Troubleshooting Points:

It is important to note the WSP Customer Service staff has no control over the connectivity between the agency and ACCESS. If your technical department updates any of the following, it may affect the encryption between ACCESS and your agency’s regional state link connection:

1. Router, Firewall, NIC card, or switch/VLAN changes
2. Application changes
3. Changes to IGN IP addresses (must be coordinated with Kathy Paulson, ACCESS Administrator)

To perform many of the tasks listed below will require a skilled IT person familiar with the CAD/RMS server, network topology, and troubleshooting skills for the local LAN and WAN.

Responsibilities:

The Customer Service Group is responsible for monitoring the Cisco ASA 5510. (Point E) from the console (Point G).

The Intergovernmental Network (IGN) router at the Customer Service Unit, the Cisco Pix firewall, and ACCESS are the responsibility Electronic Services Division (ESD).

Points A, B, C, and D are the responsibility of the local agencies. Agencies retain ownership of all encryption devices, their maintenance, support, and disposal.

How to Reach the Customer Service Group:

Call the Customer Service Group at (360) 705 5999 or email at ITDCustomerServicesGroup@wsp.wa.gov with the email title “System Outage”.
**Point E and G: Administrative Console located in the WSP Customer Service Group**

The Customer Service Group is limited in the amount of support they can provide to agencies regarding encryption. They monitor the Cisco ASA 5510 hourly to verify traffic. If an agency is having difficulties, Customer Service can log in and verify if the agency still shows up in the Cisco ASA 5510 and has public and private IP addresses. They will also check the duration (verify it didn't have a temporary outage).

If the tunnel is up but no data traverses, the agency should reset the tunnel. This can be accomplished either by rebooting (reload) or power cycling the encryption device. The Customer Service Group must check to see if the agency has any messages in queue and clear anything pending before the agency restarts the "state link".

If the agency is not showing IP address in the ASA 5510, the tunnel is down. At this point, the agency will have to have an IT person on site for troubleshooting.
Network Testing Tools:

On Unix/AIX/Solaris/IBM

- Netstat –rn will provide a list of all routes
- Ping used to determine if remote host is alive
- Traceroute – used to determine the path to the remote host
- Ifconfig –a used to list all the network interfaces and status

On Windows server/workstation (any version)

- Route print – will provide a list of all routes
- Ping used to determine if remote host is alive
- Tracert – used to determine the path to the remote host
- Ipconfig /all –used to list all the network interfaces, IP addresses, gateways and status.

Encryption Devices

- 3002
- PC with Internet Explorer Version 5 or above and Java 1.4 and above
- Hyperterminal or other communications software
- 1800/2800 series routers
- PC with Internet Explorer Version 5 or above and Java 1.4. and above
- Hyperterminal or other communications software
- Telnet

Point A: CAD/RMS Server at the Agency

Perform the same steps as above. This is best accomplished from the CAD/RMS server. Agencies need administrative privileges to perform tests.

Step 1: Ping Test

- 198.239.158.42 – This validates the VPN tunnel is up and operational and that traffic can be sent and received by ACCESS.
If Successful:

The problem lies with the CAD or RMS server.

If Not Successful:

Verify the proper routing statements are in the CAD/RMS server.  
Example:  198.239.158.42 255.255.255.255 [Private IP address of encryption device]

If Proper Routing Statement not present:

Add routing statement back to the server (This task should be performed by a qualified IT person or your CAD/RMS vendor).

If Proper Routing Statement present:

Stop and start the state link process.  
Note:  Do not reboot CAD/RMS server unless directed by vendor.

Point B:  Any Workstation on an Agency’s Local Area Network

Steps:

198.239.158.130 – This validates the VPN tunnel is up and operational and that traffic can be sent and received by the ASA 5510 (Point E).

If Successful:

The problem lies within Point A and Point B.

If it Fails:

Use traceroute (tracert) to determine how many hops before it stops.  The information can be used by WAN support to identify where the problem resides.

If it Fails:

May need to contact WAN support (DIS, County, agency supporting connectivity to the IGN).
**Point C: Alternate Network Segment**

This segment may contain VLANs.

**Steps:**

198.239.158.130 – This validates the VPN tunnel is up and operational and that traffic can be sent and received by the ASA 5510 (Point E).

**If Successful:**

The problem lies within Point A and Point B.

**If it Fails:**

Use traceroute (tracert) to determine how many hops before it stops. The information can be used by WAN support to identify where the problem resides.

**If it Fails:**

May need to contact WAN support (DIS, County, agency supporting connectivity to the IGN).

**Point D: Network Location Outside the Perimeter (Firewall)**

**Steps:**

198.239.158.130 – This validates the VPN tunnel is up and operational and that traffic can be sent and received by the ASA 5510 (Point E).

**If Successful:**

The problem lies within Point A and Point B.

**If it Fails:**

Use traceroute (tracert) to determine how many hops before it stops. The information can be used by WAN support to identify where the problem resides.
If it Fails:

May need to contact WAN support (DIS, County, agency supporting connectivity to the IGN).

Point F: ACCESS Message Switch
198.239.158.42

Helpful Phone Numbers:

DIS Help Desk 360 753 2454
FORCECOM 503 391 7177
Intergraph 877 882 8921
Spillman 888 774 5562 Option 5