GoToMyPC®

GoToMyPC Technology Making Life Simpler for Remote and Mobile Workers

Learn why GoToMyPC is the most secure, cost-effective and easy-to-use solution for providing remote access to the desktop.

www.gotomypc.com

by CITRIX®

Today, secure remote access to your computers is no longer a luxury — it has become a necessity. Being able to tap into your home or office computer from hotels, Internet cafés and airport kiosks can greatly increase your efficiency, productivity and job satisfaction.

Yes, you can get it from here

GoToMyPC® is a hosted service that enables secure browser-based access to any Internet-connected Mac® or PC. Features include a screen-sharing Viewer, Drag-and-Drop File Transfer, Remote Printing, Guest Invite, use with multiple monitors, compatibility with many mobile devices and chat.

You can easily install and use GoToMyPC. Unlike other solutions, GoToMyPC does not require permanent client software or a network change. A resizable Viewer, launched from any browser with an Internet connection of 56 Kbps or better, enables interactive access to any desktop application (even those that are not Web based). The File Transfer feature sends and receives files, folders and directories, including those located on LAN-connected fileshares. Remote Printing allows printing to a client printer from the host computer Viewer. Third parties can even be granted temporary access to a GoToMyPC-enabled desktop with Guest Invite.

GoToMyPC's client Viewer and host are designed from the ground up for efficient, secure communication over any network. Keyboard, mouse and display updates are transmitted over a highly compressed, encrypted stream, generating an experience that's like being there. By providing fast, reliable, easy-to-use remote access to the user's native desktop, GoToMyPC can increase your productivity.

Under the covers, GoToMyPC is a hosted service, made up of four components (see Figure 1). A small footprint server is installed on the computer to be accessed – typically, a home or office computer with always-on Internet access.

Many other solutions require servers to receive incoming packets at a public IP address. The GoToMyPC host Mac or PC establishes a persistent TCP connection to the GoToMyPC broker (poll.gotomypc.com) that allows it to be notified if any connect requests have been received. The host will attempt to keep the connection open by sending TCP "keep alive" packets approximately every 60 seconds. This makes GoToMyPC completely compatible with application proxy firewalls, dynamic IP addresses and network/port address translation (NAT/PAT).

On the client side, the remote or mobile worker launches a browser, visits the secure GoToMyPC Web site, enters a user name/password and clicks on a "connect" button for the desired computer, sending an SSL-authenticated, encrypted request to the broker. During an active connection, the GoToMyPC Web site displays a session-in-use notification. Users can also review their own connection histories to confirm the absence of suspicious activity such as failed log-in attempts.

