



Integration Debugging Information

This section explains the Integration Debugging Information.

- [Debugging Information for the Cisco Adaptive Security Appliance, on page 1](#)

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	<code>debug icmp trace</code>	We strongly recommend that you disable debug messages once you have completed your troubleshooting. To disable ICMP debug messages, use the <code>no debug icmp trace</code> command.
Show messages relating to the certificate validation between IM and Presence Service /Cisco Adaptive Security Appliance or Cisco Adaptive Security Appliance/external domain	<code>debug crypto ca</code>	You can increase log level on the Cisco Adaptive Security Appliance by adding the <code>log level</code> parameter to this command, for example, <code>debug crypto ca 3</code>
	<code>debug crypto ca messages</code>	Displays only debug messages for incoming messages
	<code>debug crypto ca transactions</code>	Displays only debug messages for transactions
Show the SIP messages sent through Cisco Adaptive Security Appliance	<code>debug sip</code>	

To	Use the Command	Notes
Send log messages to a buffer (for later viewing)	<code>terminal monitor</code>	
Enable system log messages	<code>logging on</code>	We strongly recommend that you disable log messages once you have completed your troubleshooting. To disable system log messages, use the <code>no logging on</code> command.
Send system log messages to a buffer	<code>logging buffer debug</code>	
Set system log messages to be sent to Telnet or SSH sessions	<code>logging monitor debug</code>	
Designate a (syslog) server to receive the system log messages	<code>logging host interface_name ip_address</code>	<ul style="list-style-type: none"> The <code>interface_name</code> argument specifies the Cisco Adaptive Security Appliance interface through which you access the syslog server. The <code>ip_address</code> argument specifies the IP address of the syslog server.
Ping the Interfaces	<code>ping</code>	<p>Refer to the Troubleshooting section of the <i>Cisco Security Appliance Command Line Configuration Guide</i> for details on pinging Cisco Adaptive Security Appliance interfaces, and on pinging between hosts on different interfaces. To ensure that the traffic can pass successfully through the Cisco Adaptive Security Appliance.</p> <p>You can also ping an interface in ASDM by choosing Tools > Ping.</p> <p>Note You cannot ping the public IP address or Presence Service IP address. However, the MAC address of the Cisco Adaptive Security Appliance interface should appear in the output table (<code>arp -a</code>).</p>
Trace the route of a packet	<code>tracert</code>	You can also trace the route of a packet in ASDM by choosing Tools > Traceroute .
Trace the life span of a packet through the Cisco Adaptive Security Appliance	<code>packet-tracer</code>	You can also trace the life span of a packet in 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 | <pre>debug inspect tls-proxy events debug inspect tls-proxy errors debug inspect tls-proxy all</pre> |

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