VPN and Firewall Solutions for Small Offices and Homes

David M. Ihnat
dihnat@dminet.com

17 January 2004

1. INTRODUCTION

On occasion, all information technology installations encounter situations in which hardware and software administrative operations require the on-site presence of skilled personnel. This inevitably incurs additional costs such as travel expenses, as well as the inconvenience of having to schedule the on-site session.

A great number of software administrative tasks could be accomplished if privileged off-site access was a readily available option; with respect to security, this is, of course, a sensitive issue for any client.

Now, the implementation of VPN services in firewall/router appliances has matured to the point that such a solution is a viable and affordable service. This memorandum summarizes the characteristics of such a VPN connection, and suggests reasonable implementations for small office and home installations, commonly referred to as SOHO.

2. OVERVIEW

The following section is provided as an aid to those who may not be conversant with VPN solutions.

2.1 VIRTUAL PRIVATE NETWORK

A Virtual Private Network (VPN) establishes a cryptographically secure 'tunnel' between two locations over an otherwise insecure network, e.g., between two trusted sites on untrusted Internet links provided by the same or even different commercial Internet Service Providers.

A VPN link may be between two computers, for instance Windows servers running the VPN software as part of the operating system. In this case, specially permitted access between the particular computers participating in the VPN scheme must be programmed in the firewalls protecting each site (common parlance for this is "boring holes" through the firewall). While this can be done with reasonable security, it does effectively remove the firewall from the security model with respect to the VPN itself; security now relies on the operating system configuration on the servers hosting the VPN.

A much more attractive model is one in which the firewalls themselves support the VPN protocols and handle all security and link negotiations. This is accomplished both with proprietary VPN implementations and, more commonly today, with firewall-supported implementations of public VPN protocols such as IP Security Protocol (IPSEC). Most such implementations also allow use of VPN client software on one end of the link, allowing such capabilities as establishing a secure VPN between the site firewall and off-site administrators or workers who may not have a firewall, or not have a compatible firewall.

2.2 REMOTE MACHINE ACCESS AND CONTROL

Once a VPN link has been established, normal activities can be carried out as if the remote site or machine is actually attached to the local network, e.g., print services may be used and attachments made to network shared disk storage.

As with a local network, however, it's not possible to manage a Windows system remotely without additional software. This can be native, if running Windows 2000, via Windows Terminal Services. Alternatively, it can be a third-party software package—especially necessary if there are still earlier versions of Windows or non-Windows operating systems that must be maintained, or licensing for Windows Terminal Services is problematic. For Windows 98 or NT, a common commercial solution is pcAnywhere; and an Open Source package extremely popular among professionals and administrators today is the Virtual Network Computer (VNC) package or one of its many variants, available for legal use without licensing fees.

2.3 FIREWALL/ROUTER INTERNET APPLIANCES

Firewalls have, traditionally, been expensive—usually more than $10,000 each—and complex to set up and administer. In just the last few years, however, the recognized need to promulgate reasonable Internet security at affordable prices has led to the proliferation of "Firewall/Router Internet Appliances". These devices are, essentially, pre-programmed firewalls in firmware, usually combined with DSL or Cable router capabilities. Prices for reasonable home devices have come down to the range of 50-70 USD, depending on capabilities and features.

These devices usually are a bit too simplistic for business and professional use; shortcomings usually revolve around notification, logging, and administrative functions. For these purposes, a class of router/firewall appliances known by the sobriquet "SOHO firewalls" (Small Office HOme) has become popular. These usually cost a 4-6 times more than bottom-of-the-line appliances, but offer capabilities that previously were only available in full-priced firewall installations, including native VPN user accounts, more detailed control over sessions, logging/reporting to such facilities as 'syslog', etc.

3. SMALL OFFICE AND HOME BUSINESS CONSIDERATIONS

Typically, in the SOHO environment there is no on-site IT staff, nor is there an IT budget to support costly or labor-intensive support solutions. Often, when no alternative is available, support for general IT issues is provided on an as-needed contract basis, and usually requires an on-site visit, with concomitant travel expenses.

