

# GoToMyPC™

Remote-Access Technologies:

A Comparison of  
**GoToMyPC™**  
and  
**VPNs**

**expertcity.com**

## ***Table of Contents***

### **1. Executive Summary**

- Traditional Solution: The VPN
- Revolutionary Solution: Expertcity's GoToMyPC

### **2. Comparison of the Two Technologies**

- Software Installation
- Configuration
- Termination of Encrypted Sessions
- Firewalls
- NAT/IP Address Overloading
- IP Reliance
- Performance
- Authentication
- Management of Remote Clients
- Security Issues
- Interoffice Use

### **3. Summary**

## **Executive Summary**

One of the major issues confronting Information Systems managers today is how to provide secure access to corporate IS resources to people who are physically located outside of the corporate network. In today's increasingly connected society, traveling salespeople, telecommuters and staff working after hours all need access to resources on corporate networks. These resources—such as databases, sales tools, email, etc.—are usually protected by firewalls for security reasons so that they cannot be accessed from outside the corporation.

### ***Traditional Solution: The VPN***

The traditional way to provide remote staff access to internal resources is to provision a virtual private network (VPN). A VPN encrypts all data traveling between specified endpoints, ensuring the privacy of all such data even while it travels across public networks, such as a dial-up ISP used by a traveling salesperson. Typically a VPN-secured connection terminating at the edge of a corporate network will be accorded the same access rights as a local LAN connection.

### ***Revolutionary Solution: Expertcity's GoToMyPC***

Expertcity's GoToMyPC is a Web-based screen-sharing software that allows users to access and work on any of their computers registered through the GoToMyPC Web site, <http://www.gotomypc.com>. With GoToMyPC, users can see the screen of the computer they are accessing and use all of the computer's programs, files and network resources as if they were sitting at and using the computer locally, even though they may be a thousand miles away.

All communications between the computers are encrypted using 128-bit encryption. Only screen and keyboard updates are sent between the host and the client computer used to access it (unless the user initiates a file transfer), so bandwidth demands are minimal. Any Internet-connected computer can be used to control the host computer without requiring special software to be installed. The host and client computers both initiate outward TCP connections on well-known ports, so no firewall changes are necessary.

## **Comparison of the Two Technologies**

### ***Software Installation***

**VPNs:** VPNs require special VPN client software to be installed on every remote computer that will be used to access the corporate network. This is not problematic for fixed-location telecommuters, but it requires travelers to bring a computer with them rather than being able to rely on computers that may be available at their destination. It also requires the IS department to manage the installation of VPN client software on a wide variety of computers that are not physically under its control.

**GoToMyPC:** GoToMyPC allows users to access and control their host computer from any other Internet-connected computer and does not require any special software to be installed ahead of

time. It does, however, require that a computer be available on the corporate LAN for the remote users to access. For occasional telecommuters working from home or traveling salespeople with laptops who also have a desktop computer at work, this is not an issue. For employees who do not have a desktop computer, it may still be more efficient and cost-effective to provide these employees with access to a computer within the corporate LAN than to implement a VPN as a way for them to access corporate resources remotely.

### **Configuration**

**VPNs:** VPN client software must be specifically configured for every destination and with the authentication mechanisms for each destination. This can impose an onerous overhead if new sites are to be added after clients are deployed.

**GoToMyPC:** GoToMyPC is effectively self-configuring. Remote users log in to the GoToMyPC Web site and are presented with a list of all computers to which they can securely connect and control. They need remember nothing except their account user name/password and the computer access code.

### **Termination of Encrypted Sessions**

**VPNs:** VPNs require specific hardware and/or software to terminate the encrypted sessions. This centralized encryption/decryption imposes heavy CPU loads on the device, and such devices tend to be somewhat expensive, increasing in price with the scale of the number of simultaneous sessions they can support.

**GoToMyPC:** GoToMyPC connections terminate on the machines being controlled, so the encryption/decryption load is spread among all such computers and is easily handled with little impact on the machines.

### **Firewalls**

**VPNs:** To allow VPNs to function, it is necessary to modify firewalls to allow the VPN connections through to the VPN termination device.

**GoToMyPC:** Using GoToMyPC, both the host and client computers receive all communications through an outgoing TCP connection that they initiated, and thus do not require any firewall changes.

### **NAT/IP Address Overloading**

**VPNs:** VPN technology typically does not interoperate with NAT/IP address overloading. This often is problematic in situations where home users utilize a NAT device on cable modem or DSL connections to share their Internet connection among multiple computers. It can also complicate the placement of the VPN termination device in the corporate network. (The VPN cannot transit the corporate NAT device - but placing it outside may lead to security risks.)

**GoToMyPC:** GoToMyPC is completely unaffected by NAT issues.

### ***IP Reliance***

**VPNs:** VPN technology is often IP centric. There are few VPN solutions that support protocols other than IP.

**GoToMyPC:** GoToMyPC allows use of all protocols that are supported by the host machine, as it is simply passing the display image and input to and from the host machine.

