26 York Street
London W1U 6PZ
United Kingdom

Stepney Marsh SYSTEMS

+44 20 7873 2127
www.stepneymarsh.com
info@stepneymarsh.com

Remote Access

Methods & Options

4 April 2012

INTRODUCTION

Remote access technology allows users to connect to their office computing resources while out of the office. Often, this may only be to access e-mail via web-mail using a browser, but it can also comprise of access to all office applications and data. Such solutions could be accessed from the home, hotels, other offices, Internet cafés, or even outdoors via the mobile phone networks from devices such as the iPad.

Remote access can also be used for connecting a small remote office to a main office at low cost, or can be used as a form of disaster recovery. For example, if an office becomes inaccessible, users could continue working from home. No "hot site" office needs to be arranged.

Before we get into a discussion of typical remote access solutions, we need to understand the two primary methods of remote access: remote node and remote control.

Remote Node

This solution simply extends the office network to the remote Personal Computer (PC) or mobile device. The remote PC becomes a node on the main network. This is typically accomplished using a software-based Virtual Private Network (VPN) on the remote PC so that it can connect from any Internet connection.

Pros

- seamless integration for laptop computers; users have the same computing environment whether at the office or on the road
- easy to transfer files between the remote computer and the office
- Implementation costs are usually lower than a remote control solution, as even low-end firewalls come equipped with a VPN connection these days.
- The user can work on the PC without a connection to the office.

Cons

- Software identical to that on the office workstations is required on the remote PC in order to read corporate data. For example, to log onto an SAP application server, the SAP client software must also reside on the PC.
- VPN software must be installed (if not using the native Microsoft client), maintained, and supported on all remote PCs.
- "Unmanaged PCs" (those that are not maintained by the corporate IT team or consultants) bring the risk of exposing viruses onto the corporate network or inadvertently connecting that network with yet another network to which that PC may also be connecting.
- Because of the previous requirements, users typically must use their own "managed" PC or a company laptop, one that has been configured correctly.
- The previous requirements greatly increase IT resource requirements in order to support all remote PCs. This can be a more expensive solution in the long run than remote control.
- Because VPN and identical office software must reside on the PC, this solution would not enable seamless access from an Internet café or at a non-configured PC at another business' site.
- Unless the VPN is using the SSL protocol (one that is also used to access secure web sites), it is likely that the client VPN may not work from inside another business' network, as their firewall would likely block such protocols from leaving their network.
- Database applications and access to files stored on office file servers may be slow performance, as the data needs to be transferred across the remote connection to the PC.

Remote Control

A computer is remotely controlled at the office and configured with the business' standard applications. This could be a user's primary workstation or a spare. A workstation can only be used by one person at a time, whether local or remote. Alternatively, a purpose-built server can also be simultaneously and remotely controlled by many users. This would typically be a Microsoft Windows Server with Terminal Services installed, possibly also with Citrix software. Users log onto the computer and are presented with either a Desktop window (a Desktop within a Desktop) or a full-screen Desktop which "replaces" their local Desktop.

Pros

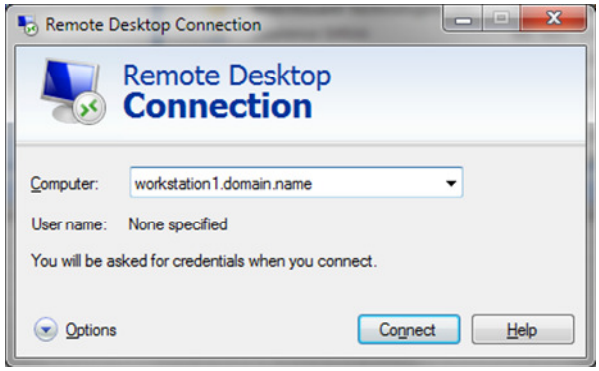
- Because the user remotely controls a session on a computer in the office, no data is transferred; therefore the performance is virtually the same as being in the office, even via a slow connection.
- If the correct remote control solution is in place, users can access office applications from any PC in the world (including from an Internet café) as long as it is connected to the Internet and has a web browser; no laptop or mobile device is required for travelling.
- Unmanaged PCs may also safely connect using this method, as there is no direct data link between them and the office network. The network is safe from any possible viruses on the client computer.
- No other software is required on the remote PC so ongoing support costs for these PCs are almost nil.

