Technical Note: \textit{xxNETserver/PC}\textsuperscript{TM}:
Configuring A Well-Site VPN Server

\textit{Draft #4}

\textbf{Prepared by:} Lawrence R. Bulduc & Paul J. Nelson
XXT Incorporated
3350 Scott Boulevard
Building Number Thirty
Santa Clara, CA 95054-3105

\textbf{Date:} Wednesday, March 19, 2008
\textbf{Project:} XXT Project: x1011 (xxMWD/PC)
\textbf{Document:} XXT #TN-08031901/LRB/PJN
\textbf{File:} XXT-TechNote-VPN-ConfiguringWellsiteVPNServer.doc
\textbf{Origin:} “Configuring a Well-site VPN Server”, Revision C,
PJN/XXT/18Mar2008
\textbf{Revision:} Original, Draft #1, Wednesday, March 19, 2008
Draft #2, Friday, March 21, 2008
Draft #3, Wednesday, April 02, 2008
\textit{Draft #4, Friday, April 04, 2008}

\textcopyright Copyright 2008 XXT incorporated
\textit{All Rights Reserved}
NOTE

xxOS/12™, xxBOOT™, xxBOOT/12™, xxNET™, xxLIB/12™, xxMPRx™, xxMPTx™, xxMWD™, xxEMT™, xxEMTxRx™, xxDRT™, xxSAPC/PC™, xxMWDconfig/PC™, xxTFOutility/PC™, xxRollTest/PC™, xxDirKUtility/PC™, xxNETserver/PC™ and xxNETmonitor/PC™

are trademarks of XXT incorporated
xxNETserver/PC™: Configuring A Well-Site VPN Server

Overview

This application note describes how an administrator may configure a PC at the well site to act as a VPN (Virtual Private Network) server allowing a remote user to connect over the internet. For a discussion of how to set up the remote PC to connect to the well site, see the related XXT tech note: “xxNETserver/PC™: Connecting to a Remote Well-Site Using a VPN” (PDF File: “XXT-TechNote-VPN-ConnectingToRemoteWellsite…”)…

By convention, XXT documentation that is released with the xxDRT/PC™ Program Suite is stored in the c:\Program Files\XXT Incorporated\xxDRT-PCSuite\Documentation folder and may be accessed directly from most applications by clicking on the “Browse Documentation” option in the Help pull-down menu.

The following describes one method of configuring a VPN server using the facilities built into Microsoft Windows. There are other third-party VPN solutions available, which should be fully compatible with XXT / xxMWD™ software although other implementations have not been tested. It should be noted that the various internet protocol layers, including the VPN connection, are in-fact transparent to xxNETserver/PC™ and other XXT applications.

Definitions

MAC Address

A MAC (Media Access Control) address is a quasi-unique identifying number associated with the network interface hardware in a PC or other network component, such as a cable modem, router or network printer. By convention MAC addresses are written as six groups of 2 hexadecimal digits, for example 20-1B-33-00-00-1E.

IP Addresses

Two varieties of IP address are involved in setting up the VPN: WAN Addresses and Local Addresses…

Local Addresses

Local Addresses are those in one of the three IANA-defined private address ranges:

<table>
<thead>
<tr>
<th>Block</th>
<th>Start of range</th>
<th>End of range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block A</td>
<td>10.0.0.0</td>
<td>10.255.255.255</td>
</tr>
<tr>
<td>Block B</td>
<td>172.16.0.0</td>
<td>172.31.255.255</td>
</tr>
<tr>
<td>Block C</td>
<td>192.168.0.0</td>
<td>192.168.255.255</td>
</tr>
</tbody>
</table>

Local addresses may be assigned either dynamically (DHCP) or may be manually defined. Small routers will generally come preconfigured to dynamically assign IP addresses from some portion of block C.

