹配的用户名为数据捕获。
- **URL**是匹配的URL前缀为数据捕获。请使用这些URL格式之一：请使用/http获取所有数据。请使用/http/0/<server/path>捕获HTTP数据流到<server/path>识别的服务器。请使用/https/0/<server/path>捕获HTTPS流量到<server/path>识别的服务器。

请使用**debug menu webvpn 67 0命令**为了禁用捕获。

在本例中， WebVPN捕获工具启用捕获访问网站wwwin.abcd.com/hr/people的user2的HTTP数据流：

```
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#
```

在本例中， WebVPN捕获工具禁用：

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

寻找并且上传WebVPN捕获工具输出文件

请使用**dir命令**为了寻找WebVPN捕获工具输出文件。此示例显示输出**dir命令**并且包含生成的ORIGINAL.000和MANGLED.000文件：

```
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#
```

使用**copy flash命令**，您能上传WebVPN捕获工具输出文件到另一台计算机。在本例中，ORIGINAL.000和MANGLED.000文件上传：

```
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： 为了避免可能的文件系统损坏，请勿允许original.<nnn>和mangled.<nnn>文件从将覆盖的上一个捕获。当您禁用捕获工具时，请删除旧有文件为了防止文件系统的损坏。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco ASA 5500系列可适应安全工具配置指南
- 技术支持和文档 - Cisco Systems