Ford ANX Troubleshooting Procedure for use by C3P Trading Partners

Step 1:	**Verify Internal Routing on Trading Partner Network**
Action:	Verify packets are routing correctly through Trading Partner LAN/WAN and Trading Partner firewall to the trading partner's ANX connection (traceroute can be used).
	See page 3 for instructions
Responsible Party:	Trading Partner Network/Firewall Administrator

Step 2:	**Verify Trading Partner Firewall**
Action:	Verify firewall rules (and NAT-if applicable) at ANX egress
	See page 4-5 for instructions
Responsible Party:	Trading Partner Network/Firewall Administrator

Step 3:	**Verify Trading Partner ANX Connection**
Action:	Verify ANX network connection.
	See page 6 for instructions
Responsible Party:	1. Trading Partner Network/Firewall Administrator 2. If necessary, contact ANX Certified Service Provider Helpdesk

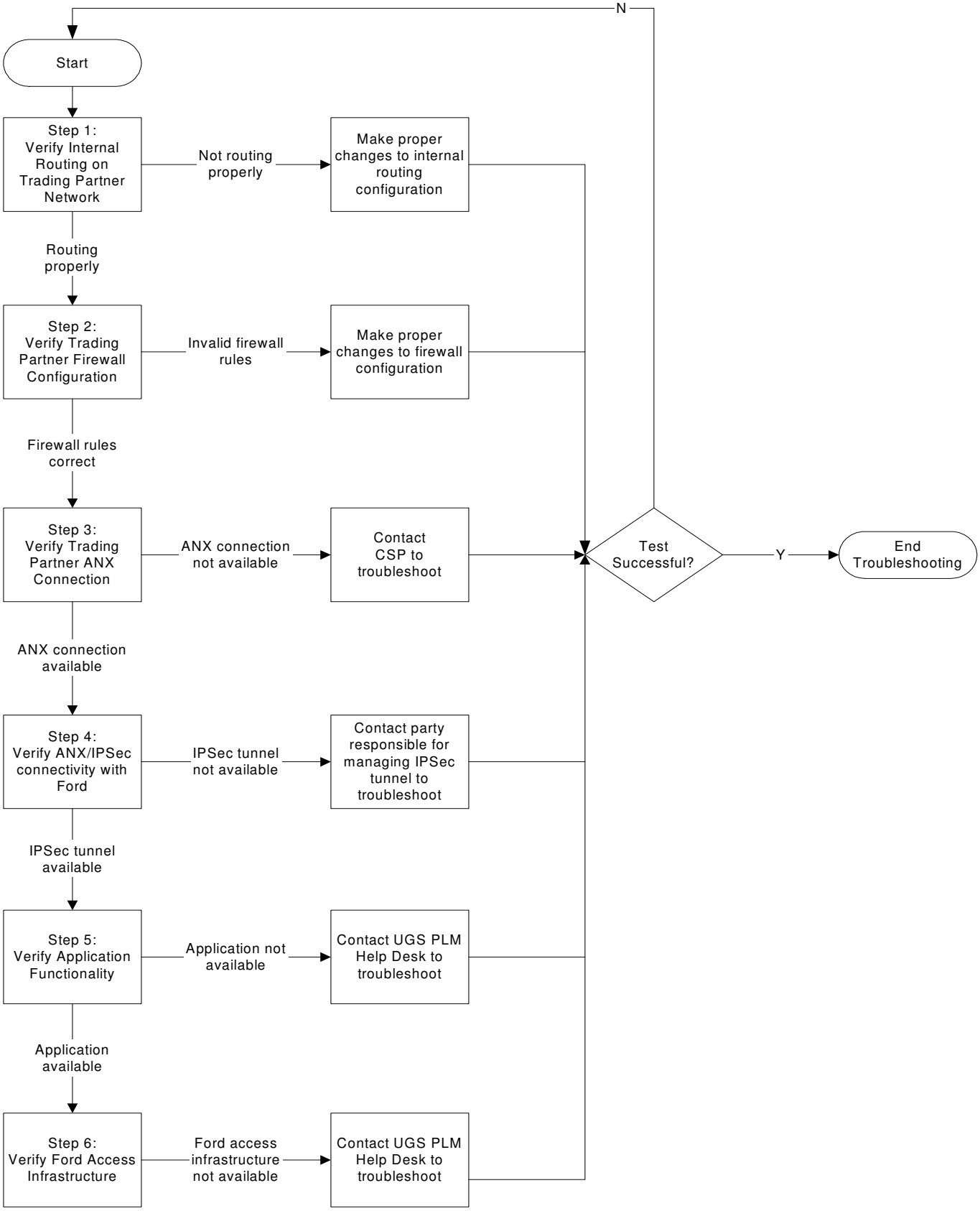
Step 4:	**Verify ANX Connectivity with Ford**
Action:	Verify network connection and IPSec tunnel with Ford.
	See page 7 for instructions
Responsible Party:	Trading Partner Network/Firewall Administrator

