Remote Access

Section 5

“Connecting The Dots”

Introduction

GENERAL

Remote access plays a vital role in extending your network. What technology you provide and how you go about securing it can make or break stability. Cost is a big portion in the decision making process, but in reality it is *value* that should dictate who and how remote access is provided. Before you build a solution, you need to know what and why it is being built. Think of remote access as opening holes in your network security. Each and every connection outside of your network provides a hole in the fabric that protects it. The more holes you make, the more danger you expose your network too. The real problem is that you have to allow for these holes.

The benefits you get from outsourcesing your e-mail and web pages, is that they are outside your network shield and accessible to those who have to travel. No holes are needed to let your business traveler access either of these resources. It is planning like this that helps you to take control of your remote access without compromising security. Balancing access with strategic business alliances can have great benefit if done correctly. Here are some of the resources that require remote access:

- Administration (managing the network from home)
- File Sharing (getting files from work at home)
- Communication (Intranet web pages, e-mail, meetings)
- Presentations (demos, sales pitches, etc.)
- Remote Installations (installing software over the Internet)

The Internet acts as a conduit for your network to *connect the dots* (outside and inside the LAN boarders). You can think of it as a virtual network interface.

Looking In From The Outside

SECURITY ISSUES

To truly understand remote access and what it means for your network you must first separate yourself from the network. You should take into consideration what is normally put in place for users to access their remote resources and what hackers are looking for when the are trying to break into your network. Downloading hacking tools and testing your security exposes many of the things you don't think of when looking form the inside out. This is not a one time deal -- you must constantly keep up with the tools out there and how they are used.

Most hackers look for simple things that make your network vulnerable. Some obvious points of interest are:

- RAS[101] servers
- Terminal Services
- E-Mail
- Web Services

TEST STATION

The network administrator should have a testing station (using a modem or any other access device *other then the office gateway system*) to test the access level of the company Internet gateway. Figure 5-1 represents a topological view of how both the test station and the network access internet resources. In setting up an internal testing station, you are able to test your network external access and also use this station for verifying each remote laptop or workstation you deploy outside the network.

This test environment should not have access to internal network connection (Ethernet) so that the connection properties are solely made by the modem access and not confused by internal access settings. Making sure that the test station is not connected to the internal network via Ethernet also limits any damages that could result from someone hacking into the network via the test environment.

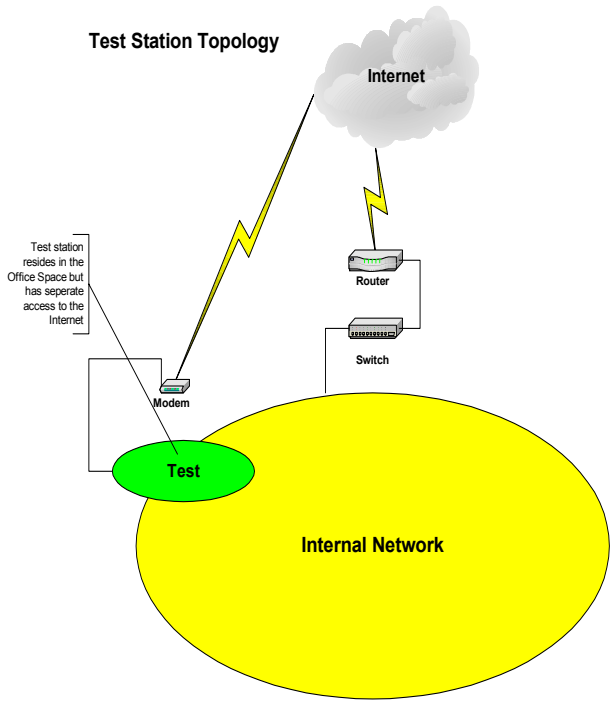
You should remember that the *testing phone line* must be a POTS[102] line and can not be part of the PBX. This line should not be configured for long distance nor for any special features (such as call waiting, call forwarding or messaging services).

You should be careful not to let many people know what the test phone number is. Since this phone line can be a potential security risk, only those that need to know of its' configuration need be aware that it exists.

101.RAS - Remote Access Servers that are configured to allow members of a network the ability to connect to internal resources as if they were inside the security barrier. Usually associated with modem access, these servers let people log into the network and access storage, printers, and other internal resources using their remote computers.