Cons

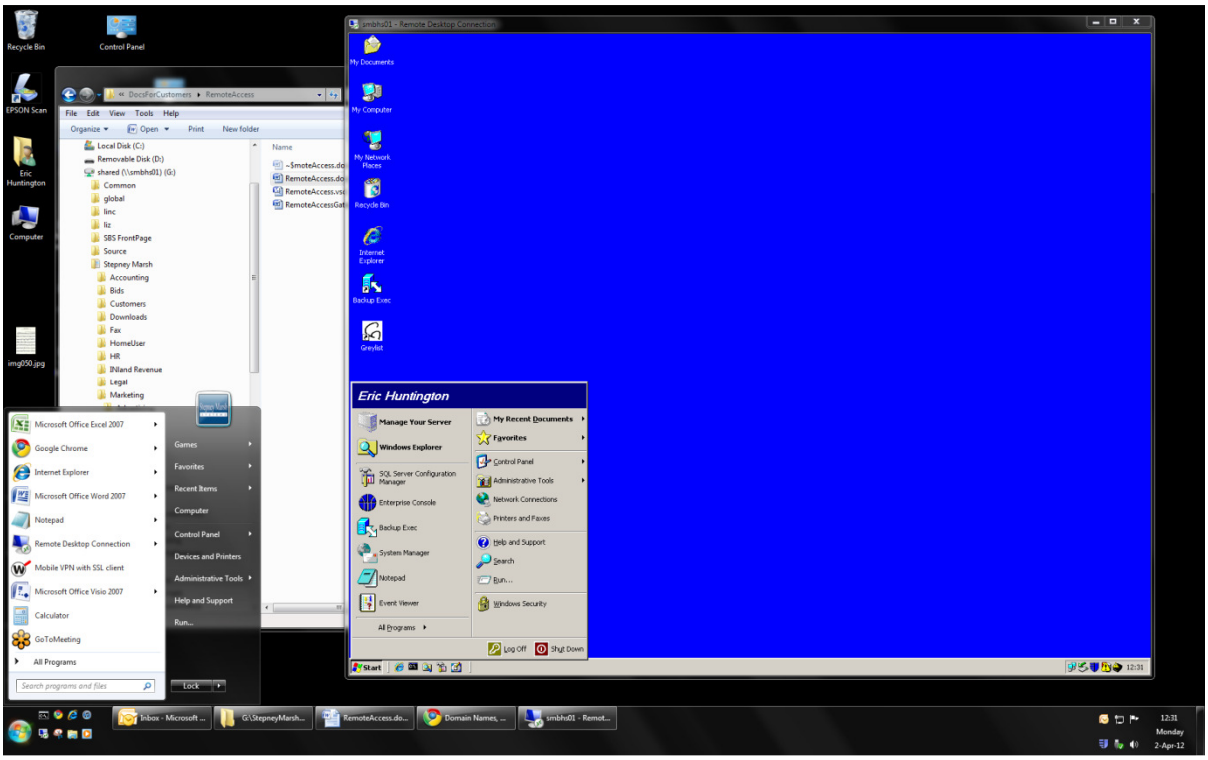
- This can be a significantly more expensive solution to implement than a remote node solution.
- An Internet connection is required in order to do any work. For example, it would be inaccessible from a laptop computer on an airplane (although this is changing).

Other Terms

- The term "Desktop" with a capital "D" in this document refers to the screen that Windows presents to the user on the monitor: the background, the Task Bar, the System Tray (bottom right corner by the clock), the Start Button and Menu, and the Desktop icons.
- "Remote Desktop" is the user-friendly name for Microsoft's Remote Desktop Protocol (RDP), the software and protocols to remotely view and control a Desktop on another Windows computer. The initial screen is shown to the right.