### ***Performance***

**VPNs:** VPN throughput is often well below what is necessary to provide good performance for corporate applications that have been designed to run on a fast LAN. Often the VPN connection will be a modem, and the VPN overhead reduces the available bandwidth in most cases.

**GoToMyPC:** Because the application is running on the remote computer that is on the LAN, users will experience the same performance as they do when they are physically on the corporate LAN. Because GoToMyPC is only passing the display and input to and from the remote machines, and has uniquely efficient compression algorithms built in, it is an extremely efficient user of bandwidth. Screen response is quite good even over a modem connection.

### ***Authentication***

**VPNs:** VPN solutions often authenticate the machine connecting, not the user. This provides little security in the event of an unauthorized person using an external VPN client (such as a stolen laptop).

**GoToMyPC:** GoToMyPC requires password authentication in order to access a user's GoToMyPC account on the GoToMyPC Web site. Once logged in, users can see the list of computers they can connect to. In order to control any of those computers, they must also enter the specific computer's access code. (Note: Computer access codes are never sent across the network, even in encrypted form.) Further, they will be subject to the security controls of the machine they are connecting to, just as if they were in front of it (e.g., needing NT domain or NDS user name/password to log in or to deactivate the screen saver, etc.).

### ***Management of Remote Clients***

**VPNs:** The most serious difficulty with VPN solutions is the management of the remote VPN client system. The remote system requires the same applications as local machines on the corporate LAN in order to provide the same functionality. However, the installation and maintenance of such applications is much more difficult because IS staff cannot usually visit the machine.

**GoToMyPC:** Because the machine that the remote user operates needs nothing more than a Web browser, remote management needs are eliminated. The remote user can take advantage of all applications that are present on the machine being controlled, and corporate IS can manage the machine being controlled in a systematic and familiar manner.

## **Security Issues**

**VPNs:** The most serious flaw with most VPN solutions from a security point of view is that they effectively take an external machine, which has not been protected in the same manner as machines on the internal LAN, and accord it the same privileges as internal LAN machines. The fact that a remote machine has a VPN client installed does not ensure that it has current virus protection or any firewall protection, or even that the machine has any of the default vulnerabilities disabled. Yet it will be allowed into the internal network and trusted to the same degree that managed internal machines are. It is likely that it was this type of VPN weakness that was exploited by hackers to break into Microsoft late last year<sup>1</sup>. There is little point in ensuring that firewalls and current virus scanners protect corporate machines if VPN clients are allowed in without determining if they have any protection at all.

**GoToMyPC:** GoToMyPC eliminates the security exposure of VPNs because changing the security of the corporate LAN is not necessary. It is irrelevant if the remote machine is infected with a virus because it is never made part of the corporate network. All the remote machine does is provide a secure channel to use the well-secured computers on the corporate LAN.

## **Interoffice Use**

**VPNs:** VPNs allow interoffice links to use the commodity Internet and still be protected by encryption.

**GoToMyPC:** GoToMyPC is not suited for protecting communications between offices; it provides a mechanism that allows a remote computer to securely control another, but not a tunnel between arbitrary numbers of endpoints.

## **Summary**

In contrast to a VPN, GoToMyPC can provide IS management with a way to provide secure remote access to corporate computing resources with no downside in terms of extra management, loss of security or loss of performance. Because of the need for special hardware, software and configuration, VPNs can be very time-consuming and expensive to implement and support. In contrast, GoToMyPC is a completely Web-based solution that can be implemented in minutes. VPNs are still the solution of choice for interconnecting different LANs over untrusted networks, but for remote users, GoToMyPC offers a much easier, and much more secure, solution.

<sup>1</sup> See "New account of Microsoft attack", MSNBC, <http://www.msnbc.com/news/482011.asp?cp1=1>

## Comparative Overview of GoToMyPC vs. VPNs

	<b>GoToMyPC™</b>	<b>VPNs</b>
<b>Software Installation</b>	No client software required.	Software must be installed on clients.
<b>Configuration</b>	Self-configuring.	Client software requires configuration.
<b>Termination of Encrypted Sessions</b>	End-to-end encryption. Load spread among all machines used.	Centralized encryption requires hardware and/or software and imposes heavy CPU loads.
<b>Firewalls</b>	No changes required.	Firewalls must be specially configured.
<b>NAT/IP Address Overloading</b>	Transparent to NAT issues.	Does not interoperate with NAT/IP address overloading.
<b>IP Reliance</b>	Allows use of all protocols on host computer.	IP-centric.
<b>Performance</b>	Applications run on the LAN, only screen image transmitted. Superior performance.	Corporate applications designed for a fast LAN are very slow over a VPN. Performance often poor.
<b>Authentication</b>	Authenticates the user at multiple points	May authenticate the machine connecting, not the user. Less secure.
<b>Management of Remote Clients</b>	Client computer only needs a Web-browser.	Is difficult and costly to install and maintain applications on the remote system.
<b>Security Issues</b>	Does not impact security of corporate LAN.	Gives external machine LAN rights, which creates potential security risks.
<b>Interoffice Use</b>	Not a network, but rather a secure tunnel to a particular computer.	Can be used to connect offices.