102.POTS is a term sometimes used in discussion of new telephone technologies in which the question of whether and how existing voice transmission for ordinary phone communication can be accommodated.

FIGURE 5 - 1. Test Station Connectivity Settings



TESTING PLAN

Once the test station is in place, you need to set up a test plan. This plan should explain as simply and directly what it is you are looking for and what you see as the goal your trying to achieve. This may sound simple and obvious but there are too many times that a test environment is created without fully defining what it is your trying to test for and what you want to achieve.

Your test plan must:

- Define an objective
  - Successes
  - Failures
  - Show Stoppers
- Establish a consistent approach
  - Beginning and End
  - Standard Routine
  - Mile Stones

You should research what others have done and how they went about doing it. There is a lot of information on the Internet and a lot of people have done what you are trying to accomplish -- use their experience to build your testing process.

Building forms that everyone can understand, design a methodology for how you go about proving your solutions:

TABLE 1. Example of a Test Plan

Step #	Description	Expectation	Result
1	Test Remote Connectivity	Dial Tone	Hear Modem Dial Tone
2	“““	Dialing Notes	Hear Dialing Notes
3	“““	Modem Noise	Hear Modem Noise
4	“““	Remote Response	Hear Remote Response
5	“““	Connection Icon	See Connection Icon
6	“““	Launch Internet Browser	See Internet webpage

Building these simple forms allows you the ability to test a process many times over with the same steps. In doing so you are able to assure that each and every test follows the same scrutiny that the previous test went through. Keeping the results of these tests also help you to use this information in assessing hardware and software compatibility as well as functionality.

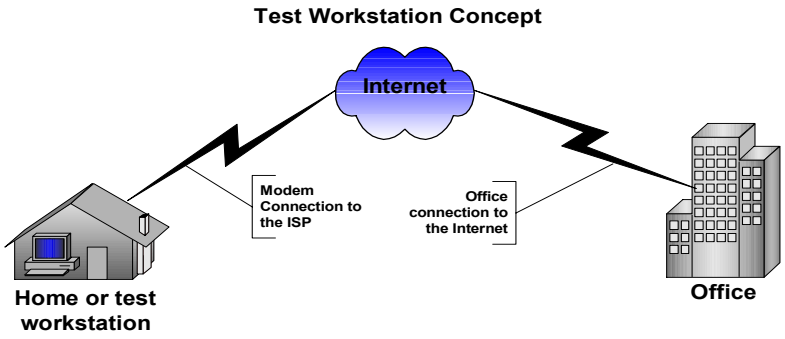
TESTING ISP

Your test station connection to the internet will most likely be a standard modem account with an ISP[103] (maybe DSL). Your test workstation ISP should be any other provider then your office ISP so that there are no conflicting configurations (different ISPs offer their own TCP/IP configuration settings). Always test the ISP connectivity thoroughly. Your goal is to mimic the topology of an outside connection. This connection should resemble a home or travelers environment.

Figure 5-2 represents the topology your trying to achieve. Even though your workstation is actually located inside your office it should have a network topology that duplicates an outside connection. As stated earlier there can be no connection between the Office network topology and the test workstation -- all connectivity should be enacted through the test workstation’s independent internet connection.

103.Internet Service Provider

FIGURE 5 - 2. Test Environment Topology



Once you have configured a testing environment you are ready to work through the issues of remote access. This process should be performed one step at a time so that you can confirm that each process is working the way you would like.

Since we outsource our e-mail and web services for our network those aspects of remote connectivity have been taken care of. In larger companies these would be important considerations that might require special hardware and security configurations (we will look at this more when we discuss a corporate network environment).

When you connect to your office network from home you do so over a public network (the Internet). This means that anyone wishing to listen in to your conversation can do so. If your information is confidential that can be a problem. Protecting your office network not only requires plugging up all the holes on the firewall (or router) but also ensuring that each connection made to the office network is encrypted so that information remains secure.