---------- UGS PLM Solutions Help Desk 800-955-0000----------

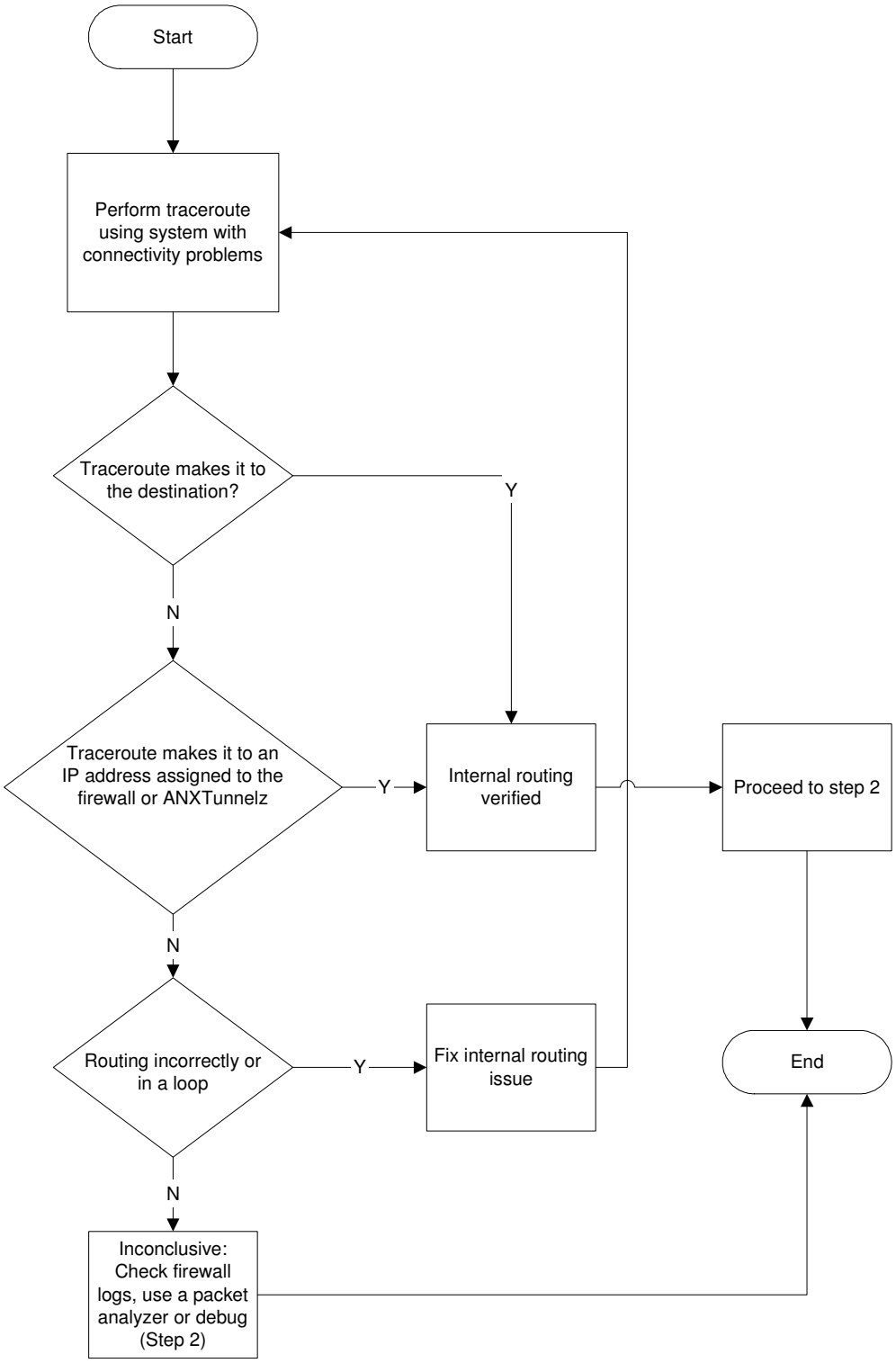
Step 5:	**Verify Application Functionality**
Action:	Verify C3P application is configured properly Verify application availability on Ford end.
	See pages 8-10 for instructions
Responsible Party:	UGS PLM Helpdesk 800-955-0000 (Keep ticket open until resolution)

Step 6:	**Verify Ford Access Infrastructure**
Action:	Verify steps 1-4 on Ford end. Verify Ford internal routing, Ford firewall rules, Ford ANX connectivity and Ford IPSec Connectivity.
Responsible Party:	If no resolution, UGS PLM will organize a conference call with Trading Partner and Ford resources

