access INFRASTRUCTURE FOR THE ON-DEMAND ENTERPRISE

GoToMyPC® CORPORATE

WHITE PAPER

Citrix GoToMyPC Corporate Technology

MAKING LIFE SIMPLER FOR REMOTE AND MOBILE WORKERS

Learn why Citrix® GoToMyPC® Corporate is the most secure, cost-effective and easiest-to-manage solution for providing remote access to the desktop.

CITRIX® online

Today, providing remote and mobile workers with secure remote access to corporate networks is no longer a luxury — it has become a business necessity. Letting employees tap into the office local area network (LAN) from customer sites, hotels, Internet cafés and airport kiosks can greatly increase business efficiency, productivity and job satisfaction. But mobile empowerment has a price, measured in IT administration and network security. GoToMyPC, a remote-access service from Citrix Online, intends to change that.

Yes, You Can Get There from Here

GoToMyPC is a hosted service that enables secure browser-based access to any Internet-connected Microsoft Windows-based PC. Features include a screen-sharing Viewer, drag-and-drop File Transfer, Remote Printing, Guest Invite and Chat. Corporate administrators have access to extensive management and reporting tools that enable central control over these remote-access services.

Unlike other solutions, GoToMyPC does not require permanent client software or a network change. This approach significantly reduces IT support requirements, resulting in lower total cost of implementation (TCI). 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. Chat supports text communication between client and host users, which is useful during help desk access to remote PCs. 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. Access to each of these services may be permitted or denied by corporate administrators, in accordance with user needs and company security policy.

GoToMyPC's client Viewer and desktop server (host) are robust Win32 applications, 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, yielding "good as there" experience over broadband and impressive performance over dial-up. By providing fast, reliable, easy-to-use remote access to the user's native desktop, GoToMyPC can increase the productivity of mobile workers.

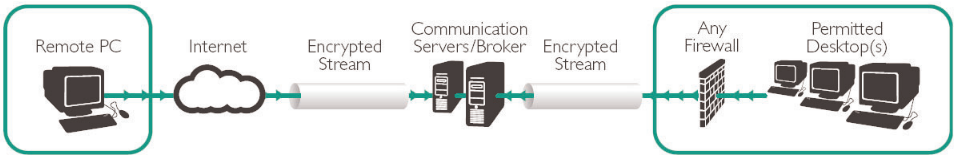

FIGURE 1 | GOTOMYPC ARCHITECTURE

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 PC with always-on Internet access. This host computer registers and authenticates itself with Citrix Online's GoToMyPC broker. For network address and firewall independence, the host initiates all communication with the broker, issuing HTTP "pings" to check for new connect requests.

On the client side, the remote or mobile worker launches a browser; visits the secure GoToMyPC Web site; enters a username/password; and clicks on a "connect" button for the desired computer, sending an SSL-authenticated, encrypted request to the broker. Of course, for security reasons, only computers configured by this user are displayed. 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.

The GoToMyPC broker is a matchmaker – it listens for connection requests, mapping 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 PCs 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 added security, corporate administrators can also require the use of One-Time Passwords or RSA SecurID two-factor authentication. For scalability, reliability and optimal performance, the broker automatically load-balances sessions across a pool of geographically distributed communication servers.

Reduce Administrative Costs

GoToMyPC enables secure remote access quickly, seamlessly and almost effortlessly. Other virtual private network (VPN) solutions try to duplicate a worker's office desktop on a home PC or laptop by tethering remote hosts to the corporate LAN over IPsec or SSL tunnels. GoToMyPC leverages a worker's existing office desktop by providing secure user-to-PC access. With screen sharing and sufficient bandwidth, employees 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 PCs. On the host side, the worker's existing PC does all the heavy lifting – providing CPU, memory, disk, enterprise applications and native access to the corporate LAN. Screen sharing eliminates the need to install enterprise application and VPN client software on remote PCs, significantly reducing client administration complexity and cost.

With a hosted service like GoToMyPC, there's no need to operate a private remote-access server (RAS) pool or install a VPN access concentrator. Like traditional VPNs, GoToMyPC can leverage the public Internet to slash recurring telecommunications costs associated with remote access. However, many IPsec or SSL VPNs – including those outsourced to managed security providers – require a gateway device to be installed at the edge of the enterprise network. Installing a VPN gateway can be tricky, requiring changes to existing enterprise network addresses, routes and firewall rules.

GoToMyPC is an end-to-end solution, designed to completely avoid enterprise network impact. Other VPN solutions fail to recognize that network-independence is important to both clients and servers. Travelers working at a customer or business partner office, staying in a hotel with broadband Internet access or using a public PC 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 TCI in a manner that allows the network owner to retain complete control over remote-access users and services.

