Securing Home Office

Matt Moberg

ICTN6865

Dr. Phil Lunsford

October 22, 2008

Abstract

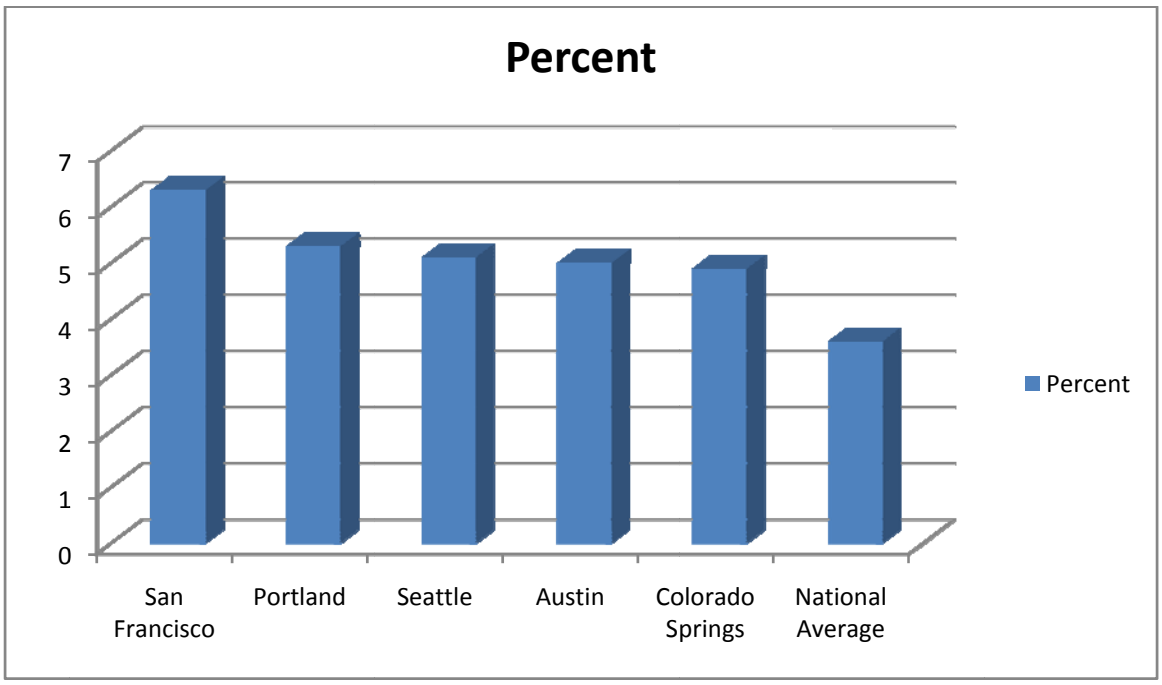
Never before has so much technology and Internet access been available to the home user. Each year, more and more Americans are working from home. Because so many people now have home offices, the need for security has never been higher. Securing the home office need not be a difficult exercise. There are several considerations that need to be addressed to safely secure the home network from the outside world. The goal of this paper is to address the common vulnerabilities of the average home office and to suggest methods to safely secure it.

Securing the Home Office

The availability of affordable computer hardware and peripherals has never been better. Technological advances have also provided the home user to incredible amounts of Internet bandwidth. These two trends have led to a dramatic increase in the number of Americans who work from home. Right now, some 4.2 million Americans work exclusively from home (Penn, 2007) with another 20 million working part time. In the last 25 years, the number has increased 650% (Whittenhauer, 2008). A nationwide study found the following cities having the highest number of home workers: (Table 1)

Table 1

Cities with the highest number of home workers



Note: Source U.S. Census 2005

Chart by Matt Moberg

It is common for almost any home to now have routers, wireless appliances, laptops, personal computers, and other common local area network hardware (LAN). This security review will focus on the following topics:

1. ISP supplied hardware
2. Wireless routers
3. Commonly used firewall ports
4. Securing applications and port usage
5. LAN considerations

Understanding the various threats or security loopholes that exist in this information age is a must for the home office. Once the home office is secured, it can provide an efficient and safe location to do one's work.

ISP Supplied Hardware

ISP stands for "Internet Service Provider." This is simply the vendor one selects to provide Internet access to the home office. There are several ways to get Internet to the home office, however, some sort of broadband Internet or DSL connection is likely. With these services, you will be provided with a modem/router device. This device is used to hand off the vendor supplied bandwidth to the local area network (LAN) in the home office.