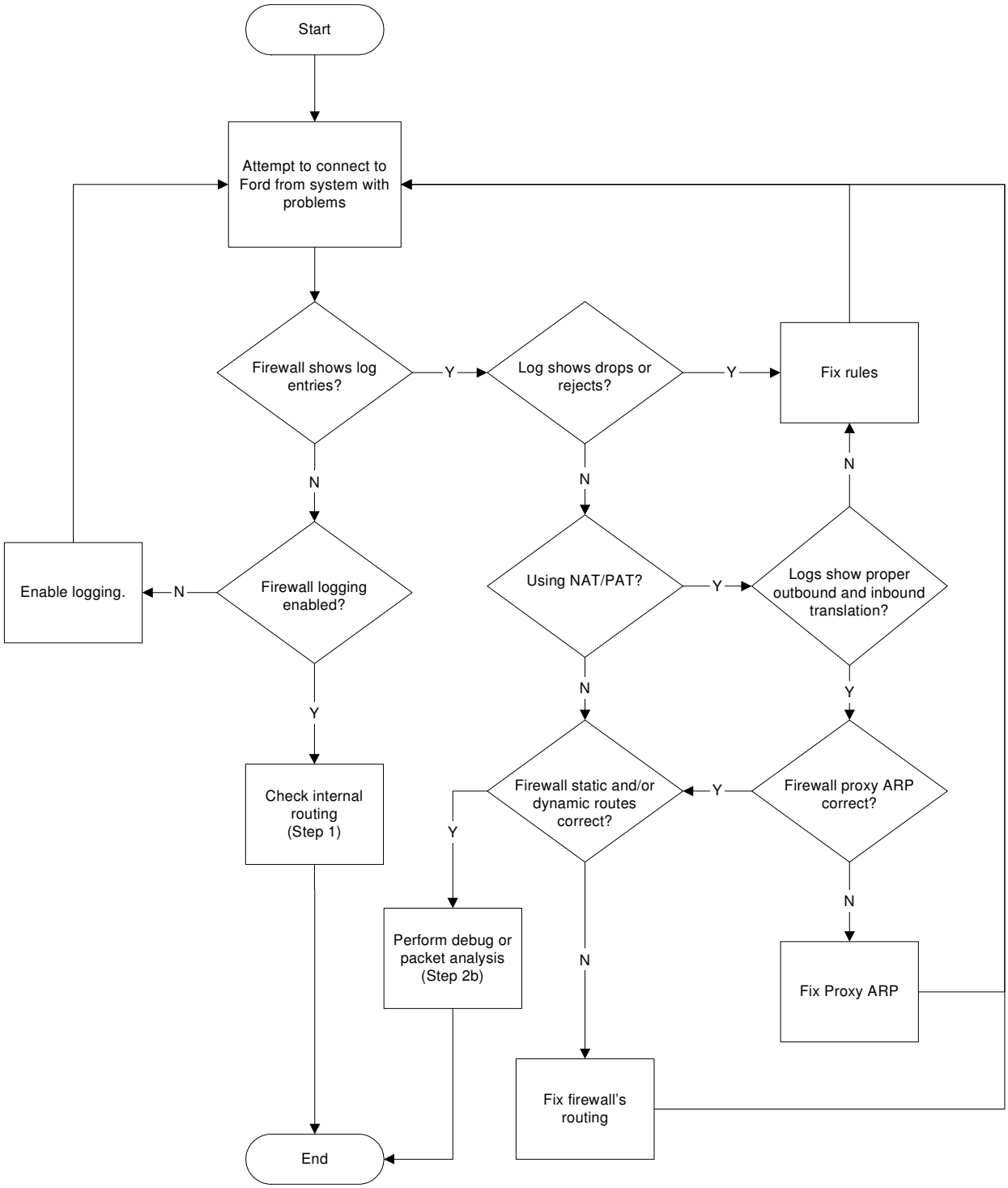
Ford ANX Troubleshooting Procedure for use by C3P Trading Partners