Remote Security

PORT SCANNERS & SECURITY CHECKERS

There are a host of Shareware[104] or Freeware[105] utilities you can download that will help you to test your network security. Here is a few that can be found on the Internet:

- **AA Tools** - shareware - **http://www.glocksoft.com** (scans a network for vulnerable computers and ports)

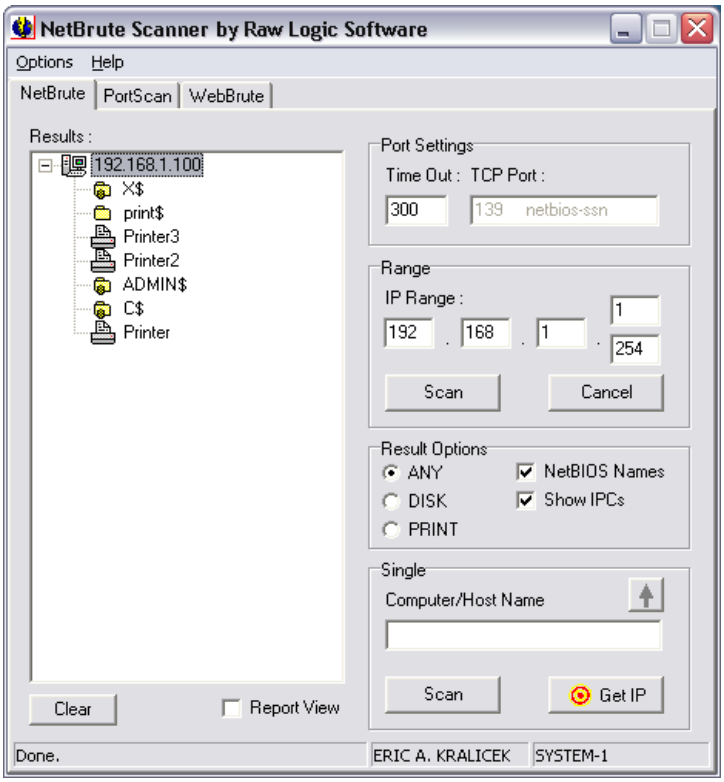
104.Shareware is software that is distributed free on a trial basis with the understanding that the user may need or want to pay for it later. Some software developers offer a shareware version of their program with a built-in expiration date (after 30 days, the user can no longer get access to the program).

105.Freeware is programming that is offered at no cost. However, it is copyrighted so that you can't incorporate its programming into anything you may be developing. The least restrictive “no-cost” programs are uncopyrighted programs that are in the public domain.

- **AntiSniff** - freeware - **http://www.10pht.com/antisniff** (helps you to detect someone sniffing your network ports)
- **Internet ports** - freeware - **brian-01641@intergov.org** (list of Internet ports and their associated application)
- **NetView** and **NetBrute** - freeware - **http://www.rawlogic.com/products.html** (Searches for shared resources and detects open ports and password security)
- **Port Blocker** - freeware - **brian-01641@intergov.org** (blocks open ports on your computer)
- **SATAN** - freeware - **brian-01641@intergov.org** (Security Administrator Tool for Analyzing Networks)
- **TJ Ping** - freeware - **http://www.topjimmy.net/tjs** (ping, tracerout and lookup utility)
- **Ultra Scan** - freeware **http://www.point1.com/UltraScan** (scans ports for open port vulnerabilities on computers)

As you can see from the list of scanning utilities, you do not have to be a computer professional to obtain tools used for assessing network security. Most “hackers” out there use these tools to break into networks and do their damage. You should use these utilities to see what hackers can see and make yourself more prepared to protect yourself from their attack.

FIGURE 5 - 3. NetBrute[106] Port Scanner



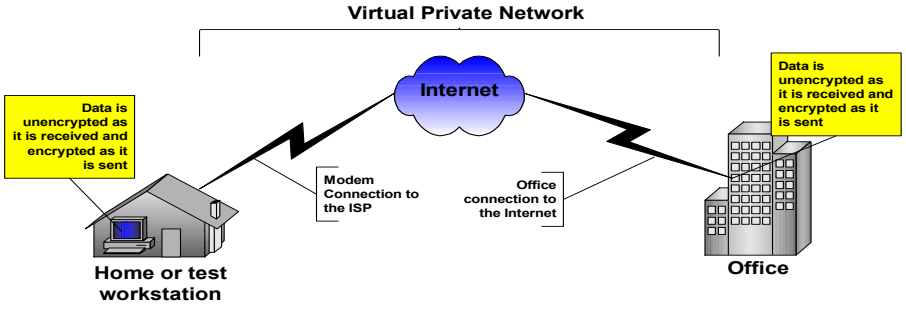
As you can see in Figure 5-3, these utilities expose file shares, available printers, and any other resource that can be exploited by someone who wants to exploit them. Its important for any network administrator to be aware of these vulnerabilities and protect against them.

