Ford ANX Troubleshooting Procedure for use by 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

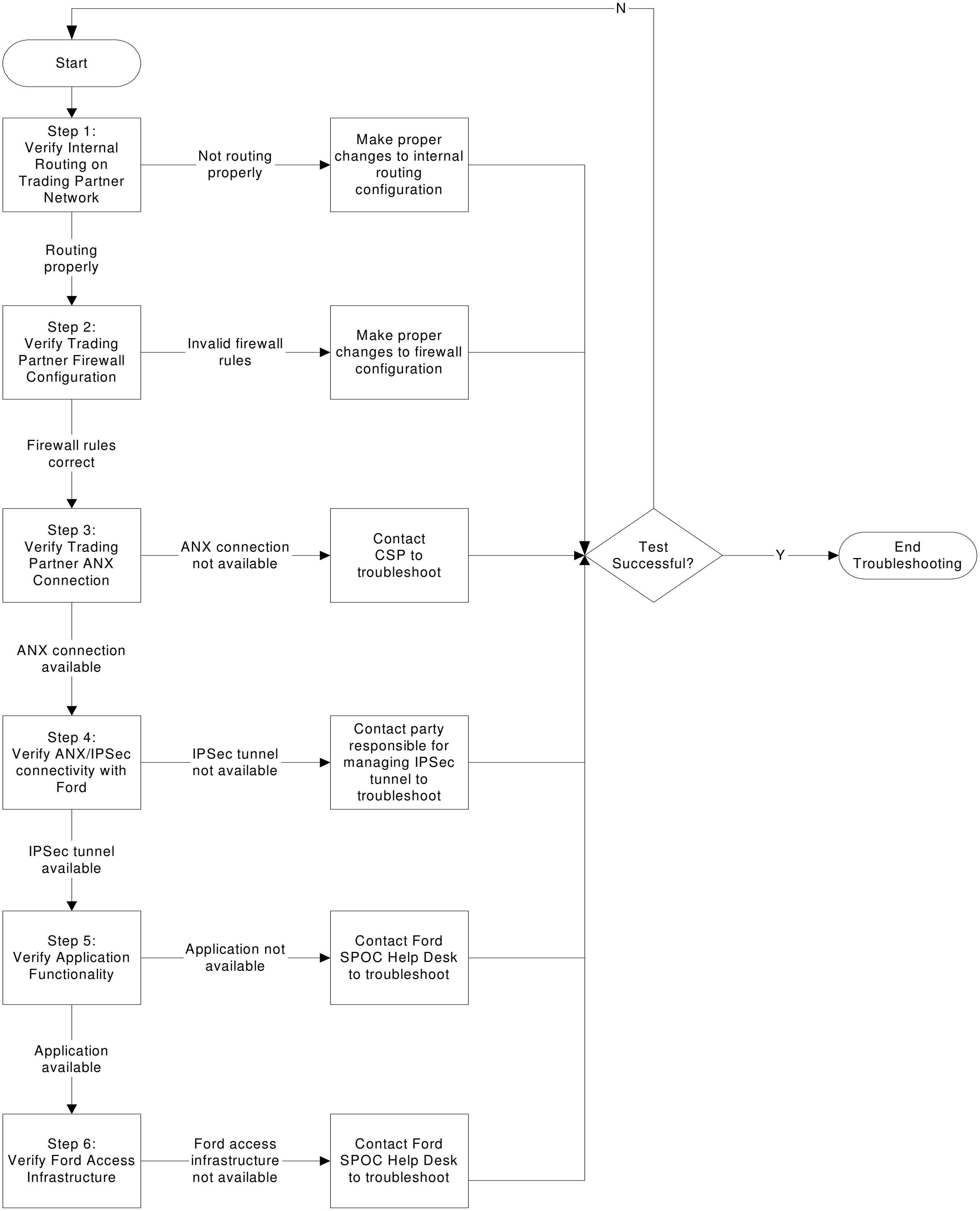
Step 4:	**Verify ANX Connectivity with Ford**
Action:	Verify network connection and IPSec tunnel with Ford. **See page 7 for instructions**
Responsible Party:	Trading Partner Network/Firewall Administrator

