



#209 | 05
May 2009

Commissioned by Citrix Online, LLC

Evaluating Secure Remote Desktop Access Models: Citrix GoToMyPC Corporate Software as a Service (SaaS) versus using Traditional Virtual Private Networks (VPNs)

EXECUTIVE SUMMARY

Citrix Online's GoToMyPC Corporate delivers easy-to-use, scalable and secure remote desktop access to users, compared to the traditional approach of using VPNs. GoToMyPC Corporate, offered as a Software as a Service (SaaS), delivers better return on investment (ROI) compared to a traditional VPN-based implementation.

With today's increasingly mobile workforce - workers on business trips, sales people in the field, telecommuting employees, IT administrators managing servers from off-site locations, etc. - there is an increasing need to provide access to corporate IT assets while the user is physically outside the corporate network. Doing so in a secure, scalable and economical way poses several challenges for the corporate IT departments.

Traditional approach of using Virtual Private Networks (VPNs) in conjunction with a Remote Desktop Protocol (RDP) application to allow remote users to connect to their desktop computer on the corporate network can often limit flexibility of deployment and the ability to scale gracefully and economically with the number of users, locations, etc.

Remote desktop access implemented using a hosted SaaS like Citrix GoToMyPC Corporate can fill the role of a VPN for some organizations or act as a complement to an existing VPN within an organization.

THE BOTTOM LINE

Citrix GoToMyPC Corporate:

- 1 Offers easy-to-deploy and easy-to-manage remote desktop access on host computers
- 2 Provides ease of access, using any modern Web-browser, from anywhere over the Internet
- 3 Uses a highly scalable and secure architecture, capable of serving thousands of users concurrently
- 4 Lowers the Total Cost of Ownership (TCO) and delivers increased Return on Investment (ROI) compared to a traditional VPN
- 5 Provides 24x7 support to end-users as part of the subscription to the service



SUMMARY OF FINDINGS

Ease of Deployment

Citrix GoToMyPC Corporate is quick and easy to implement, as there is no on-location hardware to install in order to deliver the service. In most cases, GoToMyPC Corporate can be deployed on host computers without major changes to existing network infrastructure or configuration. Furthermore, there is no need for

special client software to access the remote computers, as the user only needs to know how to use a Web browser in order to use the GoToMyPC Corporate service. Any device equipped with a modern Web browser can be used to view the remote desktop.

In contrast, deploying a VPN-based remote desktop access solution requires installation and configuration of VPN hardware and/or software that is highly customized to each specific installation. In some cases, additional remote desktop protocol (RDP) viewer applications need to be supported on

Citrix Online, LLC

GoToMyPC Corporate

Remote Desktop Access



Tested February 2009

Feature Comparison: Citrix GoToMyPC Corporate versus Remote Access over VPN

Category	Citrix GoToMyPC Corporate	Virtual Private Networks (VPNs) plus Remote Desktop Protocol (RDP)
Software Installation	No additional client software required beyond a modern Web browser.	Software may need to be installed on clients.
Configuration	Self-configuring.	Clients require configuration.
Termination of Encrypted Sessions	End-to-end 128-bit encryption. Load shared among all computers used.	Centralized encryption and decryption on VPN hardware imposes heavy CPU load.
Firewalls	Typically, no changes required.	Firewalls must be separately configured.
Network Address Translation (NAT)/ IP Address Overloading	Transparent to NAT issues.	Does not interoperate with NAT/ IP overloading.
Performance	Applications run locally on the target host computer. Only screen image is transmitted, yielding superior performance.	Performance may vary depending on the load on the corporate firewall/VPN appliance.
Authentication	Authenticates users at multiple points. One-time password generation available.	May authenticate to the network and have access to services not available when logged in locally.
Management of Remote Clients	Typically, no software installation needed on the client - just a Web browser required - so TCO is reduced.	Difficult to install and maintain applications on the remote system.
Inter-office Use	Not a network - but rather a secure tunnel to a particular computer.	VPN tunnels can be used to connect offices.