A security solution that provides better firewall and auditing capabilities, in addition to secure, on-demand and controllable remote access for those IT activities that don't require hands-on presence would result in both an improvement in security and maintainability and a significant cost savings.

3.1 SECURITY AND REMOTE CONTROL

Any solution proposal must provide three major functions:

- Ü Reasonable firewall/security functions
- Ü Secure, auditable and revocable remote VPN access to the network

- Affordable and secure remote control of Windows servers and workstations over the VPN (and possibly other platforms, such as Linux.)

3.1.1 Firewall/Security and VPN Selection and Maintenance Considerations

Most SOHO application needs are relatively modest with respect to a firewall/router appliance supporting VPN capabilities. Any solution must provide:

- The ability to provide reasonable auditing on demand.
- Individually revocable and secured VPN access.
- Reasonably flexible firewall capabilities, particularly the ability to selectively allow and deny application access through the firewall.
- The capability for secure remote administration of the device

At this point, it's appropriate to say a word about firewall protection. This is not a treatise on firewalls—a complex topic in its own right—it is to explain, at a high level, the concept of a VPN and remote control configuration. However, firewalls and VPN security are inextricably intertwined, so it's appropriate to take a very high-level look at firewalls in their own right.

Simply stated, a firewall is a specialized program that uses its control over networking functions to examine, classify, and control access requests from within and outside a network to the network's resources. Sometimes this program runs on an otherwise general-purpose computer, in which case it's called a software firewall. Sometimes it's embedded in a specialized computer dedicated to the firewall function; this comprises the most common "traditional" firewall configuration. And sometimes the software is embedded in the firmware—software that is impressed on special memory—in a hardware configuration dedicated only to supporting the firewall; these are commonly called firewall appliances.

3.1.1.1 Software Firewalls

There is a wide range in the reliability, flexibility, and capabilities of software firewalls. At the lowest end are such commercial products as *Black Ice Defender* or *ZoneAlarm*. Now, it should be said—*any* reasonable firewall is better than *no* protection. Furthermore, for applications such as laptops or desktop computers, an add-on software firewall such as these ranges from an absolute necessity (laptop) to extremely useful.

But these firewall programs share two common risks. First, they're running on a system that is continually running software not at all related to the function of being a firewall. Including, possibly, software that inadvertently or deliberately corrupts or inhibits their functioning. And secondly, they're not part of the underlying operating system—they're layered on top of it, and are usually not written or supported by the vendor or authors of the operating system itself.

Consequently, solutions such as these are inadequate for protection of more than an individual machine, and should be examined carefully while in use.

Now that the preceding caveat has been issued, it should be noted that another type of software firewall has surfaced in recent years. The Linux operating system has firewall capabilities designed into it, incorporated as part and parcel of the operating system itself; when properly configured, a Linux system makes a very adequate firewall, and if used only as a firewall, actually migrates to the next section as a Firewall in its own right.

Similarly, Windows 2000 and XP Professional provide firewall-like functions as part of the operating system networking (although most IT professionals don't grant these capabilities as

being the equivalent of a fully functional firewall). When configured, however, these provide integrated security and certainly additional support to any software firewalls on the same system.

3.1.1.2 Firewalls

These are the firewall applications that reached commercial prominence for so long—products such as *Sidewinder* and *Gauntlet*. These commonly are extremely complex, incredibly flexible, provide extensive auditing and logging functions—and have price tags far beyond the means of most small companies.

The advent of Linux, as mentioned above, has provided real firewall capabilities for much less investment in hardware and software. There are still capabilities provided in "traditional" firewalls that are only now evolving into the Linux distributions, but in most cases these are only important in the most high-level security installations—usually, far beyond the concerns or needs of business security.

3.1.1.3 Firewall Appliances

Traditional firewalls are complex beasts; difficult to properly configure and expensive. Software firewalls have vulnerabilities and don't well scale to secure support of a network of systems. Furthermore, with the proliferation of always-on broadband to small businesses and, increasingly, households across the country, some easy-to-implement and affordable solution was needed. The firewall appliance has appeared to fill this niche. These are usually totally self-contained devices, with no hard drives or "attackable" software. The programs that provide the firewall functions are "burned" into firmware—generally unmodifiable storage[1]—and the devices are pre-programmed with the most commonly useful and applicable configurations that are encountered in the field.