The first security assessment we can make is the actual security risks of the services themselves. Since I have referenced cable and DSL, let us look at the way each service is provisioned. There are many in the industry who feels that DSL is clearly more secure than cable supplied Internet. Their reasoning is based on how each service is deployed. Cable service is dropped on a shared, single wire to each area. All the nodes in this area are accessing the service

from the same hardwire. In theory, one house could see the networks on the other houses sharing this Internet feed. In the past, this indeed did sometimes cause problems. Since then, cable providers install proprietary firewall rules on their appliances. Additionally, most cable companies run Data Over Cable Service Interface Specification (DOCSIS) on their devices (Mitchell, 2008) which provides authentication and packet filtering.

DSL however uses a dedicated connection to each respective client. Now, this comparison sounds like one service (DSL) is clearly superior than the other, however, there are other considerations. Both these services provide “always on” functionality. This is great for the home office because resources can be used at any time. However, since the connection is hot at all times, this provides an attacker a large window of opportunity. One other thing to address is how the IP is assigned to the device. A statically applied IP address provides a fixed point of attack for a hacker while a dynamically assigned address can change periodically. In summary, both services mentioned thus far are reliable in today’s networks. For security of the home office, the user should ask questions such as “Do you statically apply addresses or is it dynamic?” or “Does your appliance have firewall rules and run DOCSIS?” This type of information will allow a home office user to obtain a quality, secure service.

Wireless Router

A wireless router is an excellent and convenient piece of hardware that any home office can benefit from. The main concern with this appliance is security. The following is a list of recommendations that one should consider when deploying a wireless router:

1. Change the SSID and do not broadcast it. In a larger working area, the SSID is a useful feature. However, in a home office, there is no need to broadcast your SSID as the home user is locally situated.
2. Enable MAC address filtering. The router will keep track of all MAC addresses connecting to it. By manually entering the MAC address of every appliance that will use the router, you can limit access to what you want to control. Note however that is only a moderate option as hacker software can imitate MAC addresses.
3. Assign static addresses for each network appliance. The convenience of DHCP is well known, however, by manually telling what each IP address can access the router you are increasing your security.
4. Disable Auto-Connect to Wi-Fi networks if this option comes with your home router.
5. Use a WEP/WPA key. There are some concerns however that one must address. According to the EURASIP Journal on Wireless Communications and Networking, WPA encryption is susceptible to DoS flooding attacks (Rango, Lentini, Marano). This journal suggests an extension to the authentication phase of Wi-Fi protected access (WPA 1-5) and IEEE 802.11i. Another thing that must be considered is the WEP key. Using the RC4 algorithm, a WEP key of 128 bits is a secure method of protection. However, there have been some questions about RC4/WEP security on a wireless platform (Stallings, Brown, p. 610). According to the authors, it isn't necessarily RC4 itself that can produce a vulnerability but rather how the keys themselves are generated.

One also may consider the location of the wireless router. Some external broadcasting will inevitably take place, but, perhaps a centrally located area in the home office will limit this. One

may also consider turning the wireless router off during long periods of inactivity. Finally, changing the default administrator password should also be considered. For example, anyone who has worked in the IT field for any amount of time knows that for every new Linksys wireless router, the credentials for the device are no user id and a password of “admin.” You can go to Linksys’s website and download the user manual for the device and this information is published as well. Clearly such public knowledge means that hackers can take advantage of this information.

Commonly Used Firewall Ports

Now that the security for the Internet router/modem and the wireless device has been discussed, it is time to make all of the assets on your home LAN usable for the authenticated users. Using a firewall is an excellent way to control access/use to the home network. Some of the vendor supplied routers/modems have a firewall interface; however, access to this appliance administratively is not usually welcome. You can use the firewall that commonly comes with the wireless router or purchase a traditional firewall appliance such as a Cisco Catalyst or HP Procurve. Regardless of the appliance being used, the rules on port usage don’t change. Each service that your home office can use has some sort of port assigned to it. While these ports and their usage are not set in stone, there are certain ports that use commonly accepted port numbers. Internet Assigned Numbers Authority (IANA) has assigned ranges for particular uses. The IANA does not enforce these port ranges, but rather uses these ranges as a recommended practice. For security reasons, it is important to note this fact. A hacker can use their nefarious code on a port normally reserved for something else. See Table 2 below for the IANA ranges:

Table 2

IANA assigned ranges

Range Name	Port Range Assigned
Well known ports	0 – 1023
Registered ports	1024 - 49151
Dynamic/Private ports	49152 - 65535