Source: Tolly, March 2009

Figure 1

the client and host computers, often requiring further modifications to existing network configuration.

Ease of Use

Citrix GoToMyPC Corporate is very easy and intuitive to use without requiring any specialized technical training. In most cases, the user only needs to know how to use a Web browser in

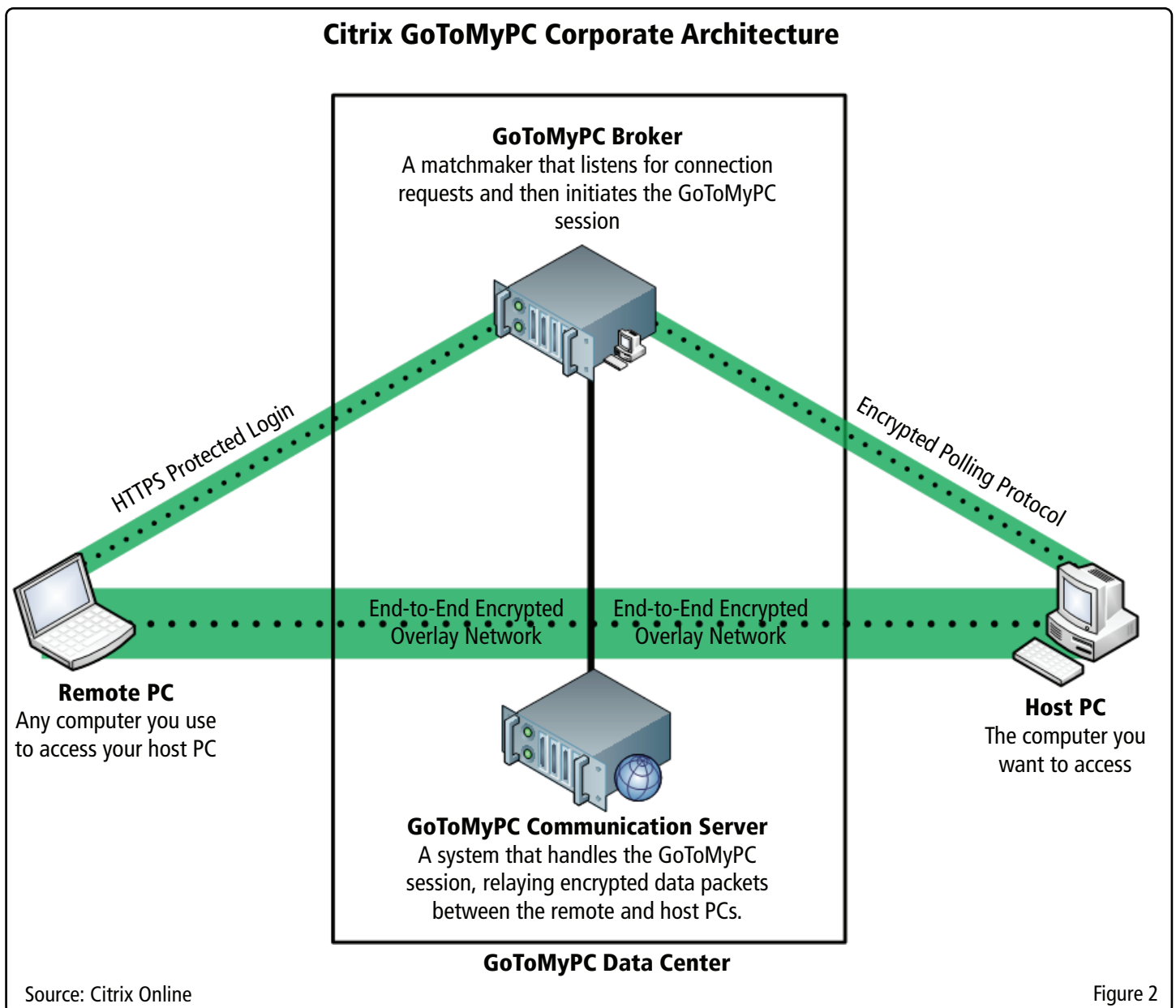
order use the GoToMyPC Corporate Web site (<https://www.gotmypc.com>) to connect securely to the remote PC.