When setting up the VPN, the administrator will choose local addresses from one of these address ranges which must not conflict with the addresses in use by any other PCs at the well site.
**WAN Addresses**

WAN addresses are any non-local address. When a PC or router is connected to a satellite or cable modem at the well site which is connected to an internet service provider (ISP), it will supply its MAC address to that ISP, which will then assign a WAN address to that MAC address and thus to that PC or router. NOTE: This address may be changed at any time by the ISP, and if the satellite or cable modem is reset the likelihood is very high that a new IP address will be assigned. Likewise, whenever a broadband mobile connection is established a new IP address will be assigned. See the section **Dynamic DNS** below.

**Hostname**

The Hostname of a PC is the name defined as the computer name when Windows is configured. To determine the hostname of a PC, right click on “**My Computer**”, select “**Properties**”, go to the “**Computer Name**” tab and make a note of the name labeled “Full computer name”.

**DNS**

DNS (Domain Name System) addresses are text strings associated with WAN addresses, for example [www.google.com](http://www.google.com) is associated with “209.85.173.147”. DNS servers provide a public means for network applications to retrieve the numeric WAN Address associated with a given text string.

**Dynamic DNS**

To avoid problems due to WAN IP addresses being changed by the ISP, it is highly recommended that a dynamic DNS service be used along with a DDNS-capable router, or DDNS software when a router is not used. A dynamic DNS service allows you to automatically associate the numeric WAN address with a stable text string, for example “PNTest01.dnsalias.org”. If the ISP changes your WAN address, the router or DDNS software automatically updates the dynamic DNS service. There are many dynamic DNS services available, although routers will generally support only a few specific ones. During testing, XXT have successfully used [DynDNS](http://www.dyn.com) as a DDNS provider. However, XXT have not evaluated any other DDNS providers and does NOT recommend or endorse the use of DynDNS over any other provider. A Google search will find many DDNS providers.

**Mobile Broadband Connection**

As used in this document, “**Mobile Broadband Connection**” refers to the use of cellular-phone modem broadband connections to the internet. When configuring a VPN Server PC to use this type of connection, follow the [Connecting Directly To The Internet](http://www.xxtinc.com) instructions even though a router may be used to connect other well-site components to the VPN Server PC.
Administrator Requirements

The administrator will be required to perform the following PC tasks, as described later in this document:

⇒ Determine the hostname of the VPN server PC
⇒ Define one or more user accounts on the VPN server PC
⇒ Configure the VPN server and enable remote logon for the user accounts.
⇒ Configure the PC security settings
⇒ Configure the PC firewall, if any

In addition, if a router is used the administrator will need to be able to perform some or all of the following tasks:

⇒ Determine the current address of the router on the internet
⇒ Assign a fixed IP address to the VPN server PC
⇒ Forward port 1723 to that IP address
⇒ Determine the current primary and secondary DNS server addresses
⇒ Register the router with a DDNS provider

Refer to the router manual for the specifics of performing these tasks. Different manufacturers use varying configuration screens and terminology, such as “Port Forwarding”, “Virtual Server”, or “Rules”. Some may have the VPN port (1723) predefined in a list, while in others you may have to enter port 1723 manually. Some routers make it simple to assign a fixed IP address to a PC while others do not.

Configuration Procedure

The first part of the configuration procedure is dependent on the way that the well-site internet access is connected to the PC.

If the internet is connected through a cell modem/Mobile Broadband Connection, through a network cable directly to a cable modem, or otherwise directly to the internet, see the section Connecting Directly To The Internet below.

If the internet is connected to a router, which then provides the internet to the PC, see the section Connecting to the Internet Through a Router below.

Note that, even if a router is being used to connect multiple PCs at a well site, if the internet connection is NOT provided through the router then see the section Connecting Directly To The Internet below.
Connecting Directly To The Internet

Connecting directly to the internet specifically means that the internet connection is not made through a router, although a router may be required to connect other well-site LAN components or may be desired for greater security. Again, if a router is used to connect to the internet, refer to the Connecting to the Internet Through a Router section below to configure the PC.

