App F Direct Captures on Cisco WAE Accelerators

This workflow is provided in case you prefer to capture directly on the accelerators themselves using tcpdump. However, it is recommended that you capture on the accelerators using Capture Manager, as described in Capturing on Cisco and Riverbed Accelerators.

Note—The following information is based on the experiences of engineers working in a lab environment, and is not intended to provide comprehensive documentation about specific devices. If you need detailed information about capturing on a specific device, contact your IS organization or the device vendor.

The direct workflow consists of the following steps.

1) Log in to both accelerators using telnet, putty, or a similar utility.
   Note—You must be in Executive mode to capture traffic.

2) Identify the interfaces to capture on (see Identifying the WAE Interfaces for Capturing Traffic).

   Ideally, you should be able to run the application and start/stop the captures from the same host. Suppose you are capturing on two accelerators with two interfaces each. In this situation, the most efficient way to capture is to have the following windows open on the same host:

   — Accelerator 1, LAN interface
   — Accelerator 1, WAN interface
   — Accelerator 2, LAN interface
   — Accelerator 2, WAN interface
   — Window for running the application to capture

3) Start the capture(s) on each accelerator.

   Cisco WAE devices support tcpdump, a common utility for capturing traffic. For more information, see Capturing Application Traffic with tcpdump.

4) Run the user-level application transaction you want to capture.

5) When the transaction finishes, stop the capture on each accelerator: make the corresponding window active, then press Ctrl-C.

6) Transfer the packet traces from the accelerators to the AppTransaction Xpert host (see Identifying the WAE Interfaces for Capturing Traffic).

7) Delete the original packet traces on the accelerators. You can use the following command to delete files:

   `delfile <file_name>`

   Note—For specific information about how to capture on these devices, consult the Cisco WAE documentation.

8) Fill out the WAN Acceleration Worksheet.

   Although this step is not required, you might find this information useful when you import the packet traces into Transaction Analyzer.

Identifying the WAE Interfaces for Capturing Traffic

Cisco WAE devices use a logical in-path configuration by default, with one bidirectional interface that processes both LAN-side and WAN-side traffic (as shown in Figure 11-5). In this case, you need to capture on one interface only per accelerator.

If the accelerator has an in-line module, it will use a WAN-side interface and a LAN-side interface. In this case, you must capture on both interfaces.

Interface names are specified like this:

- `eth0` - GigabitEthernet 1/0
- `eth1` - GigabitEthernet 2/0
- `eth2` - InlinePort 1/1/wan
- `eth3` - InlinePort 1/1/lan
- `eth4` - InlinePort 1/0/wan
- `eth5` - InlinePort 1/0/lan

If you cannot identify the exact interface(s) on which to capture, contact your IS organization.

Transferring Packet Traces from the WAE Device to the AppTransaction Xpert Host

The following steps describe how to transfer packet traces over a secure connection.

1) Enable SSH (Secure Shell) on the accelerator:

   a) Log in to the accelerator.

   b) Enter the following commands:

      `cmd>` **`ssh-key-generate`**

      `cmd>` **`sshd enable`**

2) Use a Secure Copy Program (SCP) to transfer the file.

   Typically, an SCP program uses a syntax similar to the **`cp`** command. For example, PSCP (PuTTY Secure Copy client) uses the following syntax:

   `pscp [`*options*`][<`*user*`>@]<`*host*`>:<`*source_file*`> <`*dest_path*`>`

   PSCP has options for specifying passwords (pw) for logging in with a specific username/password. You can also use wildcards (such as `*.cap`) to transfer multiple files at once.

Figure F-1 Enabling SSH on a Cisco WAE Accelerator: Example Session

```
cisco-edge#config
cisco-edge(config)#ssh-key-generate
Ssh host key generated successfully
Save the host key to box...
Host key was saved successfully and will take effect in new ssh
sessions.
cisco-edge(config)#sshd enable
cisco-edge(config)#
```