In contrast, a VPN-based remote desktop access solution often requires proprietary client software to connect to the VPN appliance on the remote office network. Once connected to the remote network, a remote desktop

viewer application is required to access the desktop on the target host computer.

Ease of Administration

GoToMyPC Corporate provides a unified Web-based administration panel to manage the service. Client and host PCs for the remote users can be provisioned, audited and managed



Source: Citrix Online

Figure 2

from one central management interface.

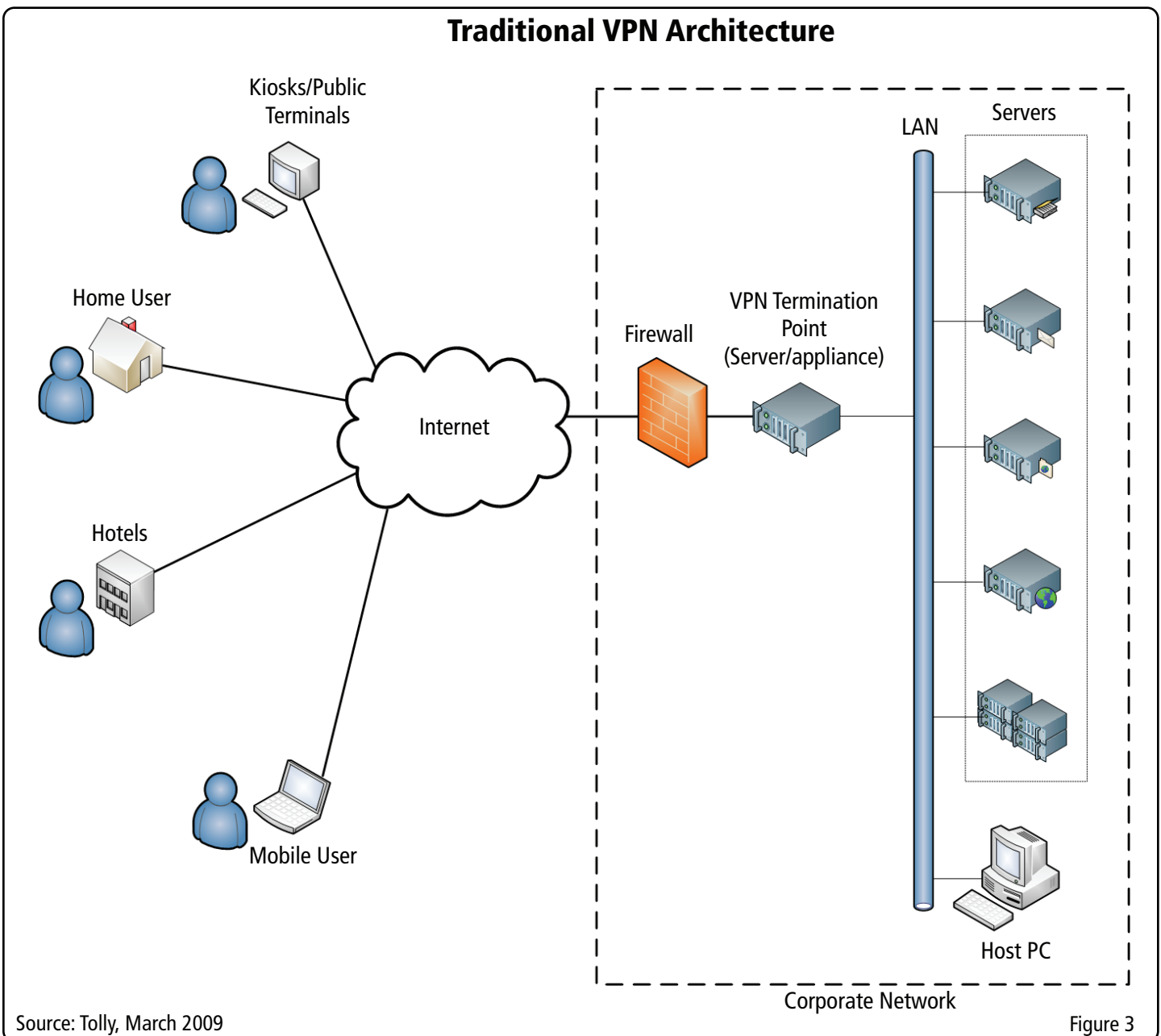
In contrast, a VPN-based remote access scenario most often requires the IT administrator to obtain unstructured data from disparate systems - firewall, VPN, router and server logs, etc. - to correlate the information in order to