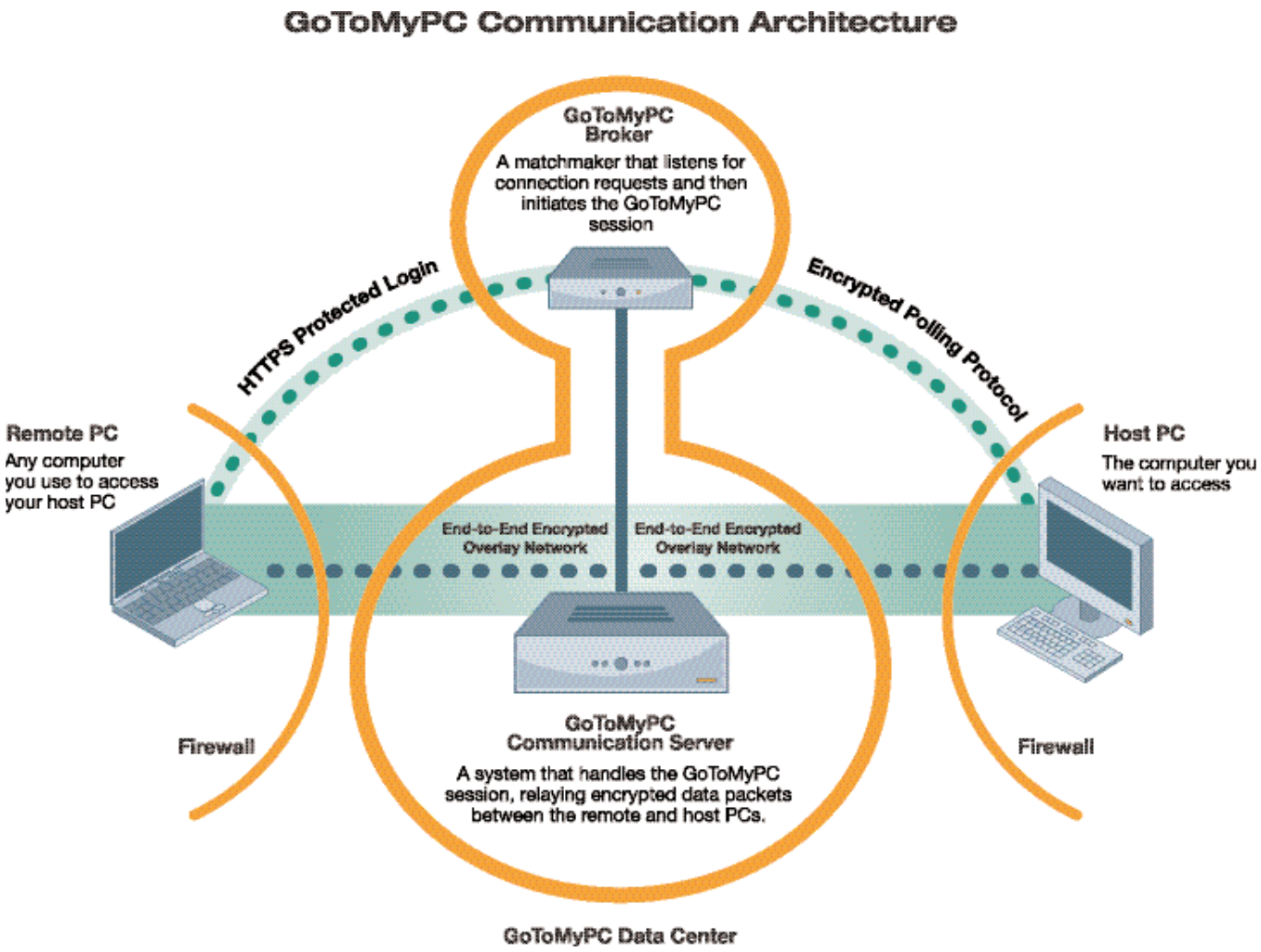

Figure 1: GoToMyPC Communication Architecture

The GoToMyPC broker is a matchmaker – it listens for connection requests and maps them to registered computers. When a match occurs, the broker assigns the session to a communication server. The client Viewer and host computer are supplied with the communication server address and a unique session ID. At this point, the client Viewer – a tiny session-specific executable – is automatically loaded by the browser's Java Virtual Machine. This Viewer gives remote workers access to their computers from any computer with a Java-enabled browser, including many wireless mobile devices.

The communication server relays an opaque, highly compressed, encrypted stream from client to host. The client and host mutually authenticate each other, using a shared secret (a computer access code) known only to them. For scalability, reliability and optimal performance, the broker automatically load balances sessions across a pool of geographically distributed communication servers.

Implementation with ease

GoToMyPC enables secure remote access quickly, seamlessly and almost effortlessly. GoToMyPC leverages an existing computer desktop by provid-

ing secure user-to-computer access. With screen sharing and sufficient bandwidth, users can have exactly the same desktop environment, whether working at the office, at home or on the road.

On the client side, even the most basic PC, Mac®, Unix workstation or Windows-based mobile device can be used as a remote monitor, keyboard and mouse. Because it requires just a browser, GoToMyPC can even run on public computers. On the host side, the user's existing Mac® or PC does all the heavy lifting – providing CPU, memory, disk and applications.

GoToMyPC is an end-to-end solution, designed to avoid any complications with your workplace network. Travelers working at a customer or business partner office, staying in a hotel with broadband Internet access or using a public computer often find these environments hostile to IPsec clients, but not GoToMyPC. Its protocol design is compatible with dynamic and static IP addresses, network and port address translation (NAT/PAT) and firewalls that block incoming sessions. GoToMyPC integrates with an organization's existing network and security infrastructure to lower total cost of implementation in a manner that allows the network owner to retain complete control over remote-access users and services.

Keep it secure

GoToMyPC can be used at your workplace. Some workers use products that get around LAN security by dialing directly into office computers. GoToMyPC eliminates this temptation by using the Internet. With GoToMyPC, there is no need to punch holes through corporate firewalls. All connections are initiated by the client and host and use outgoing TCP ports frequently left open: 80, 443 and/or 8200. GoToMyPC encapsulates all traffic – even encrypted packets carrying proprietary protocol – inside standard HTTP wrappers, ensuring compatibility with firewalls that inspect payload. IPsec – even SSL-based VPN services – usually require firewall adjustments. Instead, GoToMyPC adjusts itself to the firewall. However, enterprises that want firewall control over GoToMyPC can do so very easily, using a single IP-level filter to block traffic to Citrix Online's broker. Upon request, Citrix Online will also filter GoToMyPC connections made to a company's network address block, ensuring that only company-authorized computers can be accessed by company-authorized users.