  Sometimes the remote Desktop is maximised so it fills your entire local Desktop. It appears as if you are working on the remote computer locally. Some users do not perceive the difference. Sometimes the remote Desktop is a window in your local Desktop, as shown below (the remote Desktop with the blue background is a window within the local Desktop with the black background):

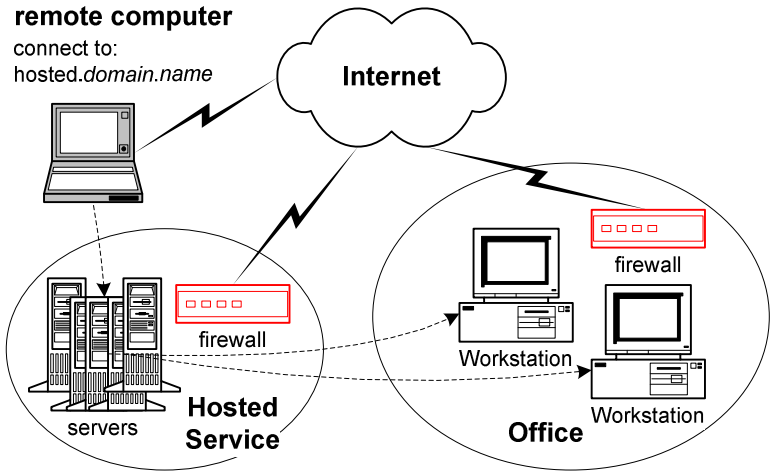


OPTIONS

Pros and cons listed in the sections below are in addition to the more general points above.

Hosted Remote Control

Third-party companies offer a service where an agent (a piece of software) runs on the office workstation which connects to their hosting servers. Users then log into their server via a web-site from any Internet-connected computer and are presented with a window that is the Desktop of that office workstation. These are typically paid for by annual subscription. Products include Citrix's GoToMyPC or Bomgar.



Pros

- reasonably cheap to buy and use
- very easy and cheap to implement for small numbers
- access from any PC
- easy to use

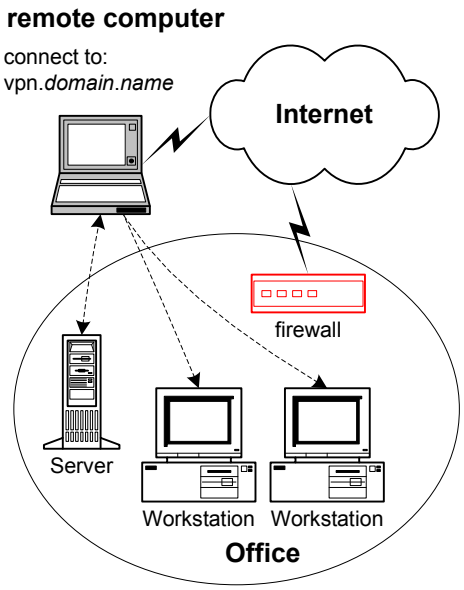
Cons

- need the controlled PC to be available, powered on, and not being used by anyone else
- would get expensive once many users are connecting to the office network
- not as secure as in-house solutions

- difficult to manage, and therefore more expensive, for a large number of workstations

VPN Only

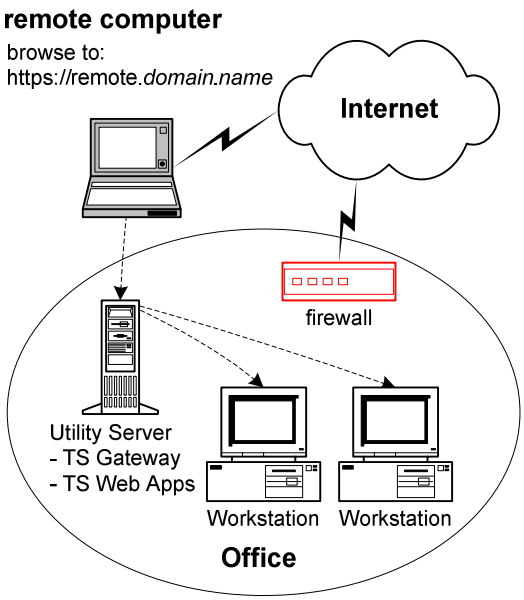
A piece of software, either third-party or Windows's built-in **Connect to a network** wizard, is launched from the client computer. It provides a virtual connection to the firewall on the office network, and thus to the internal office network. This is the only remote-node option presented as an entire solution (there are other solutions below which may provide a remote-node solution as well as remote-control).