When you see holes in your security you should evaluate their purpose and apply basic security procedures to protect them from potential attack. By this I refer to passwording file shares and blocking ports that are not necessary for business purposes. There will always be holes in your network -- there has to be in order to share Internet resources. Your job is to be aware of those holes and limit their potential for disaster.

VIRTUAL PRIVATE NETWORK

Virtual Private Networks (VPN[107]) are used to extend the security blanket outside of the physical boundaries of your office network.

FIGURE 5 - 4. VPN



Using a protocol tunneling technology (i.e.; L2TP[108]) you are able to create a secure virtual network connection between your office and a remote computer. The remote computer has access to the office network resources just as any other computer in the office network. The only limitation is speed. With the lower cost of DSL and cable modems for the home, general access to network resources over broadband technologies could look similar in performance to that of workstations on site.

106.Copyright 2002 by Raw Logic Software. Raw Logic is a trademark of Raw Logic Software.

107.A VPN (virtual private network) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.

108.Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet. L2TP merges the best features of two other tunneling protocols: PPTP from Microsoft and L2F from Cisco Systems. The two main components that make up L2TP are the L2TP Access Concentrator (LAC), which is the device that physically terminates a call and the L2TP Network Server (LNS), which is the device that terminates and possibly authenticates the PPP stream.

Most current operating systems incorporate a version of VPN. These are generally bundled with the operating system and don't cost anything to use. Other VPN solutions can be purchased on a host by host basis and provide greater security at a higher cost. The main difference is the level of security each has to offer.

If you are running a small business and most of your work is not confidential, an OS based solution should be more then enough. The average hacker would find it difficult to break the encryption and you would not have to build any elaborate security net in order to support encryption technologies. If your business is based on ground breaking research you may wish to incorporate higher levels of encryption that utilize SecureID[109] technologies.

FIGURE 5 - 5. Zezan Secure ID

The concept uses synchronized password information that is constantly changing. This greatly reduces the chance that someone could copy or duplicate your password. The password is displayed on an electronic device carried by the person who has been granted remote access. The number displayed is in conjunction with an account (synchronized with a server running special software) to verify the validity of the password. You type in your access account name and the number displayed on the Secure ID device and gain entry into your office network resources. Since the number is constantly changing, so is your password. This technique is used for highly confidential communications.

Other remote security options are:

- Logon-callback which limits accounts to specific phone numbers (you call in with your modem and the remote access server hangs up and calls you back at your designated home phone number).
- Designated IP addresses (setting up an access list based on static Host IP Addresses).
- Certificate Servers (sharing tokens between authorized hosts and the office servers).

109.Zezan Secure ID is a company which provides secure communication across the Internet. Please see: http://www.zezan.com/security.html for more on their services.Secure ID is a copyright of Zezan

Remote Administration

VIRTUAL NETWORKING

Being able to administer network resources remotely is both useful inside and outside your physical network boundary. Most current server operating systems offer remote management (Microsoft uses Terminal Server Administration). There are also free remote administration utilities such as VNC[110] (Virtual Network Computing). In each case the concept is quite simple - a remote computer's desktop is made accessible through a secure connection between a remote system and the office server.