Note: Source IANA

Chart created by Matt Moberg

The Well Known ports range is reserved for commonly accepted protocols and the programs that use them. Examples of this are FTP over port 21 or HTTP over port 80. The Registered port range contains the ports assigned by the Internet Corporation for Assigned Names and Numbers (ICANN). Finally, the Dynamic/Private ports are random and not assigned to any specific application. They are also commonly referred to as ephemeral ports. The focus of this paper is to secure the applications that normally use ports in the Well Known port range. A list of commonly used ports numbers (IANA, 2008) are described in Table 3:

Table 3

Common port associations

Port Number	Application	Protocol/s Used
21	FTP (Command)	TCP
21	Secure Shell (SSH)	TCP/UDP
23	Telnet	TCP
25	Simple Mail Transfer Protocol	TCP/UDP
53	DNS	UDP
80	Hypertext Transfer Protocol	TCP
110	POP3	TCP
123	Network Time	UDP
443	HTTPS	TCP

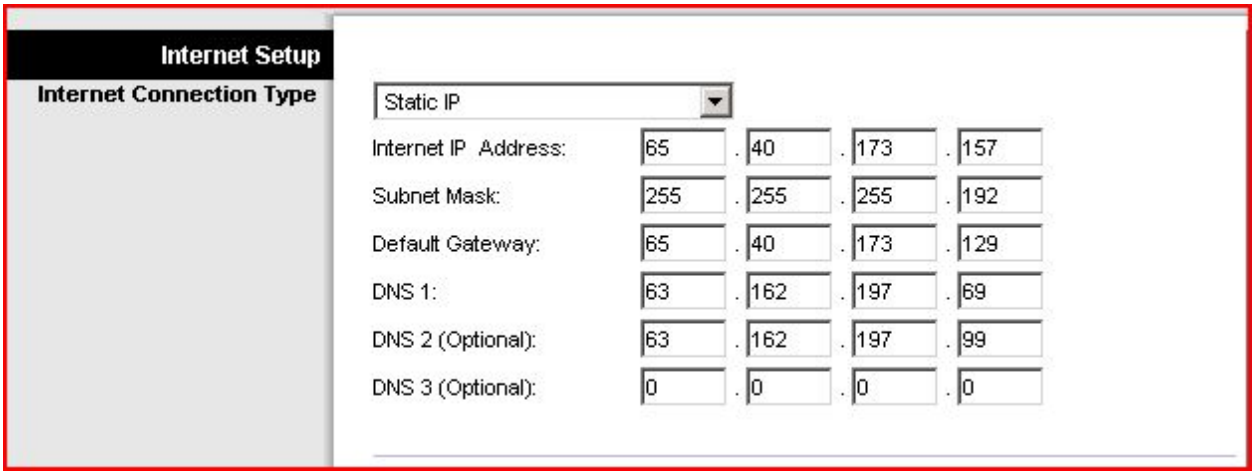
Note: Source IANA

Chart created by Matt Moberg

The next section will discuss ways to secure these commonly used ports. Both the firewall and the applications themselves will be used in this security effort. Figures 1 and 2 show screen shots of a home office Linksys wireless router currently in a production environment. This home office router is using forwarding to pass traffic that comes to its public IP address requesting servers or applications behind the firewall.