Step 1: Verify Internal Routing

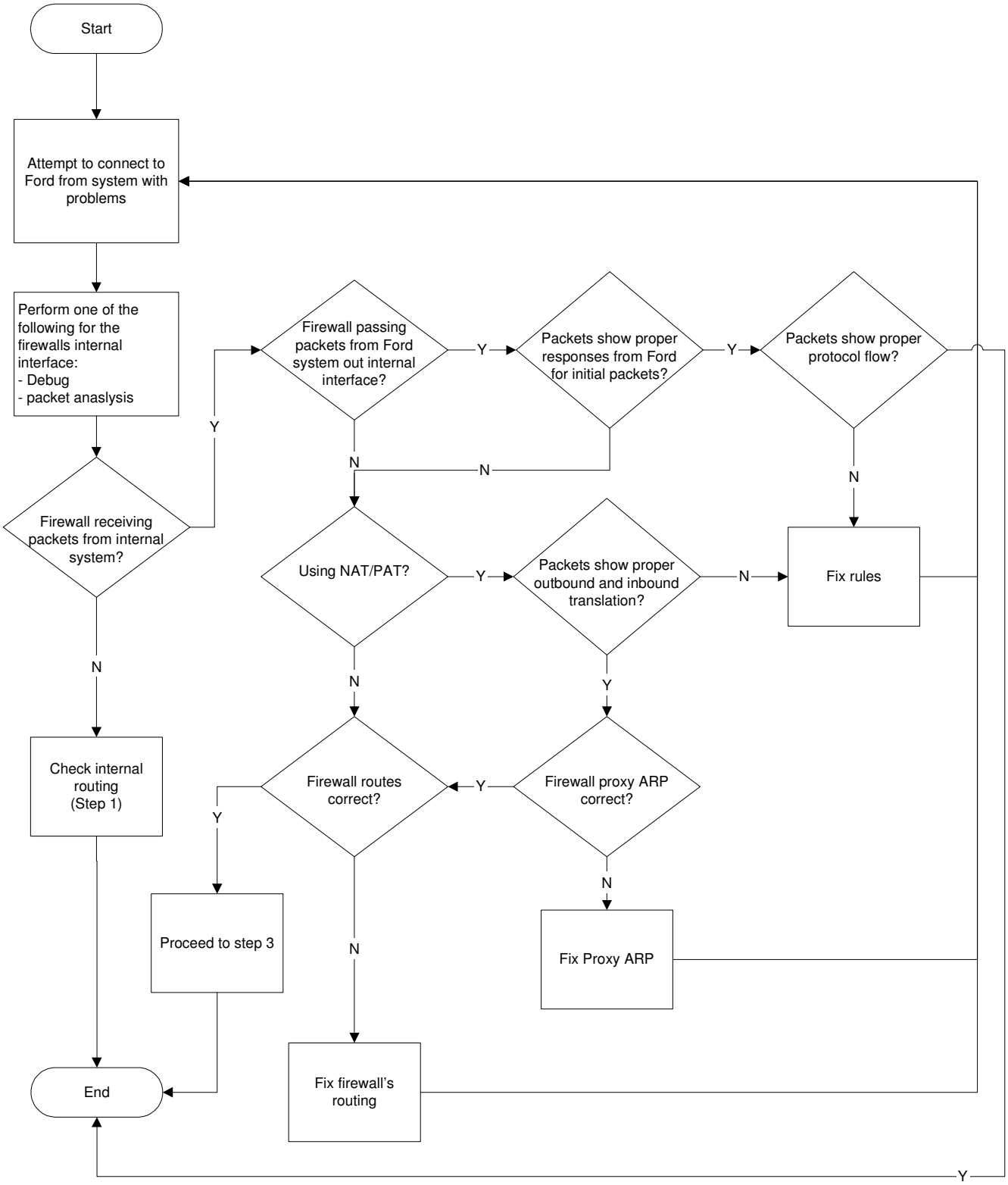


Step 2a: Verify TP ANX Egress: Firewall Logs



Ford ANX Troubleshooting Procedure for use by C3P Trading Partners

Step 2b: Verify TP ANX Egress: Firewall Packets



Step 3: Verify Trading Partner ANX Connection

1. Test application with other ANX trading partners.
    - If you can successfully communicate with another TP, your ANX transport connectivity is available. Move on to step 4.
    - If you cannot successfully communicate with another TP, your ANX transport connectivity should be evaluated. Contact your CSP Help Desk to troubleshoot your ANX connectivity.

2. Test all applications used to communicate with Ford.
    - If you can successfully establish a connection to any Ford application, your ANX transport connectivity is good. Move on to step 4.
    - If you are unable to successfully establish a connection to all Ford applications, your ANX transport connectivity should be evaluated. Contact your CSP Help Desk to troubleshoot your ANX connectivity.

Step 4: Transport Connectivity & Tunnel Verification

Verify IPSec tunnels are working properly.