A lowest-end firewall appliance, such as a Linksys or D-Link, will provide a minimal level of control, passable protection, and relatively limited reporting capabilities. It's not possible to create some of the more esoteric configurations that may sometimes be needed for business applications, and while it's possible to provide remote control of the firewall configuration, the ability to audit such access is generally inadequate.

Those devices specifically targeted at SOHO applications—the WatchGuard Firebox SOHO 6 and Sonic SOHO are the touchstones for this class of equipment—provide a greater degree of control and auditability. Some higher-end devices, such as the Sun Pix or the WatchGuard Firebox, fill a mid-level niche—at a greater cost.

3.1.2 Remote Control

Beyond establishment of the VPN itself, it's also necessary to provide for remote control of on-site servers and workstations. Most commonly today, this means Windows NT, 2000, or 2003 Servers and many versions of Windows on workstations—95/98/98SE/Me/XP. In addition, a not insignificant number of sites still run Novell and traditional Unix, and Linux is an increasing and clearly important presence both as servers and workstations; and Apples are very popular for home applications.

---

[1] Provision is almost universally made to allow the user to update these firmware programs—after all, a program is a program, and can (almost always does!) have bugs that must be fixed. But these update mechanisms also almost universally require a great degree of manual intervention to prevent corruption by the "Black Hats".

Once a VPN has been established, there are a couple of solutions available to accomplish remote control for various platforms ranging from fully supported commercial applications to robust solutions at little or no expense.

3.1.2.1 Windows

While commercial solutions exist (e.g., pcAnywhere), a good, reliable open source solution that is in wide use is *RealVNC* (Virtual Network Computer, http://www.realvnc.com) or one of its many variants such as *tightVNC*. These are all distributed under the GNU General Public License; the pertinence of this to SOHO users is that there is no cost associated with the application.

3.1.2.2 NetWare

Novell's ConsoleOne RCONJ utility provides more than adequate remote control capabilities. Another good alternative is AdRem's Free Remote Console (http://www.adremsoft.com/freecon).

3.1.2.3 Linux/Unix

For all intents and purposes, when considering remote control and access Unix and Linux are the same platform. There are two common approaches to remote access to Unix/Linux: Command Line Interface (CLI), or Graphical User Interface (GUI).

3.1.2.3.1 Command Line Interface (CLI)

CLI interfaces are commonly preferred by "old-time" administrators for a number of reasons beyond simple familiarity. They're lightweight, requiring much less bandwidth and support software on the client side. The scripting capabilities of Unix/Linux are legendary, giving the CLI user and administrator power and flexibility that is unrivalled among competing operating environments. Finally, there is a plethora of terminal emulation programs that are fully adequate to provide a CLI interface, on virtually every platform. Solutions such as *PuTTY* (free; also sports SSH capabilities), *WRQ Reflections* (commercial), or the venerable *HyperTerminal* provide access from Windows, for instance.

3.1.2.3.2 Graphical User Interface (GUI)

There are numerous choices for remote control of a Unix/Linux system; however, two are most commonly encountered.

The traditional, and most efficient, is to use an X Server package. There are numerous Open Source packages available in source or binary for Unix, Linux, or Windows—GIMP or KDE, for instance—as well as commercial ones, such as the venerable *WRQ Reflections X*.

A second alternative is to use *RealVNC* to control the native X server. This has the advantage of both a dedicated client, and a "generic" Web interface.

3.1.2.4 Apple

As with Unix, particularly as of Mac OS X (which is "Unix in disguise"), the option exists to run SSH for a CLI.

GUI interfaces are probably more favored; there are, again, numerous applications from both the Open Source and commercial camps, such as the ubiquitous Timbuktu, and Apple Remote Desktop.

4. CONCLUSIONS

There are two requirements for remote administration of a network—reasonably secure Virtual Private Networking (VPN), and tools to allow manipulation of the devices and computers on the remote network. Both of these capabilities are now available at quite reasonable costs, and should be considered by any individual or organization tasked with providing the best and most affordable possible support to networks and systems in their care.