--Ford SPOC Help Desk 888-317-4957---------------------------------------

Step 5:	**Verify Application Functionality**
Action:	Verify application configuration on Trading Partner end. Verify application availability on Ford end.
Responsible Party:	1. Trading Partner Network/Firewall Administrator 2. Ford SPOC Help Desk: log ticket with application group 888-317-4957 (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:	1. Trading Partner Network/Firewall Administrator 2. Ford SPOC Help Desk: tell Help Desk to log an EL2 support ticket 888-317-4957 (Keep ticket open until resolution)

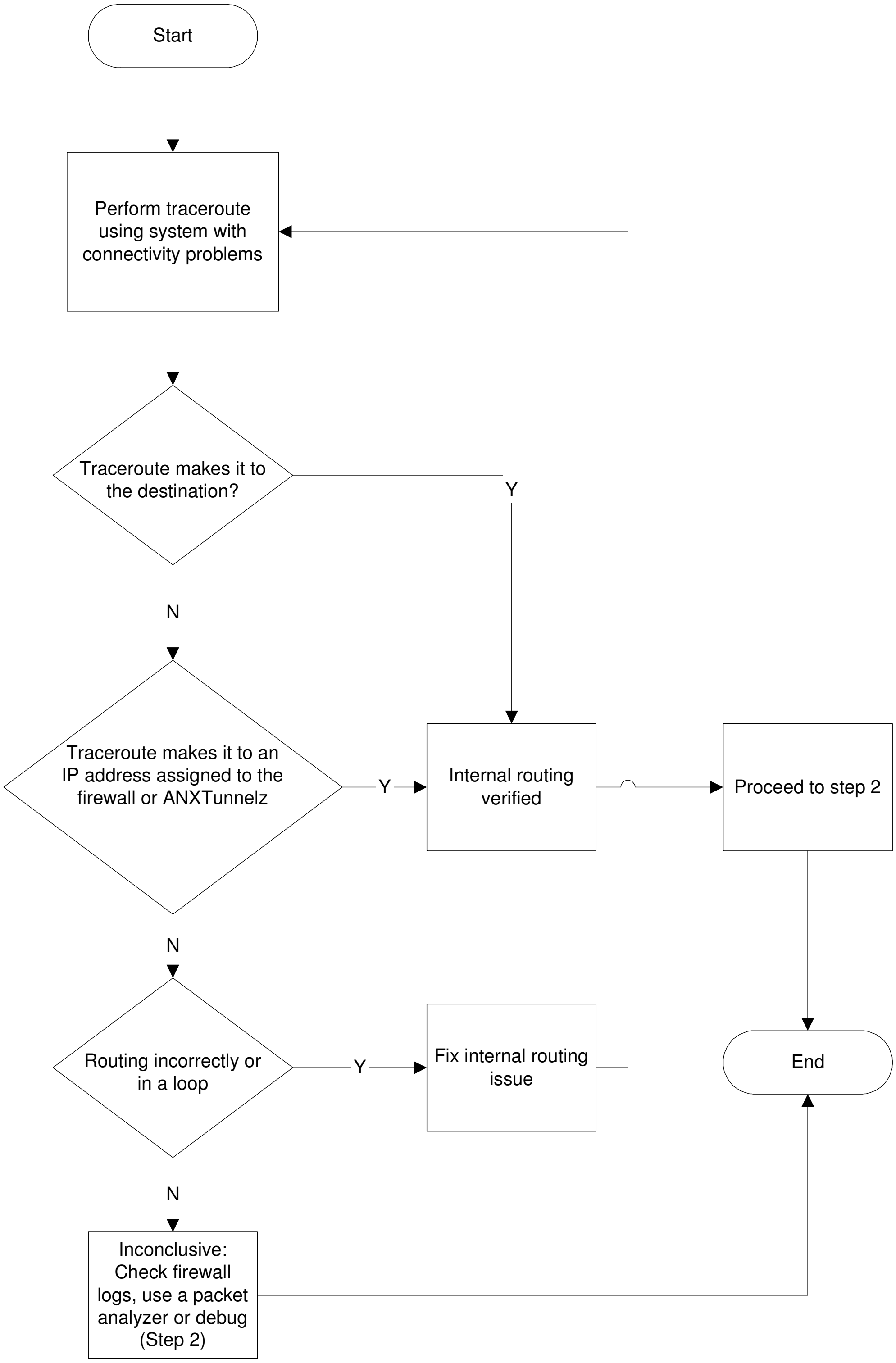
Ford ANX Troubleshooting Procedure for use by Trading Partners



