Tech Note 838

Resolving TCP Connection Restriction Issues for an Alarm Provider Running on a Workstation OS

All Tech Notes, Tech Alerts and KBCD documents and software are provided "as is" without warranty of any kind. See the **Terms of Use** for more information.

Topic#: 002630
Created: March 2012

Introduction

This *Tech Note* does the following:

- Explains what the Half-Open TCP Connections Limit is.
- Lists the OSs on which this Limit exists.
- Describes the potential connection issues for an Alarm Provider running on a Workstation with such Limit.
- Provides resolution options.

Application Versions

- All versions of Application Server and InTouch, when either one or both of them is serving as an Alarm Provider

Operating Systems

- Windows XP SP2 and SP3, Windows Vista SP1 or SP2 (with restriction registry enabled)
- Windows 7 (with restriction registry enabled)

Half-Open TCP Connections Limit

With the release of Windows XP SP2, Microsoft introduced a limit of 10 outgoing TCP connections in order to restrict the number of allowed, simultaneous, outgoing, half-open TCP connections. The restriction was an attempt to prevent a virus or malicious program to make unlimited infectious connections to other systems when the PC is compromised. This limit also exists in Windows Vista RTM, with or without SP1.

Because of enhanced security features in both design and coding, the connection limit is removed beginning with Windows Vista SP2 and Windows 7, and does not exist in any of the Server OSs, such as Windows 2003 and 2008. However, the limit can still be enforced with a registry key added to the Windows Vista SP2 and Windows 7 Operating Systems.

Impact on Wonderware Alarm Providers

The connection between an alarm client, such as AlarmViewer control in InTouch, and the alarm provider is TCP. This means that when an Alarm Provider is running on a Windows workstation such as Window XP SP2 or later where this Limit exists and is enforced, the maximum number of outbound TCP connections from the alarm provider will be less than 10, because there are always TCP connections created by the OS and third-party applications.

When the TCP connection limit is reached, in either the existing or newly opened alarm clients, you can see some or all of the following:

In **Summary** (query) mode, while the query is shown as 100%,

- None of active alarms is showing, or
- Only a subset of the active alarms are showing, or
- The alarms alternate randomly between appearing and disappearing.

In **Historical** (query) mode, while the query is shown as 100%,

- None of the historical alarms and events is showing, or
- Only a subset of the historical alarms and events are showing, or
- The alarms and events alternate randomly between appearing and disappearing.

Diagnosing the TCP Connection Limitation

To identify when and if this Limit has been reached, the following methods should be used:

Check the System Event Viewer

When this Limit is reached, **Event ID 4226** will be logged in the System Event log, with a message like

```
TCP/IP has reached the security limit imposed on the number of concurrent TCP connect attempts.
```

Use the NETSTAT DOS Command

This command, with various parameters settings, will return a list of concurrent TCP connections, and their connection status.

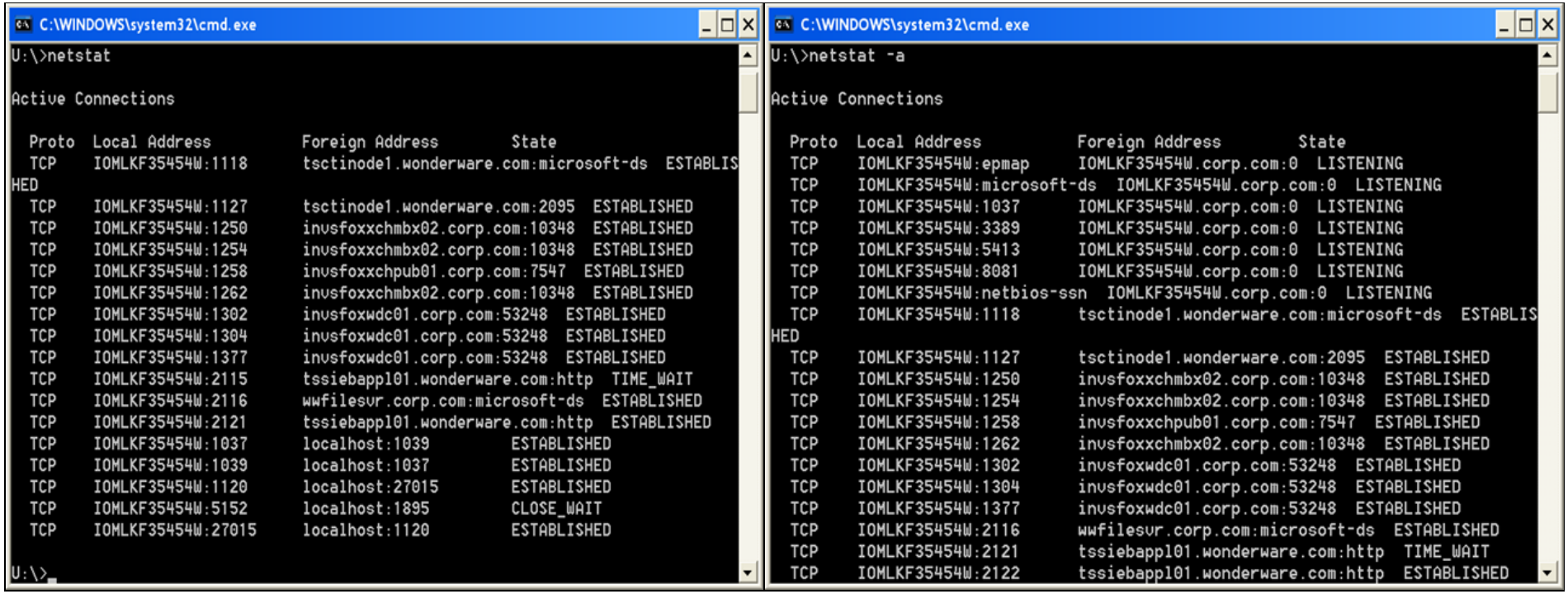

Figure 1: List of Concurrent TCP Connection Status Returned From NETSTAT Command

Resolution Options

- Replace the Workstation OS with a Server OS for Alarm Provider computers.
- Consult Microsoft, or search the internet for **Remove Half-Open TCP Connection Limit** or **Remove Concurrent TCP Connection Limit** for solutions.

Note: Invensys does not support, nor is responsible for any of the solutions provided by third-parties.

C. He

Tech Notes are published occasionally by Wonderware Technical Support. Publisher: Invensys Systems, Inc., 26561 Rancho Parkway South, Lake Forest, CA 92630. There is also technical information on our software products at **Wonderware Technical Support.**

For technical support questions, send an e-mail to **wwsupport@invensys.com**.

Back to top

©2012 Invensys Systems, Inc. All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, broadcasting, or by anyinformation storage and retrieval system, without permission in writing from Invensys Systems, Inc. **Terms of Use.**