obtain the same level of visibility and manageability as that provided by the GoToMyPC Corporate administration interface.

Flexibility of Access

Using GoToMyPC Corporate, the users are free to use any device equipped with a modern Web browser, from any

location - home office, hotels, airport kiosks, Wi-Fi hot spots at coffee shops, etc. - to access the host computer on the remote office network. When the user needs to access different host computers at multiple remote locations, it is as simple as selecting the desired host computer to connect to, by logging into the GoToMyPC Web





site. There is no need to change the host computer configuration.

Using VPN-based remote desktop access, the user is often limited to only use IT department-approved devices to access the corporate network over VPN. Furthermore, to access different networks, say at different remote office locations, the user's computer/device needs to be configured specifically to access each destination network.

GoToMyPC Corporate is currently supported only on host computers running the Microsoft Windows operating systems (Windows 2000 or newer), while VPN-based remote access solutions can be supported on a wider range of host operating systems.

GoToMyPC Corporate sessions provide user access to all protocols supported on the host computer, since only the screen image and input device data is transmitted to the client. In contrast, unless some kind of remote desktop protocol application is used to connect to the target host computer, most VPN-based remote access solutions are optimized for IP-based protocols.

Security

GoToMyPC Corporate is a very secure service, with multiple-level end-to-end authentication mechanisms, optional one-time password mechanisms, multiple-level end-to-end 128-bit AES encryption over Secure Sockets Layer (SSL), digital certificates, etc. The security posture of the client computer does not impact the security of the remote network, as the client computer is not physically connected to the corporate network.

VPN-based remote access solutions make the client computer a part of the remote corporate network. The client computer may then be granted the access rights of the user, which can compromise network security if the client computer's security is compromised. To protect against this risk, additional safeguards need to be put in place to assess the security posture of the client computer before granting it access to the corporate network. This adds complexity and cost to maintain the remote access service.

Scalability

As the number of users connected remotely to the corporate network increases, the requirements for the infrastructure to support the associated authentication and encryption mechanisms can increase dramatically.

GoToMyPC Corporate is highly scalable by virtue of being a SaaS solution, with infrastructure components hosted in Citrix Online's data centers. The encryption overhead on the infrastructure equipment is shared among all the client computers and the GoToMyPC Corporate service infrastructure.

In contrast, for VPN-based remote access the encryption and connection processing overhead is concentrated on the VPN terminating equipment on the corporate network. As the number of remote users to be supported increases, the hardware requirements and the software licensing costs of the VPN infrastructure can increase dramatically.

In general, GoToMyPC Corporate service will prove to be less expensive to serve a given number of users

compared to dedicated, VPN-based remote access solutions.

Performance

GoToMyPC Corporate provides near-real-time access to the host computer by minimizing the amount of data sent across the Internet to the client computer. Only the keyboard and mouse inputs and the portion of the screen image that change are transmitted in a highly optimized form, so that the client computer has a very fluid user experience. On most Internet connections the performance can satisfactorily mimic the experience of physically accessing the host computer.