FIGURE 5 - 6. Microsoft's Terminal Services Access Window

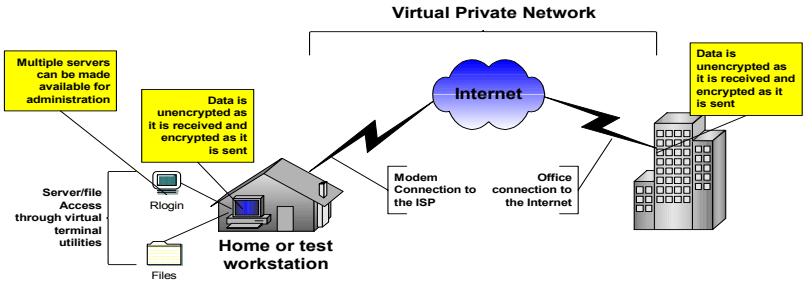
Using remote administration allows you to do things remotely with your server that you would normally have to do on the server's keyboard -- making network services more mobile. Resetting print queues or passwords, adding resources, even rebooting, everything you can do on the server can be performed remotely. You still have to log onto the server in the same way you would normally -- through either an Internet browser (VNC) or special client software (Terminal Services Client). This allows you to reduce the size of your server space (since you no longer have to have a monitor or keyboard attached) and gives your office/home workstation more functionality as a conduit to server applications. It should be noted that Apple also offers X Server Remote administration.

You should be careful to limit remote administration as best you can -- through a list of authorized static IP addresses outside the office as well as inside. The majority of security breaches are made inside the office and by those you believe you can trust. Access to remote administration should mirror the level of access you give to your server room -- only those who can enter the room should have remote access. You must also configure remote administration with your router and firewall so that any and all communica-

110.The VNC system is available for general use under the conditions of the GNU General Public Licence. Go to http://www.uk.research.att.com/vnc/gpl.html for more information.

tion can be monitored and recorded in case of a break in. Remote administration also offers the advantage of applying patches and hotfixes from home when no one is in the office. Most service packs and hotfixes require rebooting the server or disrupting services to the LAN, being able to run these updates remotely allows you the benefit of not having to be on site during non-working hours to perform many of those duties. Prior to remote administration utilities, many network administrators worked late through the night and over the weekends in the office to get their job done. Now this can be done in your home without having to waist travel time or even having to get dressed.

FIGURE 5 - 7. Virtual Network Computing



Virtual Network Computer Ports:

- Microsoft and Citrix Terminal ports - 1604 (UDP 1494)
- VNC - 5800, 5801, 5900, 5901

Which ever administrative virtual access technology you deploy for your office network, you should read all of the information from the vendor as well as from RFCs[111] that specify any technology parameters.

SSL

Secure Sockets Layer[112] (or port 443) is a technology that allows encrypted access between a remote computer and a server's web pages. Often used in on-line banking, purchases or business transactions over the Internet. SSL uses public and private keys to ensure that both parties are encrypted from point to point so that data can not be easily intercepted. One great use for SSL protocol is in allowing access to Intranet folders and files for people working remotely.

111.A Request for Comments (RFC) is a formal document from the Internet Engineering Task Force (IETF) that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs that supersede or elaborate on all or parts of previous RFCs.

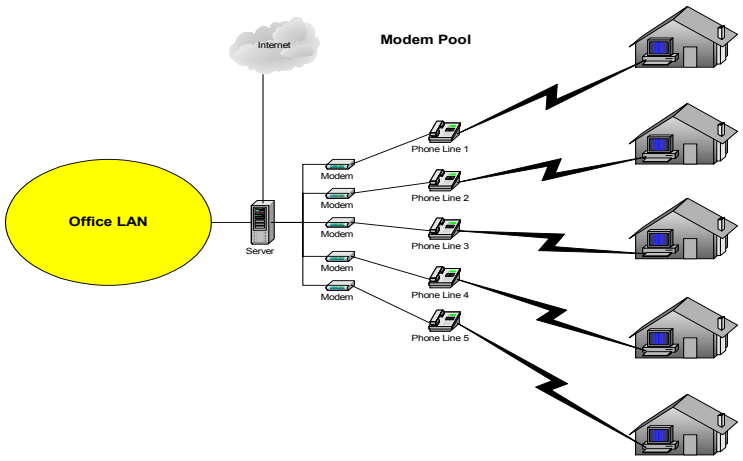
112.The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.

REMOTE ACCESS SERVICES

A remote access server manages connections between the office network and remote workstations and/or laptops. There are many types of RAS servers (modem pools, VPN, etc.), but they all do the same basic thing -- validate users with accounts and provide access to internal resources. Some companies mix modem pools with DSL gateways but the reality is that modem pools have become less and less popular as broadband becomes cheaper. Still, it is a good thing to go over the concept of a modem pool just for good measure.

