Table of Contents

WebVPN Capture Tool on the Cisco ASA 5500 Series Adaptive Security Appliance

Document ID: 65096

Introduction

The Cisco ASA 5500 Series Adaptive Security Appliance includes a WebVPN capture tool that lets you log information about Web sites that do not display properly over a WebVPN connection. You can enable the capture tool from the Command Line Interface (CLI) of the security appliance. The data this tool records can help your Cisco customer support representative troubleshoot problems.

Note: Enabling the WebVPN capture tool has an impact on the performance of the security appliance. Be sure to disable the capture tool after you have generated the output files.

Prerequisites

Requirements

Before attempting this configuration, ensure that you meet these requirements:

- using the Command Line Interface (CLI) to configure the Cisco ASA 5500 Series Adaptive Security Appliance.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA 5500 Series Adaptive Security Appliance running version 7.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

WebVPN Capture Tool Output Files

When the WebVPN capture tool is enabled, the capture tool stores the data from the first URL visited in the following files:

- original.000 Contains the data exchanged between the security appliance and the Web Server.
- mangled.000 Contains the data exchanged between the security appliance and the Browser.

For each subsequent capture, the capture tool generates additional matching original.<nnn> and mangled.<nnn> files and increments the file extensions. In this example, the output of the **dir** command displays three sets of files from three URL captures:

```
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#
```

Activating the WebVPN Capture Tool

Note: The Flash File System has limitations when multiple files are opened for writing. The WebVPN capture tool can possibly cause file system corruption when multiple capture files are being updated concurrently. If this failure should occur with the capture tool, contact the Cisco Technical Assistance Center (TAC).

To activate the WebVPN capture tool, use the **debug menu webvpn 67** command from privileged EXEC mode:

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

Where:

- **cmd** is 0 or 1. 0 disables capture. 1 enables capture.
- **user** is the username to match for data capture.
- **url** is the URL prefix to match for data capture. Use one of these URL formats:
    - Use /http to capture all data.

- Use /http/0/<server/path> to capture HTTP traffic to the server identified by <server/path>.
- Use /https/0/<server/path> to capture HTTPS traffic to the server identified by <server/path>.

To disable capture, use the **debug menu webvpn 67 0** command.

In this example, the WebVPN capture tool is enabled to capture HTTP traffic for user2 visiting Web site wwwin.abcd.com/hr/people:

```
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 this example, the WebVPN capture tool is disabled:

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

Locating and Uploading the WebVPN Capture Tool Output Files

To locate the WebVPN capture tool output files, use the **dir** command. This example shows the output of the **dir** command, including the ORIGINAL.000 and MANGLED.000 files that were generated:

```
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#
```

You can upload the WebVPN capture tool output files to another computer using the **copy flash** command. In this example, the ORIGINAL.000 and MANGLED.000 files are uploaded:

```
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#
```

Note: To avoid possibly corrupting the file system, do not allow the original.<nnn> and mangled.<nnn> files from previous captures to be overwritten. When you disable the capture tool, delete the old files to prevent corrupting the file system.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- **Cisco ASA 5500 Series Adaptive Security Appliance Configuration Guides**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jun 21, 2005 Document ID: 65096