Determining the WAN Address

Go to the Start menu, select Run, enter “cmd” (without the quotes) and click OK. A DOS box will open. Enter “ipconfig” at the prompt and the IP address assigned by the ISP will be displayed. Make a note of this address. This is the Well-site IP Address that will be used by the remote user when the remote VPN connection is created (refer to the related XXT tech note: “xxNETserver/PC™. Connecting to a Remote Well-Site Using a VPN” (PDF File: “XXT-TechNote-VPN-ConnectingToRemoteWellsite…”)).

Caution: The “ipconfig” response may include multiple IP addresses for multiple connections, such as an wireless, dial-up and mobile broadband connections: Be sure to select the IP Address for the applicable connection.

Configuring the VPN Server

Continue to configure the VPN server starting at the Configuring the VPN Server section below.

Mobile Broadband Connection Notes...

There are several sources of Mobile Broadband Connection services and hardware. During testing, XXT have successfully used a factory-installed (built-in) Dell Wireless 5720 VZW Mobile Broadband (EV-DO Rev-A) card in a Dell Latitude D830 (Windows XP; SP2) and Verizon Wireless Data Service. However, XXT have not evaluated any other Mobile Broadband Connection services and hardware and does NOT recommend or endorse the use of Dell or Verizon over any other hardware and service providers.

In its testing with this specific mobile broadband hardware and service combination, XXT found that it was not necessary to make any special adjustments to the standard Dell-Verizon configuration nor was it necessary to create a special profile.

Note: In the above noted Mobile Broadband testing, the client PC was a Dell Latitude D830 running Vista Ultimate, Version 6.0, and a 26.4 kb dial-up connection.
**Connecting to the Internet through a Router**

**Determining the WAN Address**

Using the router’s user interface, determine the WAN IP address of the router. If possible, register this WAN IP address with a Dynamic DNS service. This is the **Well-site IP Address** that will be used by the remote user when the remote VPN connection is created (refer to the related XXT tech note: “xxNETserver/PC™: Connecting to a Remote Well-Site Using a VPN” (PDF File: “XXT-TechNote-VPN-ConnectingToRemoteWellsite…”)).

**Designating the VPN server PC**

When more than one PC is present at the well site, a router is used to connect them together and to the WAN. One PC must be designated to serve as the VPN server, and it must be assigned a fixed IP address.

*Example:* Let’s assume that (a) our router uses Local IP addresses in the range 192.168.1.1 to 192.168.1.255, (b) we have a DRT PC, an SAPC PC in the safe area, and (c) there’s possibly a second SAPC PC. We designate the SAPC in the safe area as our VPN server and assign it Local IP address 192.168.1.200

Most routers allow the administrator to assign a fixed IP address to a given MAC address, even if it is configured to assign addresses dynamically to other PCs. This is the preferred method for assigning the VPN server address.

If the router does not support this capability, the VPN server address must be defined in Windows. Before doing this, the administrator must use the router user interface to determine the current primary and secondary DNS server addresses, subnet mask and default gateway...

⇒ On the desktop or Start Menu, right click on “My Network Places” and select “Properties” from the popup menu to open the “Network Connections” window.

⇒ Right click on “Local Area Connection” and again select “Properties”. Note: If more than 1 Local Area Connection option, select the one connected to the router.

⇒ Double click the entry labeled “Internet Protocol (TCP/IP”).

⇒ Select the “Use the following IP address” button.

⇒ Enter the desired IP address, subnet mask, default gateway and DNS server addresses and click OK.

**Enabling the VPN in the Router**

In the router, forward port 1723 to the Local IP address of the VPN server.