The performance of VPN-based remote access may vary depending on the load on the corporate network, since VPN sessions need to be terminated on the firewall/VPN appliance before the remote access traffic can be delivered off to the target host computer.

Total Cost of Ownership

Citrix GoToMyPC Corporate delivers a scalable, secure, easy-to-deploy, easy-to-use and easy-to-manage service that can dramatically reduce the total cost of ownership (TCO) of the remote access solution.

In contrast, using VPN-based remote access solutions add additional complexity and cost due to the need to maintain dedicated VPN hardware and software at each corporate location that remote users might need to access.

Each client computer approved for remote access needs to be provisioned with a VPN client and an optional client security health check software that



Total Cost of Ownership (TCO) - Citrix GoToMyPC Corporate versus VPN-based remote access
(Lower numbers are better)

Cost Item		Citrix GoToMyPC Corporate Software as a Service (SaaS)			VPN-based Remote Access		
					Cisco ASA 5510		Cisco ASA 5520
		50 users	100 users	500 users	50 users	100 users	500 users
Cost of VPN hardware ^a	--	--	--	--	\$2,600	\$2,600	\$5,150
Cost of redundant VPN hardware (2 units)	1st year	--	--	--	\$5,200	\$5,200	\$10,300
	2nd year	--	--	--	--	--	--
	3rd year	--	--	--	--	--	--
Subscription cost ^a	1st year	\$6,450	\$12,300	\$59,520	--	--	--
	2nd year	\$6,450	\$12,300	\$59,520	--	--	--
	3rd year	\$6,450	\$12,300	\$59,520	--	--	--
SSL license cost for end user sessions (optional)	Per year	Included	Included	Included	\$2,600	\$5,100	\$19,000
SSL license cost on redundant hardware for end user sessions (optional)	1st year	Included	Included	Included	\$5,200	\$10,200	\$38,000
	2nd year	Included	Included	Included	--	--	--
	3rd year	Included	Included	Included	--	--	--
Installation and deployment cost (estimated @ \$100 per hour cost of IT resources)	1st year	\$500	\$1,000	\$1,500	\$2,400	\$2,400	\$3,200
	2nd year	--	--	--	--	--	--
	3rd year	--	--	--	--	--	--
Power consumption at steady state (taken from VPN hardware vendor data sheet)	--	--	--	--	150 W	150 W	150 W
Annual energy expenditure on VPN hardware (using average retail price of @ \$0.103 per kWh for industrial sector power in California in November 2008)	1st year	--	--	--	\$352	\$352	\$352
	2nd year	--	--	--	\$352	\$352	\$352
	3rd year	--	--	--	\$352	\$352	\$352
Estimated maintenance (hours/week) (M)	--	1	2	4	5	9	14
Cost of maintenance per hour (C)	--	\$100	\$100	\$100	\$100	\$100	\$100
Estimated maintenance costs per year (M*C*52)	1st year	\$5,200	\$10,400	\$20,800	\$26,000	\$46,800	\$72,800
	2nd year	\$5,200	\$10,400	\$20,800	\$26,000	\$46,800	\$72,800
	3rd year	\$5,200	\$10,400	\$20,800	\$26,000	\$46,800	\$72,800
24x7 Support for end users (@ \$260 ^b per user per year)	1st year	Included	Included	Included	\$13,000	\$26,000	\$130,000
	2nd year	Included	Included	Included	\$13,000	\$26,000	\$130,000
	3rd year	Included	Included	Included	\$13,000	\$26,000	\$130,000
Cost of support contract for VPN hardware	1st year	--	--	--	\$735	\$735	\$1,250
	2nd year	--	--	--	\$735	\$735	\$1,250
	3rd year	--	--	--	\$735	\$735	\$1,250
Total cost of ownership (TCO) over 3 years		\$35,450	\$69,100	\$242,460	\$127,861 ^c to \$133,061 ^d	\$229,261 ^c to \$239,461 ^d	\$626,706 ^c to \$664,706 ^d

Note:

- ^a - Cisco prices based on retail price quoted by reputed online retailer CDW.com in March 2009. GoToMyPC Corporate subscription costs based on retail price quoted by Citrix Online.
- ^b - Cost of 24x7 Level 2 and Level 3 Technical Support, according to a forthcoming model from a leading analyst firm.
- ^c - TCO without SSL VPN license.
- ^d - TCO with SSL VPN.