N
Start
Step 1: Verify Internal Routing on Trading Partner Network
Not routing properly
Make proper changes to internal routing configuration
Routing properly
Step 2: Verify Trading Partner Firewall Configuration
Invalid firewall rules
Make proper changes to firewall configuration
Firewall rules correct
Step 3: Verify Trading Partner ANX Connection
ANX connection not available
Contact CSP to troubleshoot
Test Successful?
Y
End Troubleshooting
ANX connection available
Step 4: Verify ANX/IPSec connectivity with Ford
IPSec tunnel not available
Contact party responsible for managing IPSec tunnel to troubleshoot
IPSec tunnel available
Step 5: Verify Application Functionality
Application not available
Contact Ford SPOC Help Desk to troubleshoot
Application available
Step 6: Verify Ford Access Infrastructure
Ford access infrastructure not available
Contact Ford SPOC Help Desk to troubleshoot

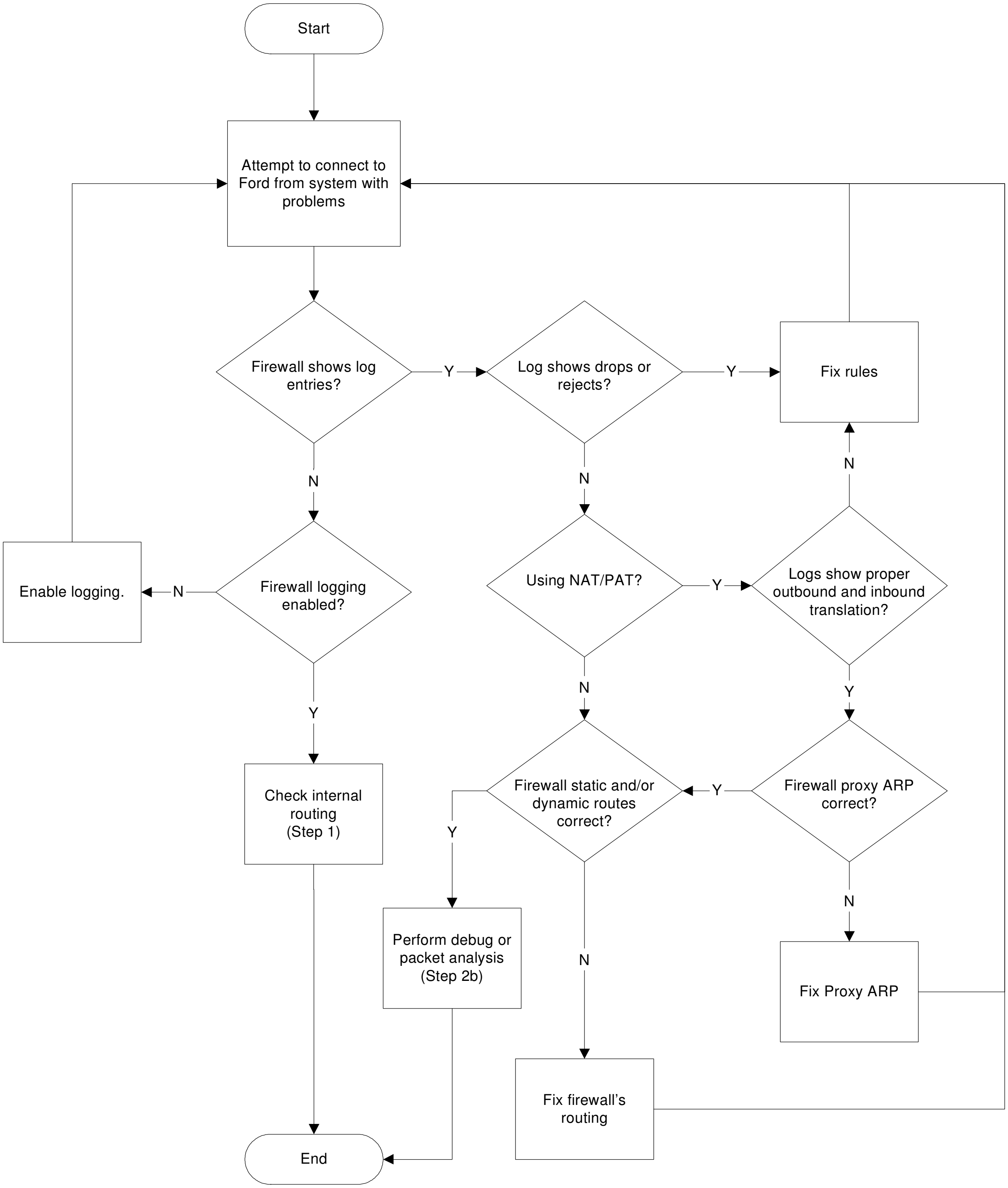
Ford ANX Troubleshooting Procedure for use by Trading Partners