*Example:* Continuing the above example, we forward port 1723 to 192.168.1.200

**Configuring the VPN Server**

Continue to configure the VPN server starting at the **Configuring the VPN Server** section that follows.
Configuring the VPN Server

Windows Vista OS Reference

If using the Vista operating system, please refer to “Setting up the Vista Point-to-Point Tunneling Protocol (PPTP) Virtual Private Network (VPN) Server” located at the following link: http://theillustratednetwork.mvps.org/Vista/PPTP/PPTVPN.html. Please use this reference in conjunction with the recommendations below.

Choosing Local IP Addresses for the VPN Connection

The VPN connection will use a block of two more contiguous Local IP addresses for communications with the remote user. These addresses must be chosen not to conflict with other Local IP addresses. However, users connecting over a public Wi-Fi, such as hotels or coffee shops, will be assigned an IP address that most likely will be in the 192.168.xxx.xxx range. If an IP address chosen for the VPN connection happens to be the same as an address on that local network, problems may occur. It is suggested that the VPN address be chosen from the range 172.16.xxx.xxx to reduce the likelihood of any conflict.

NOTE: Windows XP and Windows Vista only allow one VPN connection at a time, so it is only necessary to assign a block of two addresses. To allow more than one VPN connection it will be necessary to run under Windows Server 2003 or later.

Example: We choose 172.16.2.100 as the starting address for the VPN server. This is the VPN Server IP Address that will be used by the remote user when connecting to the well.

Enabling the VPN Server on the PC

⇒ On the desktop or Start menu, right click on “My Network Places” and select “Properties” from the popup menu. Double click the “New Connection Wizard”.
⇒ On the Network Connection Type page select the “Set Up An Advanced Connection” option and click “Next”…
⇒ On the Advanced Connection Options page select the “Accept Incoming Connections” option and click Next.
⇒ On the Devices For Incoming Connections page you may select optional devices on which you want to accept incoming connections, but this appears to not be necessary. For a Mobile Broadband Connection, select that device. Click Next.
⇒ On the Incoming Virtual Private Network (VPN) Connection page select the “Allow Virtual Private Connections” option. Click Next.
⇒ On the User Permissions page select the users that are allowed to make incoming VPN connections. To add a new user select “Add…” fill in the “New User” attributes and make a note of the User Name(s) and Password(s). Click Next.
⇒ On the Networking Software page click on the Internet Protocol (TCP/IP) entry and click the Properties button…
**xxNETserver/PC™: Configuring A Well-Site VPN Server**

⇒ In the **Incoming TCP/IP Properties** dialog box there is an **Allow Callers To Access My Local Area Network** check box. Checking this will allow VPN callers to connect to other computers on the LAN. If this check box isn’t selected, VPN callers will only be able to connect to resources on the Windows XP VPN server itself and not on other PCs on the well-site LAN (other than xxMWD™ applications via the xxNETserver/PC™). **It is recommended** that you leave this unchecked unless there is a specific reason to enable it. Below this checkbox, be sure that the **Specify TCP/IP Address** button is **selected**. Enter the VPN IP Address chosen above as the starting address, and define an ending address greater than the starting address. Click OK to return to the Networking Software page and then click “Next”, and then “Finish”.

**Example:** Continuing the above example, we would enter 172.16.2.100 as the starting address and 172.16.2.101 as the ending address.

**OS Limitations Note:** If running under **Windows Server 2003** or later, the number of simultaneous VPN connections allowed will be limited to the size of the block of IP addresses defined in this screen. So, if in our example an ending address of 172.16.2.105 were used (6 addresses total), the PC would support 5 remote connections. However, **Windows XP and Vista limit VPN connections to one regardless of the number of addresses defined in this block.**

