# Integration Debugging Information

This section explains the Integration Debugging Information.

# Debugging Information for the Cisco Adaptive Security Appliance

This section provides Debugging Information for the Cisco Adaptive Security Appliance

## Cisco Adaptive Security Appliance Debugging Commands

The following table lists the debugging commands for the Cisco Adaptive Security Appliance.

*Table 1: Cisco Security Appliance Debugging Commands*

| To | Use the Command | Notes |
|---|---|---|
| Show ICMP packet information for pings to the Cisco Adaptive Security Appliance interfaces | `debug icmp trace` | We strongly recommend that you disa messages once you have completed y troubleshooting. To disable ICMP deb use the `no debug icmp trace` comm |
| Show messages relating to the certificate validation between IM and Presence Service /Cisco Adaptive Security Appliance or Cisco Adaptive Security Appliance/external domain | `debug crypto ca` | You can increase log level on the Cis Security Appliance by adding the log parameter to this command, for exam `debug crypto ca 3` |
| | `debug crypto ca messages` | Displays only debug messages for inp messages |
| | `debug crypto ca transactions` | Displays only debug messages for tra |
| Show the SIP messages sent through CiscoAdaptive Security Appliance | `debug sip` | |

| To | Use the Command | Notes |
|---|---|---|
| Send log messages to a buffer (for later viewing) | `terminal monitor` | |
| Enable system log messages | `logging on` | We strongly recommend that you disable log messages once you have completed y troubleshooting. To disable system log m use the `no logging on` command. |
| Send system log messages to a buffer | `logging buffer debug` | |
| Set system log messages to be sent to Telnet or SSH sessions | `logging monitor debug` | |
| Designate a (syslog) server to receive the system log messages | `logging host interface_name ip_address` | • The interface_name argument speci Cisco Adaptive Security Appliance through which you access the syslo<br>• The ip_address argument specifies t address of the syslog server. |
| Ping the Interfaces | `ping` | Refer to the Troubleshooting section of t *CiscoSecurity Appliance Command Line Configuration Guide* for details on pinging Adaptive Security Appliance interfaces, pinging between hosts on different interf ensure that the traffic can pass successfull the Cisco Adaptive Security Appliance.<br>You can also ping an interface in ASDM choosing **Tools** > **Ping**.<br>**Note** You cannot ping the public I Presence Service IP address. the MAC address of the Cis Adaptive Security Applianc interface should appear in th table (**arp –a**). |
| Trace the route of a packet | `traceroute` | You can also trace the route of a packet i choose **Tools** > **Traceroute**. |
| Trace the life span of a packet through the Cisco Adaptive Security Appliance | `packet-tracer` | You can also trace the life span of a pack ASDM , choose **Tools** > **Packet Tracer**. |

**Related Information -**

TLS Proxy Debugging Commands

# Capture Output on Internal and External Interfaces

**Procedure**

**Step 1**    Enter configuration mode:

> **Enable**

> *<password>*

> **configure terminal**

**Step 2**    Define an access-list to specify the traffic to be captured, for example:

**access-list cap extended permit ip** *10.53.0.0 255.255.0.0 10.53.0.0 255.255.0.0*

**Step 3**    It is recommended that you clear the capture content before starting the tests. Use the command "clear capture in" to clear the internal interface capture, and the command "clear capture out" to clear the external interface capture.

**Step 4**    Enter this command to capture the packets on the internal interface:

**cap in interface inside access-list cap**

**Step 5**    Enter this command to capture the packets on the external interface:

**cap out interface outside access-list cap**

**Step 6**    Enter this command to capture TLS specific packets:

**capture** *capture_name* **type tls-proxy interface** *interface_name*

**Step 7**    Enter this command to retrieve the packet capture:

**copy /pcap capture:in tftp://***xx.xx.xx.xx* **copy /pcap capture:out tftp://***xx.xx.xx.xx*

Enter this command to copy the output to disk and retrieve using ASDM (choose **Actions** > **File Management** > **File Transfer**):

**copy /pcap capture:in disk0:in_1**

# TLS Proxy Debugging Commands

The following table lists the debugging commands for the TLS Proxy.

**Table 2: TLS Proxy Debugging Commands**

| To | Use the Command(s) |
|---|---|
| Enable TLS proxy-related debug and syslog output | **debug inspect tls-proxy events**<br>**debug inspect tls-proxy errors**<br>**debug inspect tls-proxy all** |

| To | Use the Command(s) |
| --- | --- |
| Show a TLS proxy session output | `show log` |
| Check the active TLS proxy sessions | `show tls-proxy` |
| View the detail of the current TLS proxy sessions<br><br>(Use when the Cisco Adaptive Security Appliance successfully establishes connections with the IM and Presence Service and the external domain) | `show tls-proxy session detail` |