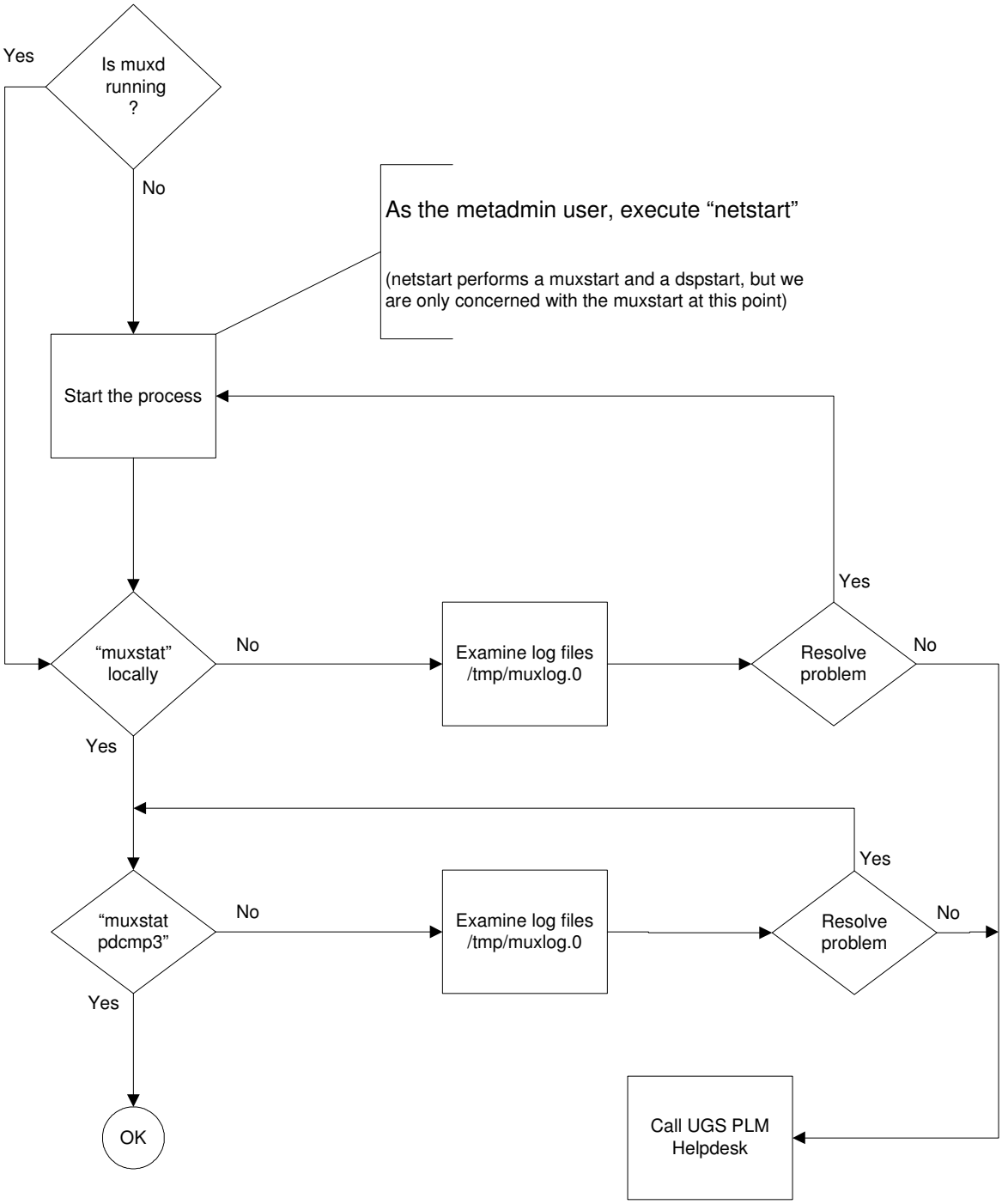
1. Ping the Ford ping test routers (19.12.1.35 and 19.12.2.29). IPSec connectivity is working if the ping receives a response.