**Configuring the VPN Server Security Settings**

⇒ On the start menu, click run and enter “secpol.msc” to run the Security Policy applet.
⇒ In the left-hand window, expand “**Local Policies**” and select “**Security Options**”...
⇒ In the right-hand window, find the entry “**Accounts: Limit local account use of blank passwords to console logon only**”. If it is “Enabled”, double click the entry and change it to “**Disabled**”...
⇒ In the left-hand window, select “**User Rights Assignment**”...
⇒ In the right-hand window, find the entry “**Access this computer from the network**” and double click it. A properties dialog will be displayed showing all logon groups authorized to access the PC over the network. Any user account which will be used to logon to the well site VPN server must be a member of a logon group listed in this dialog. To give all users access, click the “Add User or Group” button, enter “Everyone” in the text box, and click the “Check Names” button. “Everyone” should now be underlined. Click OK twice to make the change. You may receive a warning message referring you to a Microsoft web page which discusses security issues. Click OK to close the warning.
⇒ Close the Security Policy applet.

**Configuring xxNETserver/PC™**

**Run xxNETserver** and use the Connections | Configure Remote Access menu to open the Configure Remote Access dialog. Check the checkbox labeled “**Allow remote user access to this well**” and click OK.

**Configuring the Firewall**

If firewall software is being used, it will be necessary to unblock port 1723...
Allowing Access on Port 1723 ("Point-to-Point tunneling protocol")

There are several providers of internet security products available for Windows and XXT does NOT recommend or endorse the use of any one product over another. Please refer to your company procedures and requirements regarding PC firewalls before proceeding. However, that said, XXT was successful in testing with Windows firewall while it did experience issues with 3rd party firewall applications. Unfortunately, due to the large number and variations in these types of products, XXT will generally not be able to provide support or recommendations for other than Windows firewall.

Windows Firewall

XXT recommends that you first refer to Windows Help: “Opening ports in Windows Firewall” to understand some of the risks associated with unblocking ports. Also, for more information, see How to Open Ports in Windows Firewall on the Microsoft Web site (http://www.microsoft.com/). Normally if using a 3rd-party firewall, Windows firewall is disabled.

Symantec/Norton Products

There are several versions of Norton/Symantec internet security products. In general, you need to first navigate to the internet security “General Rules” dialogue and then create a rule to allow limited access to the VPN server PC from the remote site(s) via Port 1723…

⇒ Navigating to the General Rules Dialogue: Unfortunately, Symantec seems to modify the user interface each year, including terminology, making it difficult to provide assistance. You may be able to get help navigating to this dialog for your specific product at www.symantec.com/norton/support/index.jsp. However, for your convenience, XXT offers the following suggestion on a few of the common Symantec products to navigate to the “General Rules” dialogue window…

**Norton SystemWorks (Premier V11.0):** Open Norton >> select the Norton Antivirus tab >> expand “Settings” >> expand “Web Browsing” >> Click “Internet Worm Protection” >> Click “Configure” >> expend Real-Time Protection >> Click “Internet Worm Protection” (again) >> Click “General Rules” to open the General Rules Window.

**Norton Internet Security 2008:** Open Norton >> select the Norton Internet Security tab >> expand “Settings” >> expand “Web Browsing” >> Click “Personal Firewall” >> Click “Configure” >> Click “Advanced Settings” under the Personal Firewall category >> Click “Configure” under the General Rules category to open the General Rules Window.

**Norton Internet Security 2007:** Open Norton >> select the Norton Internet Security tab >> expand “Settings” >> Click “Personal Firewall” >> Click “Configure” >> Click “Advanced Settings” under the Personal Firewall category >> Click “Configure” under the General Rules category to open the General Rules Window.

**Norton Internet Security 2005:** Open Norton Internet Security >> Click “Personal Firewall” >> Click “Configure” >> Select the “Advanced” tab >> Click “General” to open the General Rules Window. *Note: If you get an error associated with "szModify" in a script file, you may not be able to “Add” a rule. This is a known problem. You can either upgrade to a more recent version from Symantec or, apparently, you can go to www.microsoft.com/athome/support/default.mspx and enter “szModify” (without quotes) in
the search box for instructions on obtaining a $5, 3\textsuperscript{rd}-party fix for this issue. XXT had not used and cannot vouch for the latter solution.

