# 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系列自适应安全设备包括WebVPN捕获工具，通过该工具，您可以记录有关无法通过WebVPN连接正确显示的网站的信息。您可以从安全设备的命令行界面(CLI)启用捕获工具。此工具记录的数据可帮助您的思科客户支持代表排除故障。

**注意**：启用WebVPN捕获工具时，它会影响安全设备的性能。请确保在生成输出文件后禁用捕获工具。

## 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：

- 使用命令行界面(CLI)配置Cisco ASA 5500系列自适应安全设备。

### 使用的组件

本文档中的信息基于运行版本7.0的Cisco ASA 5500系列自适应安全设备。

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(仅限注册客户)可获取有关本节中使用的命令的详细信息。

## WebVPN捕获工具输出文件

启用WebVPN捕获工具后，捕获工具将从访问的第一个URL中存储的数据存储在以下文件中：

- original.000 — 包含安全设备与Web服务器之间交换的数据。
- mangled.000 — 包含安全设备和浏览器之间交换的数据。

对于每次后续捕获，捕获工具都会生成其他匹配的原始文件。<nn>和损坏的文件，并增加文件扩展名。在本示例中，**dir**命令的输出显示了三组来自三个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**：当打开多个文件进行写入时，闪存文件系统具有限制。当同时更新多个捕获文件时，WebVPN捕获工具可能会导致文件系统损坏。如果此故障应使用捕获工具发生，请与思科技术支持中心(TAC)联系。

要激活WebVPN捕获工具，请在特权EXEC模式下使用**debug menu webvpn 67**命令：

```
debug menu webvpn 67
```

其中：

- **cmd**为0或1。0禁用捕获。1支持捕获。
- **user**是用于数据捕获的匹配用户名。
- **url**是用于数据捕获的匹配URL前缀。使用以下URL格式之一：使用/http捕获所有数据。使用

/http/0/<server/path>捕获到<server/path>所标识的服务器的HTTP流量。使用
/https/0/<server/path>捕获到<server/path>所标识的服务器的HTTPS流量。

使用debug menu webvpn **67 0命令**禁用捕获功能。

在本示例中，启用WebVPN捕获工具以捕获用户2访问网站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#
```

在本例中，WebVPN捕获工具被禁用：

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

## 查找并上传WebVPN捕获工具输出文件

使用**dir**命令查找WebVPN捕获工具的输出文件。此示例显示**dir**命令的输出，包括生成的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#
```

您可以使用copy flash命令将WebVPN捕获工具输出文件上传到另**一台计**算机。在本示例中，上传ORIGINAL.000和MANGLED.000文件：

```
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**：为避免可能的文件系统损坏，请不要覆盖原始文件。<nn>和损坏的文件。<nnn>文件。禁用捕获工具时，请删除旧文件以防止文件系统损坏。

# 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系列自适应安全设备配置指南
- 技术支持和文档 - Cisco Systems