Modem Pool RAS

FIGURE 5 - 8. Modem Pool Topology



Usually in a modem pool, one or more servers has a special serial port device that extends ports so that many modems to be connected. Home computers dial in to specified phone lines and gain access through the RAS server. Once part of the RAS server pool each computer has the same access as local computers and must go to the Internet using the same company gateway.

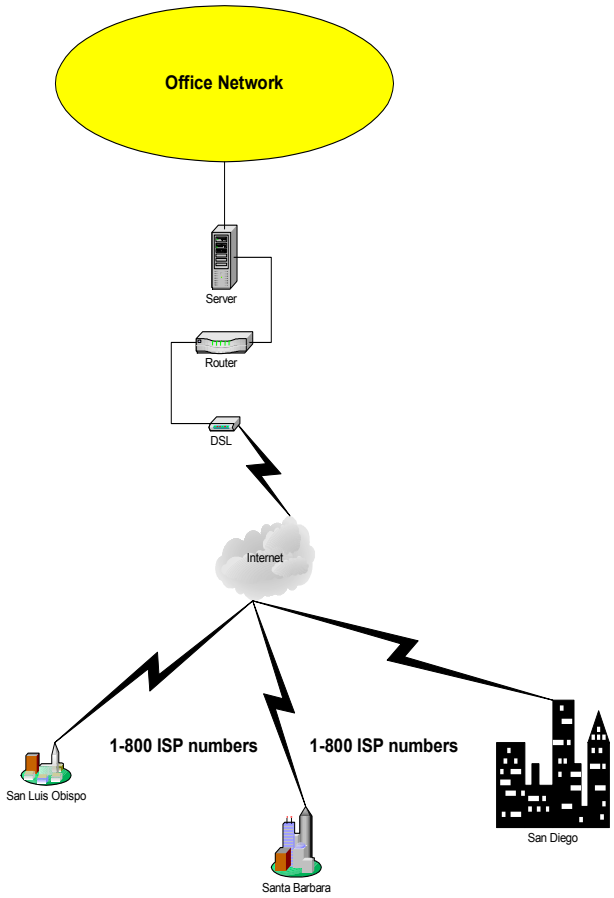
Cost alone should make you think twice about supporting modem pools in today's world. The second major drawback is security. Modem pools generally allow for remote users to avoid the firewall. In other words, you open your network up to a back door attack which could be extremely difficult to defend against. The cost of five extra POTS lines far exceeds the cost of one DSL line. The DSL line can be better protected against because you deal with a single gateway device that can be monitored more easily.

To get a handle on security most companies use RADIUS[113] to manage their remote accounts.

Your server can use the companies gateway (DSL, Cable Modem or T1) as a viable RAS server. While you don't use multiple phone lines on the local end you can use ISP dial-up connections on the remote end. This is how it works...

You need two accounts (your local network account and an ISP dial-in account) to make this work. Your local account is given a RAS access. You dial in from your remote location using the ISP's 1-800 number which gets you to the Internet. Next you run your VPN connection (which links your Internet connection to the company network gateway).

FIGURE 5 - 9. RAS Via Company Gateway



Once you've established your VPN connection with the company's network you are able to do everything as you would in the office. This method proves to be a much better solution then the modem pool and has the ability to grow with the technology at hand.