   ****Note: Not all trading partners can ping through their company's firewall****

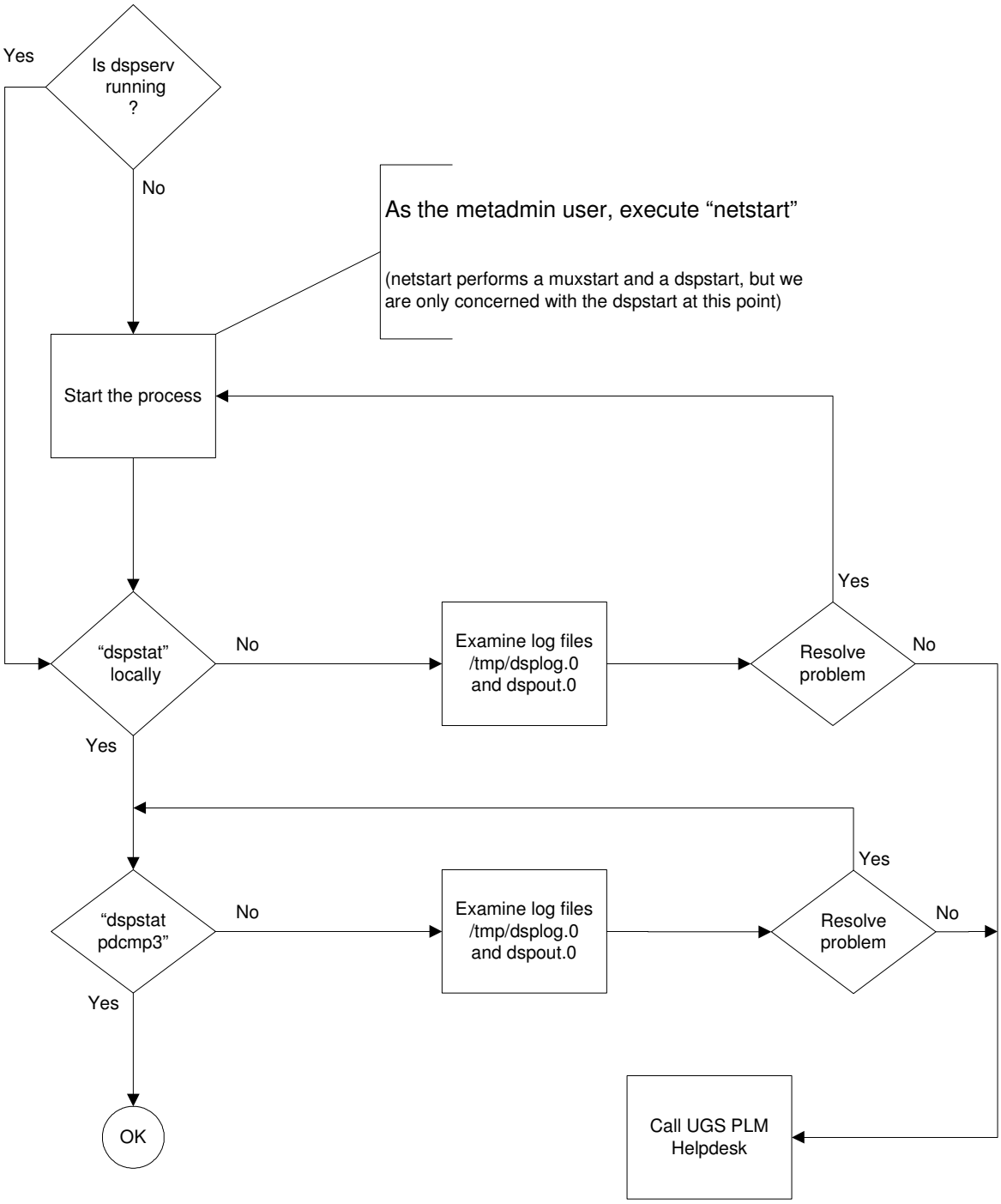
2. If the ping is unsuccessful and you are using ANXTunnelz, contact ANXeBusiness.

   - ANXeBusiness Customer Care Center: 877-488-8ANX
   - If using ANXTunnelz, use the ANXTunnelz website it to monitor IPSec tunnel availability.
     www.anx.com/ANXTunnelz.html