GoToMyPC uses multiple, nested passwords to keep outsiders away. The broker authenticates itself with a digital certificate. Clients authenticate themselves by user name/password, exchanged over SSL, with a "three strikes" rule (account disabled for a user-designated number of minutes after a user-designated number of failed log-in attempts). When hosts register with the broker, each is assigned a unique random number. Hosts authenticate themselves by signing their number with MD5 and user name/password. Thereafter, the broker and hosts exchange MD5 challenge/response messages based on a sequence known only to the pair.

For added privacy, whenever a client connects to a host, they also authenticate each other, using a shared secret known only to the end user and the accessed computer. Each end point generates a large random number and digitally signs that number with the computer's access code. This exchange also forms the basis for generating 128-bit session keys used to encrypt data. For an additional level of security, One-Time Passwords can be used to thwart keystroke capture attacks by making secret-stealing pointless.

GoToMyPC provides data confidentiality with a highly compressed encrypted stream that ensures confidentiality without sacrificing performance. GoToMyPC implements 128-bit Advanced Encryption Standard (AES). AES was selected due to its computational efficiency, flexibility, simplicity and security; it is the U.S. government's designated cipher for protecting sensitive information.

Screen sharing and file-transfer packets include a sequence number to prevent message-replay attacks. These packets carry highly compressed binary data that are framed in a proprietary protocol and encrypted with AES. A hacker cannot modify these packets without corrupting them. Any third party attempting to inject or replay packets would have to know both the session key and the current state of the AES engine. Lack of clear text makes it exceedingly difficult to "guess" the encryption key through traffic analysis. And of course, each key is good for just one session.

One of the advantages of providing remote access through screen sharing is the ability to leverage the access controls already in place on the corporate LAN. For example, when GoToMyPC connects, the remote user must enter a Windows login and password to access the computer and be granted file, host and domain-level permissions associated with his or her account. In other words, the remote user does not have tunneled access to the enterprise network – he or she only has access to a single computer's desktop, and is subject to access controls already in place for that desktop. Host screen blanking and host keyboard/mouse input blocking increase the physical security of the computer being accessed.

It's also important that remote-access sessions be terminated after inactivity. Remote users walk away from public computers without logging out and leave home computers unattended. GoToMyPC uses inactivity time-outs to help mitigate these threats. Users are automatically logged out of the GoToMyPC.com Web site when their SSL session remains inactive for 15 minutes. In addition, users can configure the Viewer to time out after a period of inactivity. Although most security features are pre-configured, users can activate additional features such as local computer keyboard/screen lockout during remote access.

Conclusion

GoToMyPC is a very attractive solution for individual desktop remote access that is secure, fast, easy to use and reliable.

Excerpted from a white paper by:

Lisa Phifer
Core Competence, Inc.
lisa@corecom.com

About Lisa Phifer: Lisa A. Phifer, vice president and co-owner of Core Competence, has been involved in the design, implementation and evaluation of data communications, internetworking, security and network-management products for over 20 years. At Core Competence, she has advised companies large and small regarding security needs, product assessment and the use of emerging technologies and best practices.

Citrix Online Division
6500 Hollister Avenue
Goleta, CA 93117
U.S.A.
T 1 805 690 6400
info@citrixonline.com

Media inquiries:
pr@citrixonline.com
T +1 805 690 2969

Citrix Online Europe
Middle East & Africa
Citrix Online UK Ltd
Chalfont Park House
Chalfont Park, Gerrards Cross
Bucks SL9 0DZ
United Kingdom
T +44 (0) 800 011 2120
europe@citrixonline.com

Citrix Online Asia Pacific
Suite 3201
32nd Floor
One International Finance Center
1 Harbour View Street
Central, Hong Kong SAR
T +852 100 5000
asiapac@citrixonline.com

About Citrix Online
Citrix Online solutions enable people to work from anywhere. Our products include GoToAssist® for remote support, GoToManage™ for IT management, GoToMeeting® for online meetings, GoToMyPC® for remote access, GoToTraining™ for interactive online training and GoToWebinar® for larger Web events.

03.15.10/B-16031/PDF