Figure 1

Static IP address for home office



Note: Source Humanic Resource Management home office router

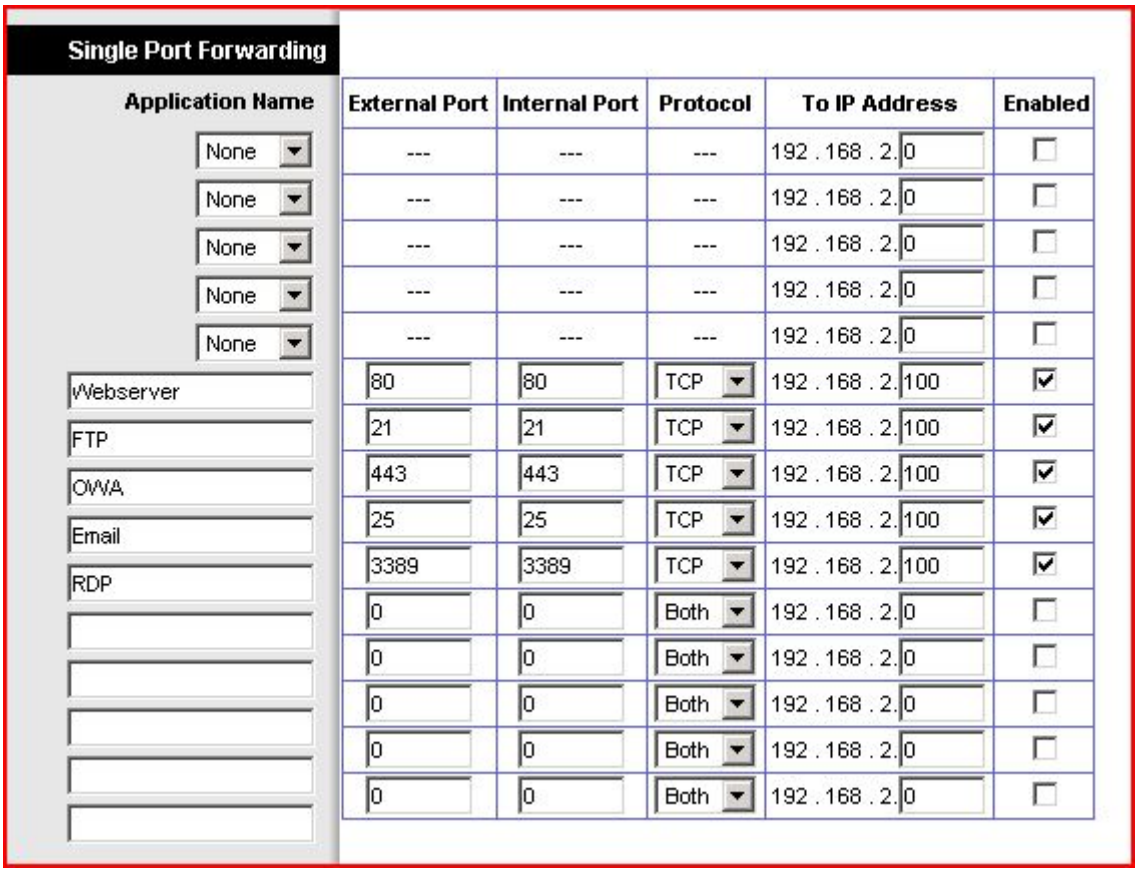
Picture taken by Matt Moberg

In this LAN, the data provider's modem is placed into bridge mode. This means that all incoming traffic simply goes through the appliance and directly to this Linksys wireless router. This home office has a static IP address. As you can see in Figure 1, the data provider's address, subnet mask, gateway, and DNS servers are all entered manually. Remember from the section on securing the home office that the use of dynamic addresses was a possible increase in security because a hacker wouldn't have a fixed target. While this may be true, the lease for dynamically assigned addresses if often as much as 12 hours. Most home users carry the same dynamic address for months at a time. Now that we have Internet access, let us look at securing it. Figure 2 shows how the router firewall is using forwarding for particular services behind the firewall. The home office in this example has an Exchange Server, FTP server, Web server, the need for

SMTP, Remote Desktop (RDP), and Outlook Web Access (OWA) for Exchange and Secure Socket Layer (SSL) connections.

Figure 2

Router forwarding table



Note: Source Humanic Resource Management home office router

Picture taken by Matt Moberg

This table is very straight forward. Notice how the table has a field for the name of the service, the port range needed, protocol, and the destination private IP address that hosts the server/application. The final field is a check box to enable/disable the forwarding.

Securing Application and Port Usage

Now that we have our Internet connection and port forwarding to several different resources, we need to look at ways to secure this home office deployment even further. The home office used in Figures 1 and 2 will be the basis for further security considerations. The following servers/applications are being used in this home office:

1. FTP server
2. Exchange server
3. Web server
4. Remote Desktop
5. Outlook Web Access

FTP server

One of the most common methods in uploading and downloading data over the Internet is File Transfer Protocol (FTP). FTP exclusively runs over TCP and by default uses port 21. The original variant of FTP is inherently unsecure. The data is sent in clear text with no encryption. This means that passwords, data, network configurations, and other such traffic can be captured by an eavesdropper or packet sniffer.