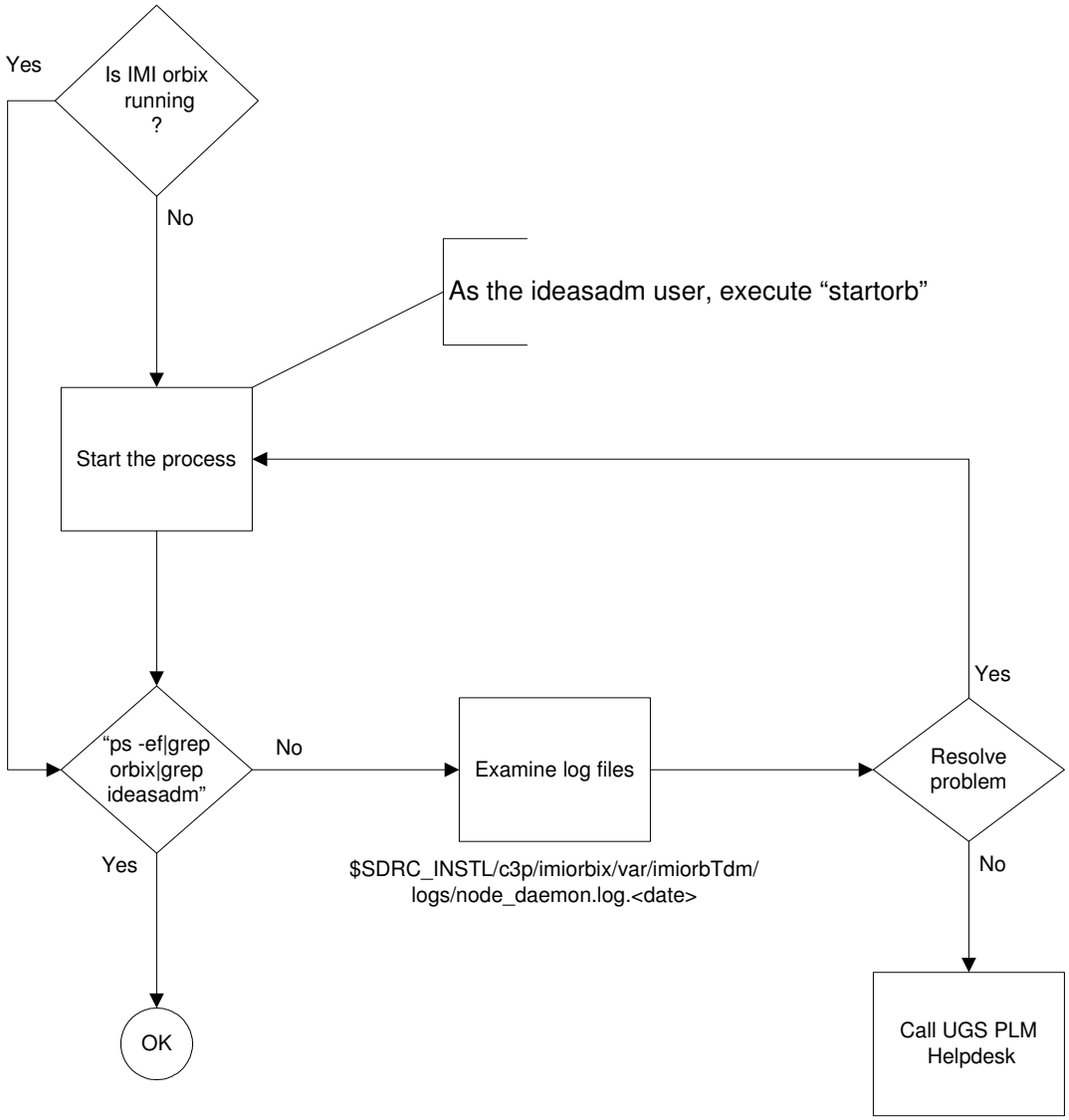
Step 5a: C3P Applications: MUX



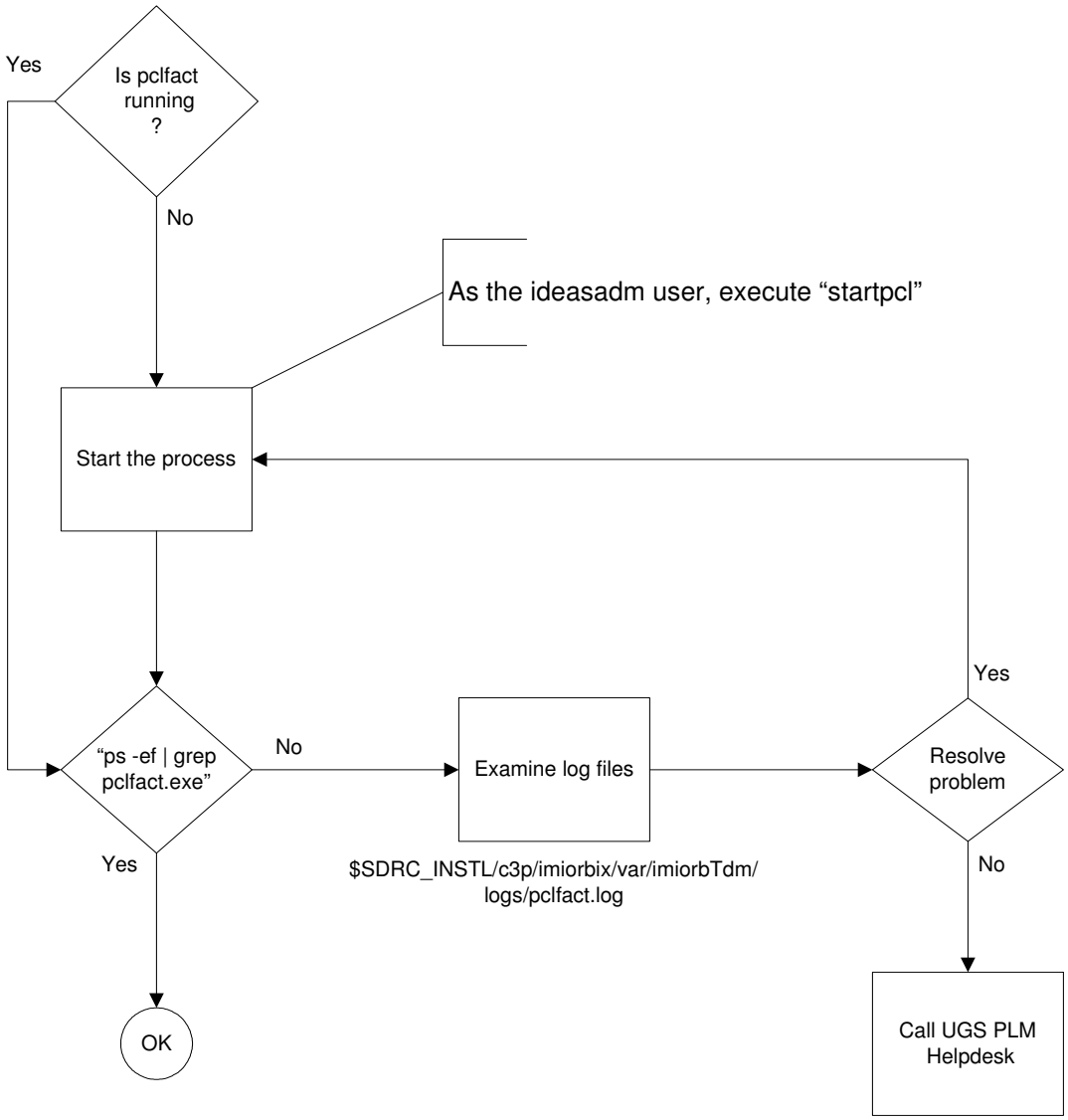
Step 5b: C3P Applications: Dispatcher



Step 5c: C3P Applications: IMI Orbix



Step 5d: C3P Applications: PCL Factory



Reference Guide for Steps 1 & 2 Troubleshooting

Traceroute

In many cases internal routing can be verified by using traceroute (tracert on Windows systems). This should be performed from the system experiencing the problem. *Depending on the security configured in the routers and firewalls the information may be limited or blocked (particularly by firewalls).*

Ping

Ping sends ICMP packets and listens for a response from the target system. Ping tracks the response time and lack of response from the target, which can be caused by a component between the endpoints. Large packets place additional stress and check for packet size issues.

Lack of response, loss of packets or error messages can indicate problems with the network communication and should be investigated

Sun: /usr/sbin/ping -s destinationaddr 30000 200
HP: /usr/sbin/ping destinationaddr 30000 200
SGI: /usr/etc/ping -s 30000 -c 200 destinationaddr
IBM: /usr/sbin/ping destinationaddr 8000 200
NOTE: The packet size of IBM's ping command is limited. If you set packet size too large ping will report a problem. Type CTRL-C to exit.
Windows: ping -n 200 -l 30000 destinationaddr
NOTE: Windows NT ping commands will not list sequence numbers nor will they report the number of packets transmitted and received. You must watch for "Request timed out" error messages. If you see a "Request timed out" error. You have lost a packet.

Ford ANX Troubleshooting Procedure for use by C3P Trading Partners

Firewall Logs

Depending on the firewall logging configuration the logs can be used to confirm packets are arriving at the firewall on the internal interface.

Cisco Debugging

Cisco routers and Pix firewalls have debugging commands that allow troubleshooting and can be used to verify packets are received on the internal interface.

Packet Analyzers / Captures

Many firewalls have the ability to analyze or capture packets for debugging purposes. Additionally there are dedicated packet analyzers and software that can be loaded on to systems that support promiscuous mode adapters. Listed here are some of the commonly available packages that are available with the operating system or Open Source.