Annual Energy expenditure calculation for the redundant appliance configuration used the formula:
(2 appliances)*(150W/1000 kW)*(\$0.103 per kWh)*(24 hrs/day)*(365 days/year)*1.3
 The factor **1.3** is included to account for the assumption that cooling costs add a 30% overhead to the cost to power the appliances.

Source: Tolly, March 2009

Figure 4



could dramatically increase the total cost of ownership.

Furthermore, as the number of corporate locations that need to be provisioned for remote access increases, the Total Cost of Ownership of a VPN-based remote access solution can increase dramatically due to the need to maintain VPN termination equipment at each individual location. Citrix GoToMyPC Corporate can turn out to be much less expensive, in this scenario, by virtue of being a hosted SaaS solution that does not require dedicated VPN hardware at each location.

ENGINEERING ANALYSIS

GoToMyPC Corporate Architecture

The GoToMyPC Corporate service is delivered as a hosted SaaS solution by Citrix Online. The architecture of the solution consists of the following components, as explained by Citrix architects and as illustrated in Figure 2.

Host Computer: GoToMyPC Corporate installs a small footprint server on the host computer to communicate with the GoToMyPC Corporate service.

Browser: A modern Web-browser on the client computer that logs into the GoToMyPC Corporate Web site at (<https://www.gotomypc.com>) to connect to the host computers.

Broker: The broker listens to the connect requests from Web browser on client computers, and matches the

request to the correct destination host computer.

Communication Server: The communication server acts as the trusted middle man in the communications by relaying an opaque, highly optimized, encrypted stream of traffic between the client browser and the host computer.

The small footprint server located on the host computer maintains a persistent TCP connection to the GoToMyPC broker sending TCP “keep alive” packets at regular intervals. This enables the GoToMyPC Corporate service to work across most firewalls that allow outbound connections, even in the presence of Network Address Translation (NAT).

The client browser logs into the GoToMyPC Corporate Web site using an assigned user name and password, and a Web browser. Upon successful authentication, the user can select the desired host computer to connect to, from a list of computers accessible with that user account.

Upon selecting the desired computer to “Connect to,” an authenticated, SSL-encrypted connection request is sent to the broker.

The broker listens to the connection requests from clients and maps the requests to available host computers. Once a match is made, the broker hands off the session to the GoToMyPC Communication Server. To ensure optimal performance and session reliability, the broker automatically load balances the user sessions and assigns sessions to various geographically distributed Communication Servers.

The client and server computers are supplied the address of the Communication Server and a unique session ID. At this point, the ActiveX component or the Java Virtual Machine in the client Web browser launches a session-specific viewer that gives client users access to the desktop of the host computer. The client browser and the host computer authenticate each other with a shared secret known only to them.

The Communication Server relays the communications between the host computer and the client browser.

VPN-based Remote Access Architecture

Traditional VPNs rely on a hardware VPN terminating gateway appliance - either a dedicated appliance or embedded into a firewall, etc. - at the edge of the corporate network, and client software running on the user’s Internet-connected device.

The VPN client initiates a secure, authenticated and encrypted connection to the VPN appliance. The VPN appliances are typically integrated into the firewall appliances or implemented as a dedicated appliance by itself. In either case, VPN-based remote desktop access may require further configuration of the network infrastructure to allow the Remote Desktop Protocol (RDP) traffic to reach the host computer on the corporate network.

Once the credentials of the client have been authenticated by the VPN appliance, the client device is given access to the corporate network with rights appropriate for the user identity.