Remote-node is the only method where users may access resources on the office network other than using remote control software. For example, a copy of the logon script may reside on the user's local Desktop, which they can click and, voilà, mapped network drives exist, just like at work. Remote Desktop may also be used. The pros and cons to this are sufficiently described in the introduction above.

Remote Control via a Gateway

This solutions is in many ways similar to the Hosted Remote Control option described above. The gateway to which the client connects, however, is located at the office network. Furthermore, the gateway usually uses the internal user database with which to authenticate users, so they may log on with their usual Windows network user name and password. The products chosen here are Microsoft's Terminal Services Gateway (TS Gateway) and Terminal Services Web Access (TS Web). These components are both included with the Microsoft Windows Server operating system; they do not need to be purchased separately.



Users access workstations in the office by browsing to a secure web-site, logging on with their usual credentials, and then selecting from a list of available computers on the network to remotely control.

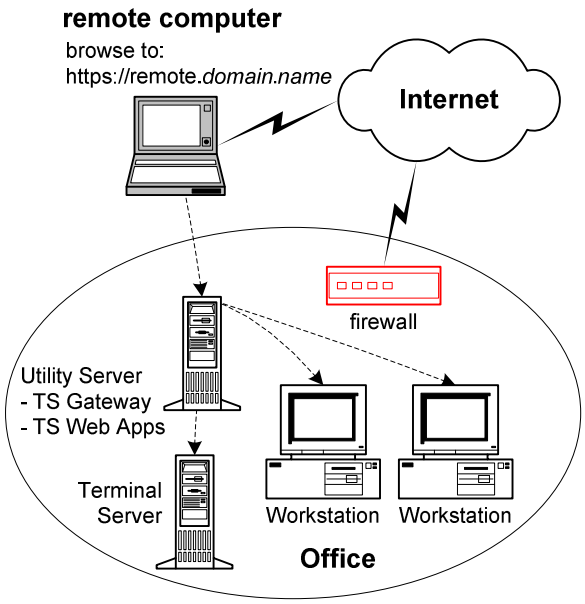
Pros

- easy to use for end-users
- reasonably cheap to set up and maintain

Con

- need the controlled PC to be available, powered on, and not being used by anyone else

Terminal Server



The connection technology and method uses the same TS Gateway and TS Web as described above. The only difference is that there is also a dedicated Terminal Server on the corporate network which users remotely control. Think of it as a Windows workstation with the sole difference that many users can remotely control a session on it concurrently. The TS Web may be set up to only allow remote users to the server or it may continue to allow connections to individual Windows workstations.

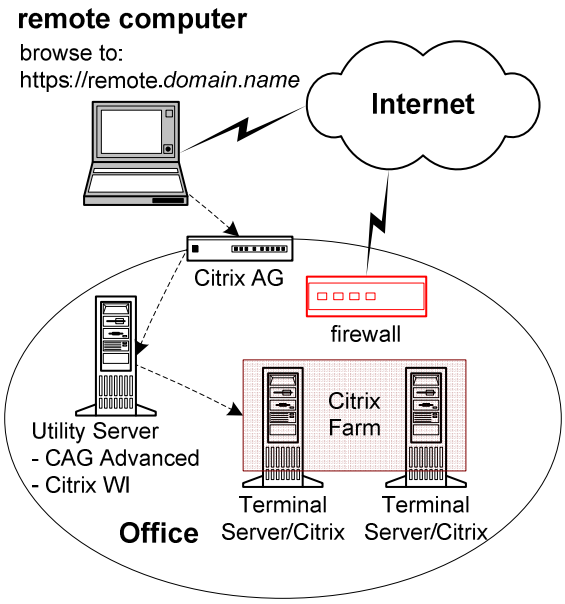
Pros

- The main benefit is that users no longer need to have a workstation available to which to connect.
- even easier for end-users to use; it can be configured with a single icon of one remote server to select from the web page
- it provides a built-in form of disaster recovery, many users can work from home or other locations if the office becomes physically inaccessible