There are several ways to secure your FTP traffic. One method would be to use a VPN connection between the client machine and the FTP server in the home office. Once the VPN connection is established, the FTP client can use the private IP address on the FTP server to connect. Once the connection has been established, all traffic will be passing between two private networks and the VPN tunnel. Figure 3 shows the connection:

Figure 3

VPN connection

Note: Image sources Microsoft Clip Art

Figure created by Matt Moberg

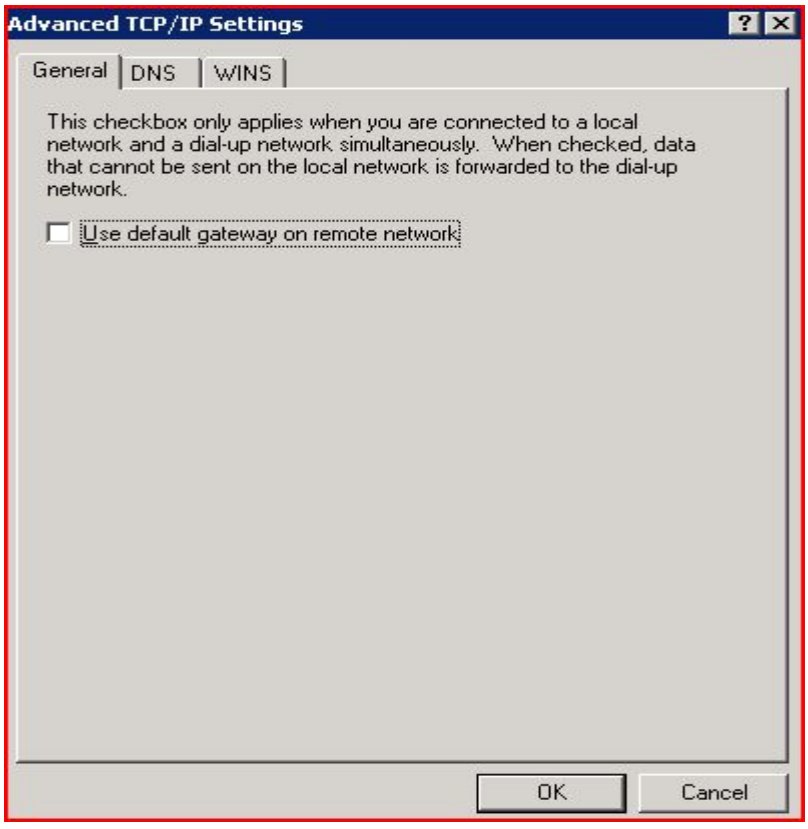
In this example, we can imagine the client machine grabbing a private address from a hotel room or some public Wi-Fi location. The FTP server is located back at the home office. Once the credentialing is completed on the FTP server, the user on the client machine can run the VPN client software to establish a connection over the Internet. Once connected, the FTP client software can be run and the address for the FTP client would simply be the private address of the home office FTP server. Despite the fact that the client machine is on a 192.x.x.x network and the home office LAN is running on a 172.x.x.x network, the VPN connection brings both

networks together. In our example, once the VPN connection is established, the client machine could successfully ping the 172.x.x.x network.

One further method in securing this VPN connection is to force the client machine to use the downstream server's gateway for Internet access. Simply go into the Advanced Properties of your VPN client connection (On Windows appliances, this will be located in the Network Connections applet) and check the box "Use default gateway on remote network."