Step 1: Verify Internal Routing


Start
Perform traceroute using system with connectivity problems
Traceroute makes it to the destination?
Y
N
Traceroute makes it to an IP address assigned to the firewall or ANXTunnelz
Y
Internal routing verified
Proceed to step 2
N
Routing incorrectly or in a loop
Y
Fix internal routing issue
End
N
Inconclusive: Check firewall logs, use a packet analyzer or debug (Step 2)

Ford ANX Troubleshooting Procedure for use by Trading Partners

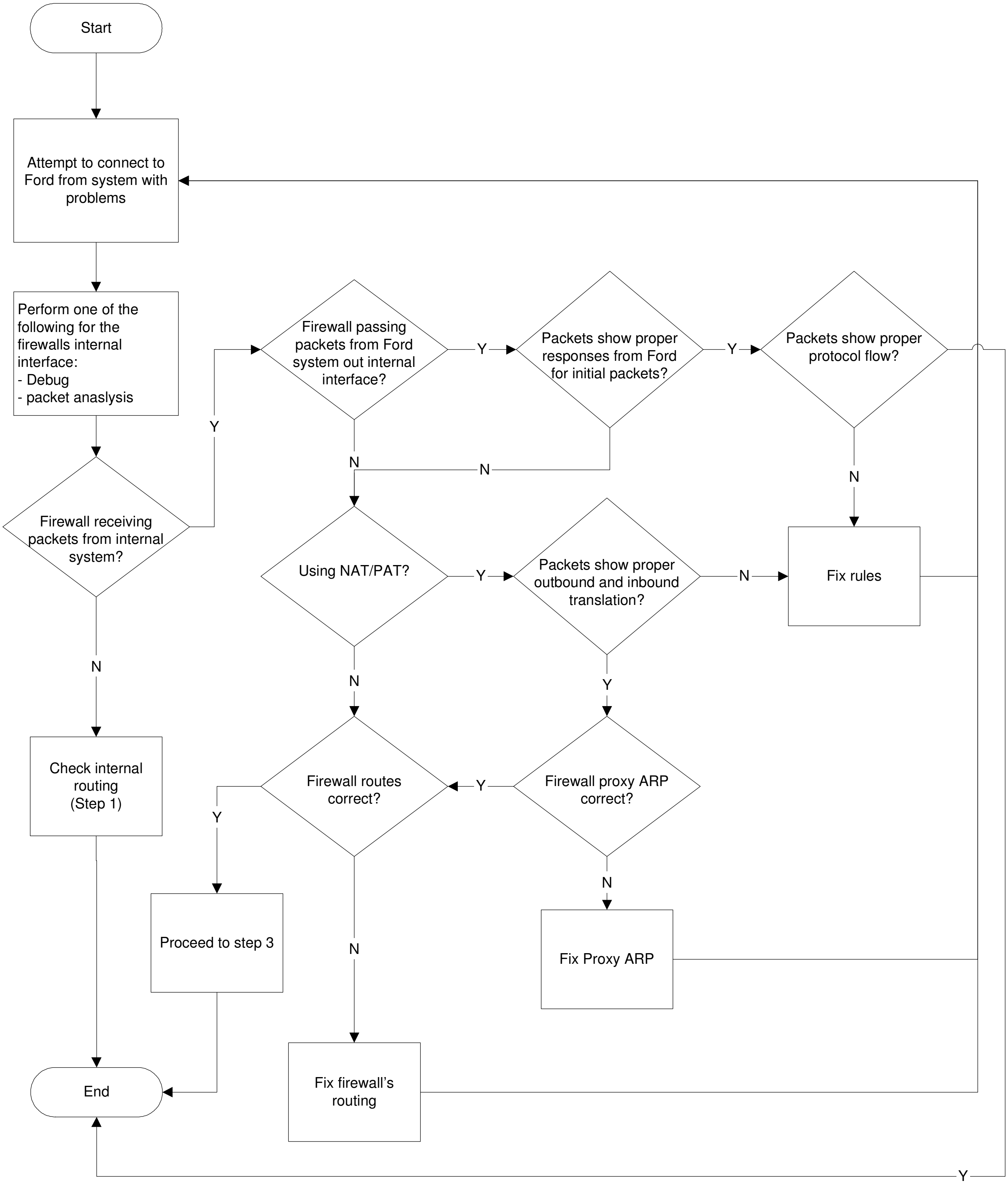
Step 2a: Verify TP ANX Egress: Firewall Logs