Con

- As many users may be using this server at one time, it must be reasonably powerful, which adds significantly to the cost of the whole solution (whether in price for a new bare-metal server or resources for a virtual machine).

Citrix



Citrix is combination of hardware and software components that add on to a Terminal Server and remote access solution. The software would be installed on top of the Terminal Server described above, using the same hardware resources for that piece. Other software would replace the TS Web component on the utility server described in the Gateway section above, though installed on the same physical (or virtual) server. A hardware component called the Citrix Access Gateway (CAG, which may now also be called the NetScaler Access Gateway) sits outside the network firewall and performs similar functions to the Microsoft TS Gateway component.

Citrix makes the whole solution a bit more seamless for the end-user. Single sign-on will always work, even with two-factor authentication described below. Single applications can be "published", that is, an icon is presented on the web page after logging in that can run one application only, and it would appear to be running locally on the workstation. Citrix has its own remote control protocol, ICA (Independent Computing Architecture) which is a little faster than Microsoft's RDP, and handles features such as remote printing, sound, and colour depth better than RDP.

If the solution were to ever grow to two or more Terminal/Citrix servers, Citrix also seamlessly deals with load-balancing user sessions among the servers. It does this in a much more flexible and manageable way than Microsoft's method.

Pros

- best seamless experience for the end-user
- fastest performance
- much easier to grow, both in scope and in maximum concurrent users
- infrastructure in place for in-house application publishing, another topic involving savings of managing applications
- This is also the most secure solution, as the CAG can be configured to do numerous checks against the client computer before allowing it to connect. Microsoft has a similar offering, but Citrix has always worked on all platforms (Mac, Linux, hand-helds), and not just on Microsoft clients.

Con

- most expensive solution, both in terms of product pricing and consulting required for installation

SECURITY

Any type of remote access solution enables some form of connectivity to the office, which becomes a potential weak area in network security. All methods above connect over a secure connection, which means that if someone were to capture that network traffic, the contents would all be encrypted. While it might be possible to crack these secure sessions, this is not the real problem.

The trouble is someone logging on, pretending to be an employee or partner, and then having access to your resources (over their own "secure" connection). Whether they crack your password using brute-strength utilities, retrieve the username and password that is stuck on a monitor or under a keyboard while strolling through the office posing as a visitor, or obtain the credentials using social engineering - this is a much easier method to illicitly gain access to a corporate office with remote access enabled. This risk is true for any remote access method.

- **Hosted Remote Control** aids this issue in that the end-user needs two sets of credentials: those to log onto the provider's web-site and those to then log onto their workstation. A new risk is added, however, in that we must now also trust the security of this provider.
- **VPN** is a somewhat risky solution because not only could someone log in as the identity of a valid user, but they could possibly download and then delete all data from the network if that user ID had sufficient rights. Computer viruses and other malware can also be uploaded onto the network in this manner.
- **Remote Control via a Gateway**, **Terminal Server**, and **Citrix** are all remote control solutions using in-house resources, so their risks are the same. In fact, these are the least risky solutions.

All solutions would gain added security with a two-factor authentication mechanism. This is where the user possesses a physical token, often in the form of a key fob that either shows a constantly changing number to be typed in or contains a key that plugs into most computers. For the user to gain access to corporate resources, they must provide something they know, their user name and password, and something they possess, the number on the token or the physical key.

Different technologies exist to provide a reliable and secure connection to corporate computer resources from virtually any location on the planet, each with their pros and cons. The benefits are numerous, but such solutions must be implemented properly and with sufficient respect to network security.