Figure 4

Advanced TCP/IP Settings



Note: Source of picture Humanic Inc

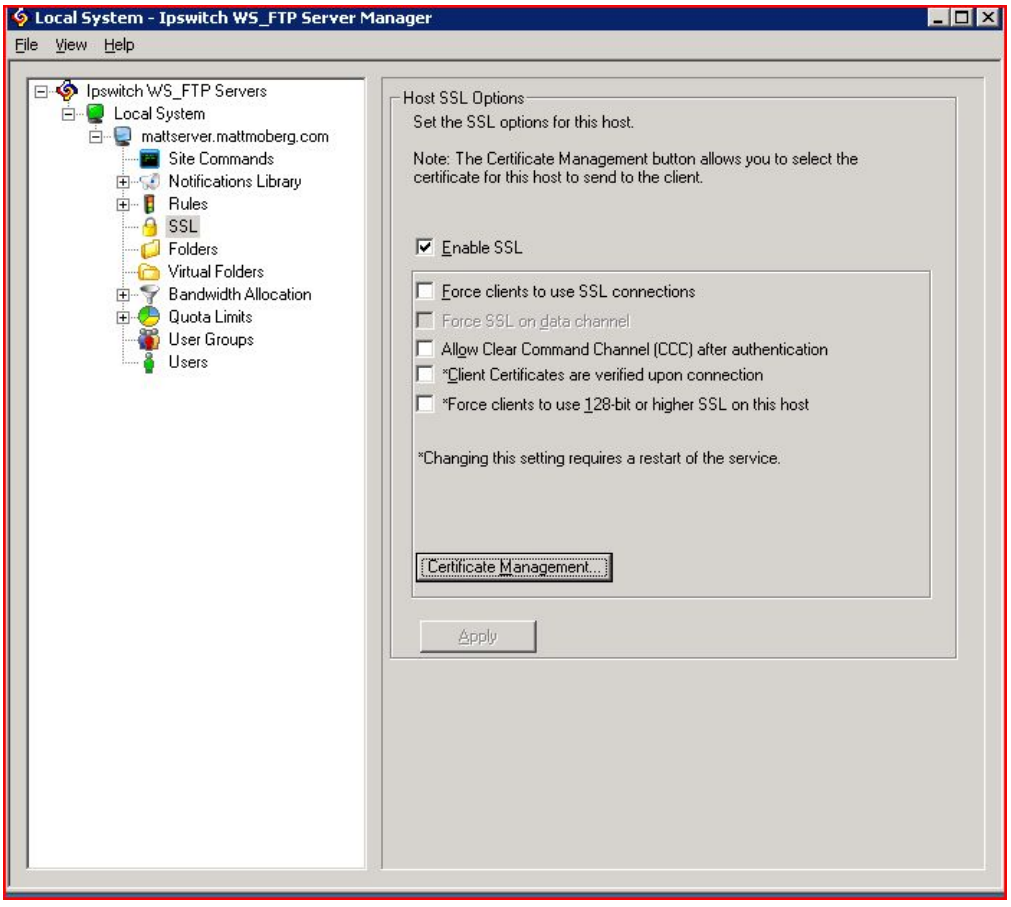
Picture created by Matt Moberg

Once this check box is selected, any Internet/browser activity on the client machine will come from the server on the VPN connection. This is especially useful if a client machine is on an unsecure public network.

More security can be found by assigning connection requirements on the FTP server itself. Figure 5 shows an FTP server and its SSL settings:

Figure 5

FTP server SSL options



Note: Source Humanic FTP server

Figure created by Matt Moberg

As Figure 5 shows, there are many options available to add security to the FTP server. The Certificate Management button opens an applet that will allow the creation, modification, and application of a certificate.

There are other common ways to secure FTP traffic. One could use SSH File Transfer Protocol (SFTP). This is a network protocol that allows the movement of data over a network connection and is usually used with SSH protocol (Port 22 TCP). Another method of secure data transfer could be accomplished by using a FTP over SSL (FTPS) server. The security with this method is accomplished by the servers generating public key certificates. Regardless of the method in which one would secure an FTP server, is it vital that the need be addressed so that the home office can remain secure.

Exchange Server

Microsoft Exchange server is one of the most popular email servers in use today. It has a rich list of resources and can perform many other tasks besides email exchanges. Securing your email server is a priority. The actual deployment of the Exchange server and the administrative tasks you can apply to it go beyond the scope of this paper. A step by step security design can be found online at the intranetjournal.com website. (Taylor, 2005) It is an excellent resource for an Exchange administrator. The link to this resource can be found on the reference page. Other things to consider for the server in the home office would be location. Since this in fact is a home office, there will likely be other members of the family that will be near these production assets at some part of the day. The best solution security-wise for this server and any other LAN appliances would be to secure them in a small room or closet so that they can’t accidentally be

taken off line or broken. Cooling and power requirements are other considerations to take as a server can give off quite a bit of heat.

Another important consideration for the Exchange server and its secure use is to require a certificate for user access. The most common method is a Secure Sockets Layer (SSL) certificate. A SSL certificate enables traffic encryption, verifies the owner of the certificate, and also carries information specific to the certificate owner. The certificate uses a both a private and public key. The private key essentially deciphers what the public key encrypts. A 128 bit SSL certificate is recommended. These certificates can be purchased online from one of many providers. Each vendor will provide step by step instructions on how to generate the cert and apply it. Phone assistance is also very common.

Web Server

As with the Exchange server, a web server will benefit greatly with an SSL certificate. As with Exchange server, once the certificate is applied to the server, you must go to the application to configure and run the system using the SSL certificate. Configuring a home office web server to use SSL is beyond the scope of this paper, however, an excellent website with step by step instructions can be found online at the Petri IT Knowledgebase (Petri, 2008). The web address can be found in the references section.

Another way to secure your web server is to use security white papers from the vendor of the software. For example, one very popular web server is Microsoft Internet Information Server (IIS). The Microsoft website has excellent documentation and checklists on all the considerations one should make to secure the web server. These same resources are also available from other web server providers.