At this stage, in a traditional VPN, the remote client device is accorded the same level of network access as that of a computer physically connected inside the corporate LAN - irrespective of the security posture of the client device.

Some sort of network access control methodology should be employed to validate the security posture and quarantine devices that do not meet the corporate security requirements.

Total Cost of Ownership Analysis

Tolly engineers estimated the Total Cost of Ownership (TCO) of the Citrix GoToMyPC Corporate SaaS solution versus the traditional approach of using a VPN to deliver remote desktop access.

Several assumptions and estimations have been made - especially regarding the cost of IT workers' time spent on installation, maintenance, user training and support for both remote access solutions. The assumptions were based upon an in-depth, hands-on evaluation of the Citrix GoToMyPC Corporate service deployed in Tolly's corporate production network. Estimates regarding traditional VPN-based remote access solution were based on Tolly engineers' prior experience on the complexity of configuring and managing a VPN-based remote desktop solution.

Engineers used representative VPN hardware and software from Cisco Systems, Inc., and prices were obtained from respected enterprise class reseller, CDW.com. Prices for Citrix GoToMyPC Corporate service were obtained directly from Citrix Online, LLC.

Cost of Hardware

For the VPN-based remote access solution, engineers assumed a one-time procurement and installation cost for the dedicated VPN hardware during the 1st year of ownership, and no further capital expenditure in the second and third years of ownership. Furthermore, engineers assumed that hardware redundancy is required to ensure continuous access to the corporate network over VPN.

Since GoToMyPC Corporate is delivered as a SaaS solution, there is no need for dedicated hardware on the corporate network, thereby resulting in considerable savings in the up-front costs to deliver the service. Also, since all hardware redundancy is taken care of by Citrix Online, the cost savings to the users are significant.

Cost of Software

The need for a client software on the user computers to access the VPN can incur additional cost. Engineers assumed that the software licenses and support contracts to be a one-time expense during the first year of the 3-year deployment period.

Citrix GoToMyPC Corporate is offered as a SaaS solution, and no dedicated client software (apart from a modern Web browser) needs to be installed on the user computer. The subscription to the service is sold on a monthly or annual basis, and will need to be renewed annually over the 3-year deployment period.

Operational Costs

For the VPN-based remote access solution, the need for dedicated

hardware on the corporate network incurs additional operational expenditure to power, cool and manage the hardware. The infrastructure for GoToMyPC Corporate service is maintained by Citrix Online, so the user does not incur operational costs on the hardware.

In addition, the need for dedicated hardware and software for VPN-based solution incurs additional installation, maintenance and end-user support costs. GoToMyPC Corporate minimizes the installation and maintenance costs, and global, 24x7 technical support is included in the subscription fee.

Energy Consumption Costs

The need for dedicated VPN hardware on the corporate network results in additional costs to power and cool the hardware. Since GoToMyPC Corporate is a hosted service, users do not incur additional energy consumption costs for the service infrastructure.

For the representative Cisco VPN hardware, engineers obtained the power consumption (in Watts) at steady state from the vendor supplied data sheet. Engineers further assumed that the cost to cool the hardware was 30% of the cost it takes to power the hardware. This power consumption value was then calculated over a one-year period, using representative pricing of \$0.103 per kWh, obtained from the average retail price of industrial sector power in the state of California, USA, for the month of November 2008 (data available online at

http://www.eia.doe.gov/cneaf/electricity/epm/table5_6_b.html).



About Citrix GoToMyPC Corporate

To learn more about Citrix GoToMyPC Corporate, please call 1-866-646-0016. If you are calling from outside the U.S., dial +1-805-690-5780.

You can also get a free evaluation at <http://www.gotomypc.com/corp>

About Tolly

The Tolly Group companies have been delivering world-class IT services for 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company via E-mail at sales@tolly.com, or via telephone at +1 561.391.5610.

Visit Tolly on the Internet at: <http://www.tolly.com>

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.