

Troubleshoot Commands in ASA CLI

Contents

[Introduction](#)

[Overview](#)

[Troubleshooting and Raising a Support Case](#)

Introduction

This document describes how to use troubleshooting commands in the ASA CLI.

Overview

Use these steps to deploy your Cisco ASA firewall to connect to the Cisco Umbrella SIG Data Center and Secure Web Gateway using an IPSEC IKEv2 Tunnel: <https://docs.umbrella.com/deployment-umbrella/v1.0.6/docs/add-cisco-asa-tunnel>

Troubleshooting and Raising a Support Case

If you are facing issues with your Cisco ASA deployment, please raise a Support case with umbrella-support@cisco.com. When raising the case, please provide: A description of the issue, the output of the commands (shown here) and any relevant ASDM screenshots. Please run the commands via the Cisco ASA CLI.

- show version (Displays the ASA software version)
- show tech (Displays the ASA hardware information)
- show run (Displays the running configuration)
- Show crypto ikev2 sa (Displays the state of the phase 1 Security Association SA)
- show crypto ipsec sa detail Displays the state of the phase 2 SA)

Use this command to simulate a packet from the inside interface, with a specific source IP address and port and a specific destination IP address and port. The response indicates whether the packet flows through the tunnel.

This example simulates HTTP traffic from 10.0.0.1 to 72.163.4.161. These are hosts that can communicate over the tunnel. If This doesn't work, and no SA's formed. So, phase-1 is a good place to focus on.

Command format:

```
packet-tracer input [src_int] [protocol] [src_addr] [src_port] [dest_addr] [dest_port] detailed
```

ciscoasa#

packet-tracer input inside tcp 10.70.134.11 34500 72.163.4.161 443 detailed