Remote Desktop

Remote Desktop Protocol (RDP) is a client that can allow a user to remotely connect to another computer running Microsoft terminal services. By default, this protocol will use port 3389 for this traffic. RDP is a convenient method to logon to a remote system and work on it as if you were physically there. RDP uses the RC4 encryption algorithm (128 bit) and supports TLS/SSL security. There are several considerations to make to secure your terminal server:

- Configure the permissions and rights for each user according to their needs
- Manually set the level of encryption that you want to employ
- Adjust the inactivity time for connections to the server
- Control the number of concurrent connections

For a Windows based server, setting up user groups is an efficient method for controlling the access and permission rights for different groups of users. Controlling the amount of activity on the server and disconnecting inactive client connections is also useful. Dropping unused connections allows other users access to the server. An inactive session could also be a client connected computer where the user has walked away and possibly not secured the computer from unauthorized access. By dropping the session, you remove this potential exposure. An administrator can also adjust the level of encryption that the service uses. An example could be a Windows based server. To configure the encryption level, logon with an account that has administrative rights. Now complete the following:

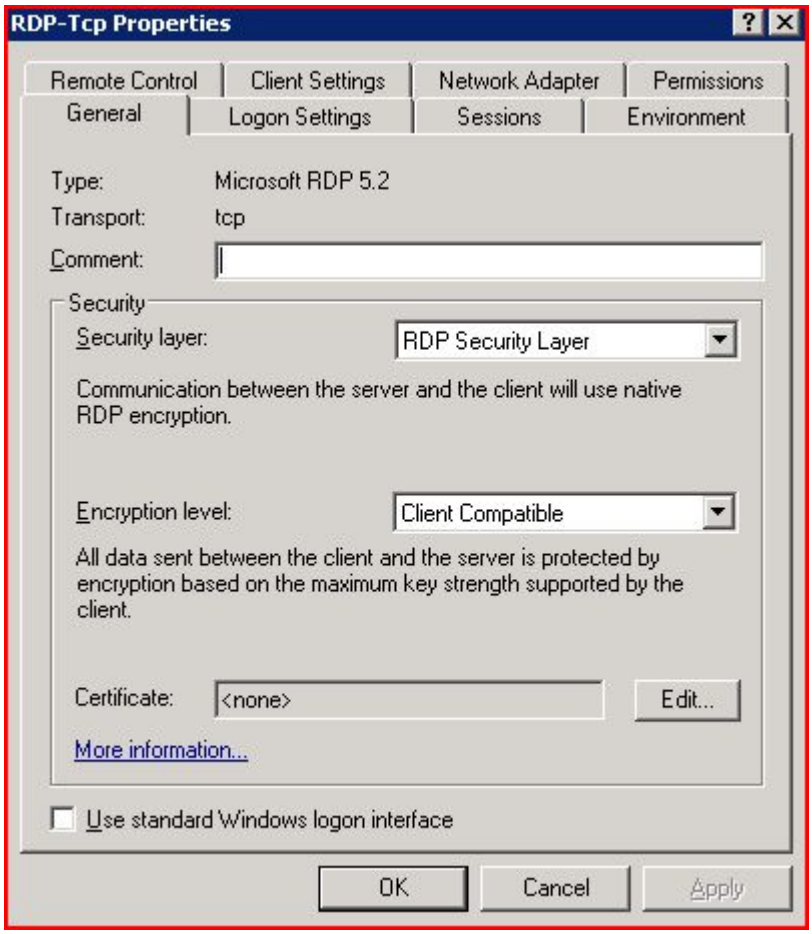
1. Go down to the Start button, then select Programs, then Administrative Tools
2. Now select Terminal Services Configuration
3. Select the General tab

4. Under Encryption Level, select the level you want to employ
5. Click OK when done

Figure 6 shows this applet:

Figure 6

Configuring Encryption Terminal Services



Note: Source Humanic Windows 2003 server

Figure created by Matt Moberg

This one applet allows for the configuration of the certificate, security layer, logon and client settings, and many other security related features.

Outlook Web Access

One of the excellent features of Exchange server is the ability to logon to the email server and use your email account using an Internet browser. Outlook Web Access (OWA) by default will pass traffic over port 443. The web interface will look somewhat different than a traditional Outlook client session on a local area network. Despite the differences, the appearance looks very similar and gives the remote user the full functionality of the Exchange server.

The secure use of OWA is mostly covered by the security deployed on the server itself. Other considerations would be that the remote user lock their computer if they walk away while connected via OWA. A remote user should never share their credentials. If the computer using OWA is running Outlook in Cached Mode, (A mode where the user's mailbox resides on the server AND the client computer) locking and physically securing the computer is vital.