Keep It Secure

Some workers use products like Symantec pcAnywhere™ to get around LAN security by dialing directly into office PCs. 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 username/password, exchanged over SSL, with a "three-strikes" rule (account disabled for N minutes after M failed log-in attempts, where N and M are configurable).When hosts register with the broker, each is assigned a unique random number. Hosts authenticate themselves by signing their number with MD5 and username/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 and which is never seen or stored by Citrix Online. 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® Corporate also supports two-factor authentication through integration with a company's existing RSA SecurID infrastructure. Administrators can enforce use of One-Time Passwords and SecurID throughout an organization by setting user and group options.

GoToMyPC Corporate also gives administrators a way to maintain control over the endpoints of the remote connection by pre-authorizing uniquely fingerprinted client and host devices. By requiring explicit approval during host computer setup, administrators are able to restrict the host computers within an organization and the specific client Viewer computers outside the corporate network that can be used to access them. In addition, an administrator can prevent non-permitted GoToMyPC access by limiting host computers within a network to a specific GoToMyPC Corporate account.

GoToMyPC provides data confidentiality with a highly compressed encrypted stream that ensures confidentiality without sacrificing performance. GoToMyPC implements 128-bit Advanced Encryption Standard (AES) in Cipher Feedback Mode (CFB). 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.

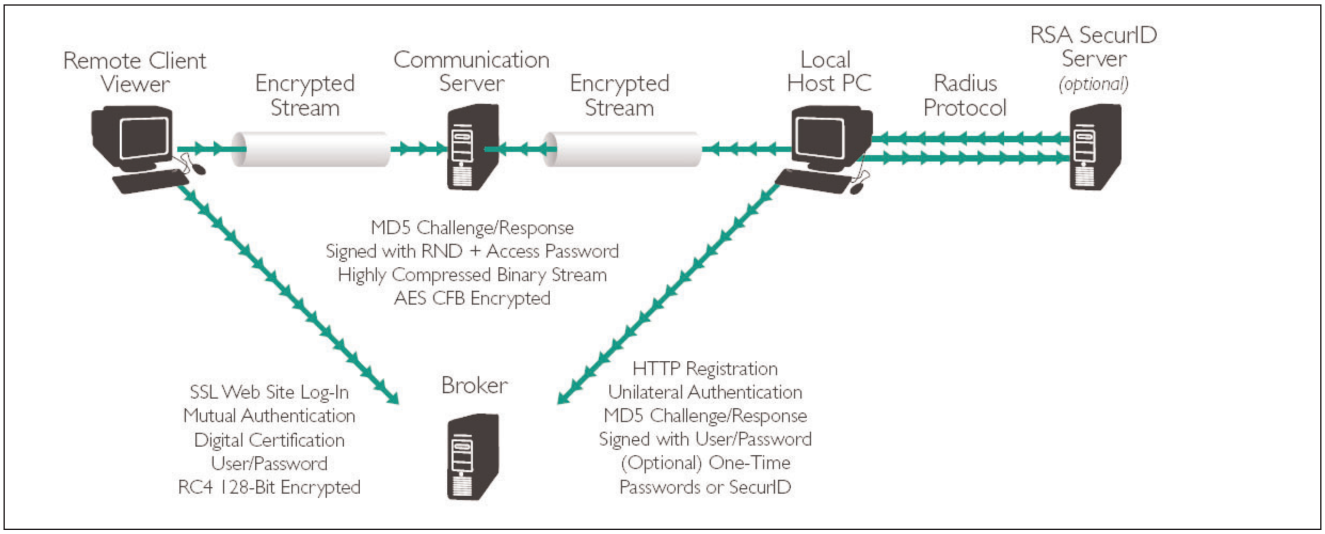

FIGURE 2 | GOTOMYPC USES AUTHENTICATED, ENCRYPTED CHANNEL

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. Because it is possible to modify encrypted text without corrupting it, chat packets also carry a signed MD5 hash to ensure message integrity.

Any third party (man in the middle) 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/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 PCs without logging out and leave home PCs 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 fifteen minutes. In addition, users can configure the Viewer to time-out after a period of inactivity, subject to limits set by the administrator.

Although most security features are pre-configured, users can activate additional features such as local computer keyboard/screen lockout during remote access. Administrators can disable remote-access services for users and groups to meet corporate security needs. For example, healthcare organizations might disable file transfer, clipboard sharing and remote printing capabilities to adhere to federal privacy regulations.

With GoToMyPC Corporate, administrators can match corporate security policies by making certain security features such as screen blanking mandatory. In addition, administrators can define days of the week and time periods when users are allowed to remotely access their computers, set the maximum number of computers per user, define password expiration policies and customize failed authentication lockout rules.

As a testament to the security of GoToMyPC, Citrix Online has achieved SiteSecure Certification from TruSecure Corporation, an industry-recognized security assurance program that certifies all aspects of information security, ranging from network and system analysis and assessment to physical and policy evaluation. The certification tests are performed regularly to ensure that Citrix Online continues to meet certification requirements.