Start
Attempt to connect to Ford from system with problems
Firewall shows log entries?
Y
Log shows drops or rejects?
Y
Fix rules
N
N
N
Enable logging.
N
Firewall logging enabled?
Using NAT/PAT?
Y
Logs show proper outbound and inbound translation?
Y
N
Y
Check internal routing (Step 1)
Firewall static and/or dynamic routes correct?
Y
Firewall proxy ARP correct?
Y
N
Perform debug or packet analysis (Step 2b)
N
Fix Proxy ARP
Fix firewall's routing
End

Ford ANX Troubleshooting Procedure for use by Trading Partners

Step 2b: Verify TP ANX Egress: Firewall Packets


Start
Attempt to connect to Ford from system with problems
Perform one of the following for the firewalls internal interface:
- Debug
- packet anaslysis
Firewall receiving packets from internal system?
Y
N
Check internal routing (Step 1)
Firewall passing packets from Ford system out internal interface?
Y
N
Packets show proper responses from Ford for initial packets?
Y
N
Packets show proper protocol flow?
N
Fix rules
Using NAT/PAT?
Y
N
Packets show proper outbound and inbound translation?
N
Y
Firewall proxy ARP correct?
Y
N
Fix Proxy ARP
Firewall routes correct?
Y
N
Proceed to step 3
Fix firewall's routing
End
Y

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 to the Ford ping test routers (19.12.1.35 and 19.12.2.29). IPSec connectivity is working if the ping receives a response from either server.

   ****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 5 & 6: Verify Application Functionality & Ford Access Infrastructure

Once you have completed Steps 1-4, please contact the Ford SPOC Help Desk for further assistance. **Ford SPOC Help Desk can be reached at 888-317-4957.**

Please provide the following information:

1. What application are you trying to access?
2. Is internal routing configured properly?
3. Are firewall rules configured properly?
4. Is your IPSec tunnel an ANXTunnelz tunnel?
5. Has your ANXTunnelz tunnel been verified using the ANXTunnelz website? www.anx.com/ANXTunnelz.html
6. Can you complete a successful ping to the test routers?

7. 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).*

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.*

Ford ANX Troubleshooting Procedure for use by Trading Partners

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.