LAN Considerations

The home office clearly is not designed like a typical office. Even if a home user sets aside one room for the office, it will likely not have available the many things a traditional office will contain. For example, a traditional office will have:

- A server room
- Telephone and data demarcation points
- Wired local area network
- Lockable offices and conference rooms

Securing your home office hardware is an important consideration. It is likely that the home office will not have a server room that is lockable. If this is the case, the home user will have to determine the best location for each asset. Clearly, the workstation locations would be dictated by desk availability and how the room is situated. The location of the Telco provided data service is often static and the demarc is located where the installers have their data cable located. If this is not convenient for the desired home office, the Telco will usually be willing to move it to another location. (May include a cost)

The location of the Telco provided modem is important if a wireless router is going to be deployed. The data cable will connect into the Telco provided modem. This same modem will have a LAN port to pass the data traffic to a LAN appliance- or in this case the wireless router. Most residential wireless routers will also incorporate a small 4 port hub function. Once the Telco traffic passes to the wireless router, it can then be broadcasted over the wireless network or can be accessed by connecting a computer via a patch cord to one of the hub ports. According to the International Journal of Computer Science and Network Security (IJCSNS) the location of the wireless router should have several considerations (Tung, Ahmad, Geok, 2006). First of all, the physical makeup of nearby objects such as walls or metal structures can affect the signal strength of the router. While the router should be deployed so that the wireless network users can have access, the wireless signature should also be such that it does not broadcast too far from the home itself. Physically, it should also be located so that it is safe from family members or pets. The wireless router should also be given a meaningful name and any factory defaults changed. The factory default removal changes known settings on the device and the meaningful name is useful for identification and troubleshooting.

Further security considerations for LAN/WAN deployments are currently being worked on by the IEEE. The emergence of high speed LAN/WAN networks and additional security requirements has solidified the demand for security at the link layer. (Singer, 2008) The new set of security protocols which will partially or fully describe how a LAN/WAN can be transparently secured is often referred to as MACsec. (Business Wire, 2008)

As census research has shown, the number of people working from home is increasing dramatically. This paper only touched higher levels on security considerations for the home office. The Internet has thousands of excellent websites that offer free step by step instructions, definitions, how to guides, and white paper knowledge bases. The excellent technology that a home office has access to means a home user can be enormously productive. However, attackers are more sophisticated than ever, so, security for the home office is a must.

References

Bradley, Mitchell (2008). *DSL vs. Cable Modem Comparison – Security*. Is one really any safer than the other? Retrieved from http:// compnetworking.about.com/od/dslvscablemodem/l/aa021101a.htm

Business Wire (2008). SafeNet Announces World's First Complete MACsec Embedded Security Solutions For LAN and Metro Ethernet Communications. Retrieved from http://findarticles.com/p/articles/mi_m0EIN/is_2008_June_9/ai_n25490212

*De Rango, Floriano, Lentini, Dionigi, Marano, Salvatore (2006). Static and Dynamic HandShake.Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i. *EURASIP Journal on Wireless Communications and Networking, Volume 2006, Article ID 47453, 19 pages Doi:10.1155/WCN/2006/47453.*

Internet Assigned Numbers Authority. (2008).

Penn, Mark (2007). *The way we live now: Home-Office Politics*. Retrieved from www.nytimes.com/2007/11/04/magazine/04wwln-lede-t.html?_r=1&oref=slogin

Petri, Daniel. (2008). *On IIS 6.0, How Do I Configure My Website to use SSL?*. Retrieved October 22, 2008 from http://www.petri.co.il/configure_ssl_on_your_website_with_iis.htm

*Singer, Steve (2008). MACsec: Protecting Your Network From the Ground Up.

Linley Tech Seminar: Embedded Network Security Design. Journal presentations retrieved from http://www.linleygroup.com/Seminars/security_program.html.

Stallings, William, & Brown, Lawrie (2008). Symmetric Encryption & Message Confidentiality. *Computer Security – Principles and Practice, pg. 610*

Taylor, L., (2006). Getting Started on Exchange Server Security. *Its Easy to Secure Windows 2000 Server Part 6.* Retrieved October 22, 2008 from http://www.intranetjournal.com/articles/200508/ij_08_17_05a.html

*Tung, Sia, Nadia Ahmad, Nurul, Kim Geok, Tan (2006). Wireless LAN Security: Securing Your Access Point. *International Journal of Computer Science and Network Security, Volume Six, No. 5B*

Whittenhauer, Kay (2008). *Number of Work-at-Home Employees to Continue Increasing in 2009.* Retrieved from http://www.associatedcontent.com/article/801555/number_of_workathome_employees_to_continue.html.