



Outsourcing Firewall Management

A Cost and Feature Effective Approach for Businesses

By Randy Johnston, Executive VP, K2 Enterprises, LLC

There are excellent software and hardware solutions available for protecting a business's connections to outside networks. This category of security of hardware and software is often referred to as the corporate firewall. These edge security solutions (to use Microsoft terminology) do far more with respect to security than just filter traffic. They also provide patch management across the network, management of anti-virus and other code blocking software, management of VPNs and other remote communications, and much more. Having a good edge security solution is clearly a cornerstone for almost any well conceived security plan.

Microsoft, Cisco, SonicWall, Symantec, Computer Associates and hundreds of other companies have solid offerings in this space. Microsoft, for example, has their Forefront Client Security, Server Security, and Edge Security and Access products. The following is a list of the features these types of applications typically perform:

- Update Client Computer Signature Files
- Use Policies to Manage Client Computers
- Alerting, Reporting, and Monitoring of Client Computers
- E-mail based Workflow
- Server Virus Protection
- Secure Remote Access
- Branch Office Security
- Full Internet Access Protection
- Added Protection for Applications Like SharePoint that Have Regular Remote Access
- All done centrally from one management console

These are important functions. If implemented and managed properly, these features have proven to protect an organization well. There are still challenges but this is a mature market with lots of well established high quality players. The products are strong but still require human expertise to achieve maximum efficiency because they are also complex.

Here in lies the rub for many businesses. The SBs (small businesses) and SMBs (small to medium businesses) don't generally have the depth and breadth of IT staff to manage these services properly. Even in shops where a business has sufficient IT staff to understand and manage their perimeter security solution efficiently, they may not be as effective as they would like because they only have experience with their one system. Outside experts have the advantage of working with multiple systems and therefore more experience with common issues and acceptable solutions.

Just for background and understanding, some of these solutions are packaged as turnkey hardware and software bundles, some like Microsoft Internet Security and Acceleration (ISA) Server are, as their name implies, complete server based solutions. In reality most are at minimum a combination of hardware and software. For example, in the well respected SonicWALL line, the baseline hardware is just the foundation. Security software forms the core security while working to take full advantage of the additional opportunities the hardware offers working in concert with the software. Software licensing fees (and not pure hardware) will clearly be your biggest commodity purchase cost in the security budget for many SBs and SMBs. The services to implement this properly will not be cheap, but will be critical to making everything work properly.

But, it is important to remember: if implemented and managed properly, the new generation of security tools is very cool and work very well. They will give you assurance that machines are patched and anti-everything is working and properly patched.

This is a level of assurance that many business computers in the US are apparently without. The CSI's 12th Annual Computer Crime and Security Survey (2007) reported that "Losses from Viruses" was the 2nd largest security cost to US Businesses. Financial fraud was first. Many of the machines suffering these attacks are poorly protected and the lack of proper protection is either the direct cause or at minimum a contributing factor. Even in larger organizations where sophisticated management workflow procedures can be implemented to control all connected platforms, it is often difficult to walk the fine line between productivity and control with devices such as connected handhelds, laptops, phones, etc.

This leads to the following two conclusions:

1. There are many small businesses that are still in need of good edge security but are not large enough to have in-house IT expertise of the level needed to manage many of these newer and better tools effectively.
2. Even in shops where there is highly trained IT staff, those staff may not have the depth and breadth of knowledge of potential problems or even current problems because the in-house people only know one system, their own.

The point after all is to get the best security at the most reasonable cost. Even in the second situation where you have quality in-house IT staff, their knowledge and understanding of the unique needs of their business may be best served by working with someone who manages the daily tasks and consults with the in-house IT staff when necessary. The in-house people will have more time to move on to unique business issues because they are relieved of the burden of daily management. The business gains the assurance from a certified independent third party that the edge security is being managed properly. This in no small point when dealing with the new era of corporate responsibility that Sarbanes-Oxley and other recent legislation brought on.

So what are the options for outsourcing perimeter security and how much do they cost? Well as it turns out there are also lots of well established players in the managed edge security services. Some you have likely heard of; Sun Microsystems, VeriSign, Vanguard, Unisys, Symantec. Some large players like BAI and Savvis are not so well known outside the security world. The following is a sampling of an offering from a company call Dotnoc:

Remote administration/support for windows servers

Remote computer support globally

Remote Support saves you time and frustration by providing quicker access and response to computer support help. Dotnoc offers remote administration and support services for Windows servers. We support major Microsoft technologies such as:

- ▣ Sharepoint Portal
- ▣ Exchange server
- ▣ Terminal Server
- ▣ ISA Server
- ▣ SQL Server
- ▣ MPS Server

Cant get a technician onsite? Give us a call to see how we can help you remotely. Dotnoc specializes in Windows server configurations, support and troubleshooting. We support your servers no matter where they are, a data center, a collocation, a rented or dedicated server or a server you have in your own location.