Control Enterprise Access

While GoToMyPC® Personal is an easy-to-use, turnkey remote-access solution for individuals, GoToMyPC Corporate makes this same user-friendly remote-access solution available to corporate users. Through enterprise-class administration features, GoToMyPC Corporate gives IT administrators complete control over secure remote access for multilevel groups and users.

Corporate administrators use the browser-based, SSL-secured online Administration Center to create, delete, suspend and modify groups and user accounts. A top-level administrator can grant access to a second tier of plan administrators to facilitate large GoToMyPC Corporate deployments. Whenever an administrator modifies a user account, customizable mail messages are automatically generated. For example, when a new user is added (identified by email address), an invitation is sent containing a one-time-use self-activation URL. The user visits the URL, defines an individual password and then adds computers to his or her own account. Alternatively, GoToMyPC Corporate administrators can perform a remote installation or upgrade of the host-side software; however, end users must perform authentication steps to activate the account. This approach streamlines large scale deployment, while retaining enterprise control over remote-access authorization and ensuring individual user account privacy and accountability.

Users add computers by visiting the GoToMyPC Web site from the host computer. The default installation method requires just one click – a signed Java applet does the rest. Those who prefer to block Java or end users from installing software can install from a file instead. There is virtually nothing to configure – just enter a username, account password and an access code (known only to the owner of the computer). Before or after a user account is created, the administrator can configure security parameters and identify the services available to this user. By configuring group-level options, large-scale changes can be made quickly, and users can easily be moved from one group to another to reflect organizational changes.

GoToMyPC Corporate also provides real-time usage monitoring and historical reports. Administrators can view active and completed connections and can end an active session immediately if necessary. Detailed reports provide data about users, computers, sessions, total time, average duration over specified intervals, features enabled for each user, hours of access, logins and the frequency of failed log-in attempts. Through GoToMyPC Corporate, administrators can optionally integrate session information into an existing reporting infrastructure by recording data into the Windows Event Log. Further connection detail, logged by Citrix Online, can be used for problem diagnosis. This kind of central visibility is essential for enterprise deployment.

The goal: Keep GoToMyPC easy to use and simple to manage, but provide the ability to implement enterprise-defined security policies at global, group and user levels.

Conclusion

GoToMyPC is a very attractive solution for individual desktop remote access by trusted "corporate insiders." This service is well suited for extended use by broadband-enabled remote workers and visiting workers with LAN access. Mobile workers limited to Internet dial-up can also use GoToMyPC for effective short-term access to PCs on the corporate network.

GoToMyPC over broadband is nearly the same as being back at the office. GoToMyPC over v.90 is fine for checking mail, browsing documents or sending and receiving files. Depending upon Internet bandwidth, the application and duration of use, many road warriors will find GoToMyPC a truly effective remote-access solution. Travelers working at a customer or business partner office, staying in a hotel with broadband Internet access or using a public hotspot at a conference, Internet café or business center will find remote access with GoToMyPC convenient and familiar.

But convenience need not sacrifice security and control. Enterprises jaded by pcAnywhere-style "back doors" and frustrated by complex VPN deployments may find GoToMyPC more secure, more cost effective, easier to administer and easier to use. GoToMyPC Corporate combines user-friendly desktop sharing with robust authentication, encryption and administrative tools – features that can help an organization implement strong security policies and comply with mandates like HIPAA. In short, GoToMyPC adheres to security measures that are absolutely essential in any enterprise remote-access solution.

For more information on GoToMyPC Corporate, please visit corp.gotomypc.com

CITRIX® | online

About Citrix Online: Citrix Online, a division of Citrix Systems, Inc. (Nasdaq: CTXS), offers the leading Web-based access, support and collaboration software and services. The division offers Citrix GoToMyPC®, the easiest-to-use solution for remote, secure and managed desktop PC access over the Web; Citrix GoToAssist™, the industry-leading remote-support solution; and Citrix GoToMeeting™, the easiest, most secure and cost-effective solution for conducting online meetings. Citrix Online products are used by more than 4,900 companies worldwide, including Verizon Online, Siemens, Cablevision and Microsoft Business Solutions. The division is based in Santa Barbara, California, and is on the Web at www.gotomypc.com, www.gotoassist.com, www.gotomeeting.com and www.citrix.com.

Citrix Online

A Division of Citrix Systems, Inc.
5385 Hollister Avenue
Santa Barbara, CA 93111 USA

Product Information:
corp.gotomypc.com
www.gotomypc.com/security

Sales Inquiries:
gotosales@citrixonline.com
Phone: (888) 646-0016

Channel Partners:
resellers@citrixonline.com
Phone: (805) 690-5711

Media Inquiries:
pr@citrixonline.com
Phone: (805) 690-2961

www.citrixonline.com