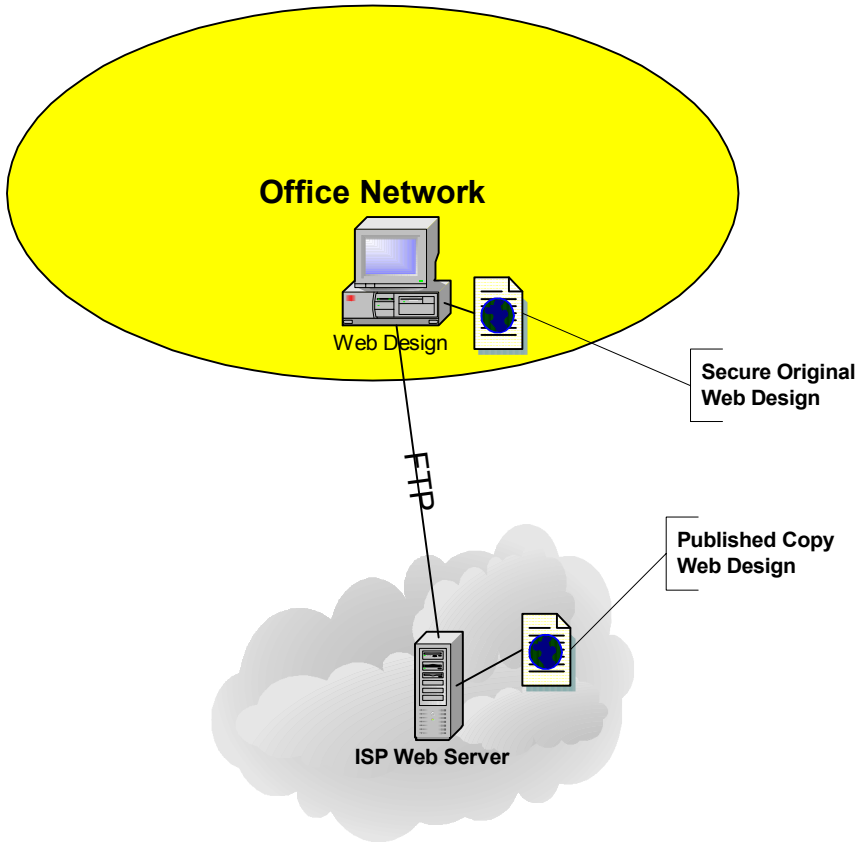
113.Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point.

Plus more then one person can share the ISP account making it more resourceful all the way around.

OUTSOURCING WEB SERVICES

Having your ISP publish your web pages does not mean you have to have them design your web pages. Many companies design their web pages on a secure computer located safely inside their firewall. Once they have a good design, they then push the web design to the ISP hosting site via FTP. This works to both parties advantage. If the web site (on the Internet server) is hacked you can reload a copy of the clean web design and get it quickly back up and running.

FIGURE 5 - 10. Publishing a web page



Having the secure original inside the firewall makes it easier to backup files and restore files without disruption to the actual public site. It also acts to hide the original location of the web design and further protect the web page from possible damage that can not be repaired.

OUTSOURCING E-MAIL

There will come a time when you should have internal E-mail services, but for now the price is too high. Having a few account (less then 100), makes outsourcing a must have. The savings just for security alone is worth it. When you open your LAN to sending and

receiving e-mail you open your network to one of the most common modes of virus infection. There are several ports that are opened for each of the flavors of e-mail protocol:

- SMTP - ports 25, 366
- POP - ports 109, 110, 995
- IMAP - ports 143, 220, 993

If your E-mail is outsourced these ports need never be opened. Further, you don't have to configure or install any FAT clients[114]. This makes your workstation software installation simpler and reduces the potential for application problems. It also reduces the bells and whistles that can be added to your E-mail browser. On the other hand wireless technologies are opening up new avenues for collaboration through PCS and Cellular features that provide E-mail and web connectivity.

SUMMARY

Remote access can be a complicated topic. With all of the possibilities for extending your companies assets you also extend the liability and potential for damage to be caused by outsiders. While you can't lock down your network completely, you can limit the possibilities for danger. Using the same tools that hackers do, you can open your eyes to your networks vulnerabilities. Knowing is everything.

Establishing a sound testing process with a complete testing environment will help you to better understand your network from the outside. Taking time to build resources (testing and then implementing) will put you in a better situation to protect your network. Building and documenting the testing process will make it simpler for you to refine each process and continue to improve your approach to adding new technologies to the mix.

Limiting the holes you make in your network will make it easier for you to troubleshoot problems as they occur. Testing those holes will help you to see what the hacker sees and maybe stay one step ahead.

Using remote administration technologies will improve you life and extend your reach -- both inside the LAN and from the outside. Always think security when you implement remotely and limit server access across the board.

Avoid modem pools whenever possible and force external access through one main administrative source so that you can control access. Use VPN whenever you can and always use some type of encryption method when communicating across a public network.

114.FAT Client - an enhanced e-mail browser that provides additional functionality that is usually not possible through Internet browser E-mail clients.