⇒ Creating the Rule to Unblock Port 1723: Again, the exact user interface to create a rule from the General Rules dialogue varies, but the philosophy and most of the terminology appears to be similar. Hopefully, if a rule for port 1723 already exists, it will be appropriately designated in the list. If so, select it and click “Modify”. Otherwise…
  o Click Add…
  o Block or Allow Option: Select “Allow”. Click “Next” or the “Connections” tab…
  o Connections: Select “Connections from other computers” (it may be the only option). Click “Next” or the “Computers” tab…
  o Computers: Select “Only the computers and sites listed below”. Click “Add”. Follow the instructions to add computers individually by name (such as “www.homeoffice.com”, or by internet address. Click OK. Click “Add” again to add additional clients that may also access the well-site. When finished, click “Next” or the “Communications” tab…
  o Communications Options: Select the “TCP and UDP” protocol option. Then select “Only the communications or ports listed below” – or something to that effect (do not select the all computers option). Click “Add” and a “Specify Ports” window should appear. Select “Known ports from list”. Scroll down to “Port: 1723 (Name: pptp; Description: Point-to-Point tunneling protocol)”, check the box and click “OK”. Click “Next” or the “Tracking” tab…
  o Tracking: You may choose to log an event each time that a client connects through port 1723. Click “Next” or the “Description” tab…
  o Description: Give the Rule a name such as “Port 1723 (tunneling for VPN access)”. Click “Next” or, if available, the “Locations” tab…
  o Locations (optional): Check the locations for which this rule will apply (usually all 4 options).
  o Complete the process.

Point-to-Point Tunneling Protocol (“pptp”) Issues and Observations

Once a VPN connection has been established between the VPN client and the VPN server through Port 1723, each PC as part of the “pptp” protocol will occasionally issue an “echo request” to which the other PC is supposed to respond with an “echo reply”. These exchanges normally occur at 60 or 120-second intervals, but there appear to be other conditions that impact the “normal” timing. If the VPN client does not receive an “echo reply” packet, the VPN connection will, in XXT’s experience, disconnect in approximately 3 minutes (there are several documents on the internet describing this type of VPN, 3-minute disconnect behavior). XXT has not experienced this issue when using Windows firewall, but has experienced the problem with third-party firewalls and, as of this writing, continues to determine acceptable resolutions for this issue. If for whatever reason, you require a third-party firewall and experience this type of issue, XXT recommends that you confirm that the problem does not occur with Windows firewall enabled and the 3\textsuperscript{rd}-party firewall disabled and then contact the 3\textsuperscript{rd}-party firewall support group to resolve the problem. It should be noted that the pptp “echo-request” and “echo-reply” are not the same as the TCP/UDP “echo” (port 7), ICMP “echo” (port 0), or ICMP “echo reply” (port 8). It should also be noted that the various internet protocol layers, including the VPN connection, are in-fact transparent to xxNETserver/PC™ and other XXT applications.
Connecting to the Well Site from a Remote Location

In order to connect to the well site from a remote location, the user must be provided the following information:

⇒ The Well site IP Address
⇒ The VPN Server IP Address
⇒ The Hostname of the VPN server PC
⇒ A Username and Password for logging on to the VPN server PC which has been selected on the “User Permissions” page as having access through the VPN, as described in the section “Enabling the VPN Server on the PC” above.

For details on how to set up the remote PC to connect to the well site, see the related XXT tech note: “xxNETserver/PC™: Connecting to a Remote Well-Site Using a VPN” (PDF File: “XXT-TechNote-VPN-ConnectingToRemoteWellsite…”)

By convention, XXT documentation that is released with the xxDRT/PC™ Program Suite is stored in the c:\Program Files\XXT Incorporated\xxDRT-PCSuite\Documentation folder and may be accessed directly from most applications by clicking on the “Browse Documentation” option in the Help pull-down menu.