Switches

Switches, *in their default configuration*, will prevent packet captures of packets that are not sent from or sent to the computer performing the packet analysis. This can be circumvented by using taps, hubs or configuring the switch to mirror traffic destined for certain ports to a port connected the computer performing the packet analysis.

Linux, IPSO and many Unix versions

Tcpdump (http://www.tcpdump.org/) – This is a command line tool that allows viewing of packets real-time or capturing the packets to a files for additional analysis. Tcpdump supports Berkeley Packet Filter (BPF) to filter out unwanted traffic. Captured data may be loaded into other applications, such as Ethereal, for additional analysis. IPSO uses a special file format with their version of tcpdump that can be converted to allow other application to read the file. See the tcpdump man page on IPSO for details.

Ethereal (http://www.ethereal.com) – This has a GUI interface and a command line interface (teathereal) that has more features than tcpdump.

SUN Solaris/SGI Irix

Snoop - is the application that comes with Solaris and Irix.

Windows

Windump (http://windump.polito.it/) – This is the windows version of tcpdump the command line tool that allows viewing of packets real-time or capturing the packets to a files for additional analysis. Windump *requires winpcap (http://winpcap.polito.it/)* to capture packets and supports Berkeley Packet Filter (BPF) to filter out unwanted traffic. Captured data may be loaded into other applications, such as Ethereal, for additional analysis. IPSO uses a special file format with their version of windump that can be converted to allow other application to read the file. See the windump man page on IPSO for details.

Ethereal (http://www.ethereal.com) – This has a GUI interface and a command line interface (teathereal) that has more features than windump. *Ethereal requires winpcap (http://winpcap.polito.it/) to capture packets when run on windows.*

CheckPoint

"fw monitor" – Since version 4.0 CheckPoint Firewall-1/VPN-1 has shipped with it's own packet analyzer that is independent of the underlying operating system.