Remote administration types

Dotnoc can remotely administrate your servers via many remote services.

- ▣ Terminal Services (RDP)
- ▣ VNC (All VNC servers such as Real VNC, Tight VNC & Ultra VNC)
- ▣ PCAnywhere (third party software required)
- ▣ Client provided remote administration type

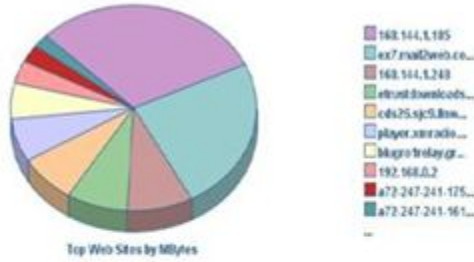
Source: <http://www.dotnoc.com/windows-remote-administration.php>

With remote support and management SB can receive a level of control, assurance, and useful reports that probably would be impossible or cost prohibitive without outsourcing. We have been using managed firewall services (<http://www.nmgi.com/netcare/index.shtml>) for several years with great success. Our contract takes care of not only keeping all hardware, code and licenses up-to-date and working property but even includes periodic hardware replacement. It is no longer a capital expenditure to “upgrade” the firewall and no additional consulting services are needed.

The reporting we receive is far superior to what we had when we managed our own firewall. Monthly, a 38 page report that is customized to show the charts and graphs that are useful and meaningful to me as a business manager. Their people interview me from time to time to make sure I am informed about issues and potential issues they think I should consider. Additionally, I receive alerts if anything goes wrong (ex. hurricane takes out power longer than generator can last). Fortunately that has not happened for a while. All for a flat monthly fee that I can budget and that costs less than I was paying previously for software and hardware upgrades and consulting.

Apparently there is software out there that organizations like NMGI can use to automate much of the remote management process for multiple networks simultaneously. This allows them to provide me with a higher quality product at a lower price. The following is taken from my March 31, 2008 NMGI NetSecure Report.

Top Visited Web Sites for 2008-3-1 - 2008-3-31



Site	Hits	MBytes	Category	% of MBytes
1 168.144.1.185	2224	809,561	N/A	30.437%
2 ex7.mail2web.com	17610	640,329	N/A	24.075%
3 168.144.1.248	7	226,059	N/A	8.499%
4 etrustdownloads.ca.com	26945	215,272	N/A	8.094%
5 cds26.sjc9.linw.net	1667	196,030	N/A	7.370%
6 player.xmradio.com	129194	185,068	N/A	6.958%
7 blugro1relay.groove.microsoft.com	297	146,778	N/A	5.518%
8 192.168.0.2	73	94,686	N/A	3.560%
9 a72-247-241-175.depl oy.akamaitechnologies.com	229	74,986	N/A	2.819%
10 a72-247-241-161.depl oy.akamaitechnologies.com	8176	71,007	N/A	2.670%
Total	186422	2659,774		100.000%

Source: Monthly Report to K2 Enterprises for Outsourced Firewall Management Team

The system also provided information on Intrusion Detection, VPN activity, attempted attacks, etc. But those reports are not as useful to me as a manager as usage, types of usages, and measurements of whether or not I have adequate bandwidth. You see, I count on the outsourced management team to take care of all the security stuff. It's their job and their core competence and not mine. I am a business manager. Shouldn't you consider using managed firewall services as well?

Sources for Further Reading:

<http://www.microsoft.com/isaserver/default.msp>

Microsoft Internet Security and Acceleration (ISA) Server 2006

<http://www.dotnoc.com/windows-remote-administration.php>

Provider of Managed Microsoft Security Solutions

<http://www.nmgi.com/netcare/index.shtml>

NMGI NetCare Managed IT Services

<http://www.verisign.com/managed-security-services/>

VeriSign Managed Security Services

<http://www.windowsecurity.com/services/Managed-security-services/>

List of 32 Companies Providing Managed Security Services

http://www.gocsi.com/forms/csi_survey.jhtml

CSI's 12th Annual Computer Crime and Security Survey (2007)