Content Security Appliances FAQ: How do you perform a packet capture on a Cisco Content Security appliance?

Document ID: 117843

Contributed by Khoa Nguyen and Robert Sherwin, Cisco TAC Engineers.
Jun 25, 2014

Contents

Introduction

This document describes how to perform packet captures on the Cisco Content Security appliances.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Email Security Appliance (ESA)
- Cisco Web Security Appliance (WSA)
- Cisco Security Management Appliance (SMA)
- AsyncOS

Components Used

The information in this document is base on all versions of AsyncOS.

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.

How do you perform a packet capture on a Cisco Content Security appliance?

Complete these steps in order to perform a packet capture (***tcpdump*** command) with the GUI:

1. Navigate to ***Help and Support*** > ***Packet Capture*** on the GUI.

2. Edit the packet capture settings as required, such as the network interface on which the packet capture runs. You can use one of the predefined filters, or you can create a custom filter with the use of any syntax that is supported by the Unix ***tcpdump*** command.

3. Click ***Start Capture*** in order to begin the capture.

4. Click ***Stop Capture*** in order to end the capture.

5. Download the packet capture.

Complete these steps in order to perform a packet capture (***tcpdump*** command) with the CLI:

1. Enter this command into the CLI:

```
wsa.run> packetcapture

Status: No capture running


Current Settings:

 Max file size:      200 MB

 Capture Limit:      None (Run Indefinitely)

 Capture Interfaces: Management

 Capture Filter:     (tcp port 80 or tcp port 3128)
```

2. Choose the operation that you want to perform:

```
- START - Start packet capture.

- SETUP - Change packet capture settings.

[]> setup
```

3. Enter the maximum allowable size for the capture file (in MB):

```
[200]> 200

Do you want to stop the capture when the file size is reached? (If not, a new
 file will be started and the older capture data will be discarded.)

[N]> n

The following interfaces are configured:

1. Management

2. T1

3. T2
```

4. Enter the name or number of one or more interfaces from which to capture packets, separated by commas:

```
[1]> 1
```

5. Enter the filter that you want to use for the capture. Enter the word ***CLEAR*** in order to clear the filter

and capture all of the packets on the selected interfaces.

```
[(tcp port 80 or tcp port 3128)]> host 10.10.10.10 && port 80

Status: No capture running

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     host 10.10.10.10 && port 80
```

6. Choose the ***start*** operation in order to begin the capture:

```
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]> start

Status: Capture in progress (Duration: 0s)
File Name: S650-00137262569A-8RVFDB1-20080919-174302.cap (Size: 0K)

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
 Capture Filter:     host 10.10.10.10 && port 80
```

7. Choose the ***stop*** operation in order to end the capture:

```
- STOP - Stop packet capture.
- STATUS - Display current capture status.
- SETUP - Change packet capture settings.
[]> stop

Status: No capture running (Capture stopped by user)

Current Settings:
 Max file size:      200 MB
 Capture Limit:      None (Run Indefinitely)
 Capture Interfaces: Management
```

```
Capture Filter:     host 10.10.10.10 && port 80
```

Updated: Jun 25, 2014 Document ID: 117843