Global Information Assurance Certification Paper

Securing the Enterprise from the dangers of remote access: Analysis of new options available for Personal Firewall management in comparison with other established and emerging remote access solutions

I. Introduction

Since the advent of the small/home office, traveling workforce, and the extension of the workday through remote computers and dial-up/high speed internet connections, it has been recognized that one of the most unprotected avenues of ingress into the corporate network are these "off-net" resources. <1 >
Over the past 2-3 years some solutions have been developed and employed to protect the corporate network as well as individual machines through VPN's and personal firewalls. Until recently there were very few ways to effectively manage and enforce firewall installation and other security policy enforcement prior to allowing connections to the corporate network. This, coupled with the increase in the need for remote connectivity, has drastically increased the exposure of the enterprise to this vector of attack.

In this paper I will further explore and document the problem as it exists today, evaluate the pro's and con's of some of the solutions that are offered today, and explore the future direction that these and other solutions might take.

II. The Problem

There has been a large increase in the number of remote workers - mobile, wireless and home workers, as well as Extranet connections to the corporate network. <2>

An increasingly favorite, and potentially much more successful, vector of attack for viruses, Trojans, and malicious code has become the home PC or other remote device used by today's professionals.<3> One much publicized intrusion that is likely to have started through this type of vector is the Microsoft attack that resulted in the theft of source code <4>. Surely this is not an isolated incident. The most common threat to the corporate computing environment from employee owned PC's used to be employees bringing in floppy diskettes from home with viruses on them in addition to the work they had been performing during off hours. Now employees are increasingly requiring remote access to corporate resources on the company network and this requirement brings with it a new level of threat.

The requirements for access by remote workers have often overshadowed or overpowered security concerns, leaving connections open and unprotected. Because of a lack of understanding or awareness throughout the enterprise, including the IT community, concerns about the security of these connections have not been addressed. Remote connections are often treated as trusted connections as long as a logon and password (or even a security token) is given and/or the connection originates from a known source or is protected by encryption. (i.e. a VPN) Typically connections made in this manner are completely trusted and allowed

full access to the internal network across all protocols so as not to hinder the productivity of the remote workers or make the system too hard to manage for the IT department <5>. However, these remote machines are often unprotected from malicious code, Trojans, viruses or other intrusion activity. Many remote machines will have virus protection installed because that has become fairly ubiquitous, but they may not have up-to-date virus definition files. Very few of them are likely to have any kind of personal firewall and if they do, many of the rules or alerts may be disabled because they cause inconvenient warnings, slow down the machine, or restrict activity.

Some protection is common and/or mandated by corporate IT departments but enforcement has been hard at best and often non-existent. It is a recognized "worst practices" policy to allow users to manage their own security related policies <6>. Many companies have policies that state that only approved laptops or other approved devices may connect to the network and that those machines must have virus protection or even personal firewall software installed. The problem with these policies is that they normally can't be effectively enforced. Once someone knows the dial-up number to the corporate network, possibly for a laptop used during travel, it is a simple thing to add those settings to a home computer or share the information with others. Unless these connections are closely controlled by allowing only certain hosts to connect (usually a management nightmare) an uncontrolled machine with a questionable history suddenly has access to your network. And the attacker probably never had to crack a password or guess an IP address. It is also common for remote workers to install unapproved applications or set up their personal Internet connection on company owned laptops or other remote machines. It is feasible to lock down the machines with policies that prevent this behavior, but this is often not done because it is difficult, reduces flexibility and increases the support costs related to remote users. Also, in many companies, laptops or other company owned remote hardware have historically been treated as much more "personal" than desktop office machines. Employees are often given great latitude in the use of this equipment.

Until recently there were very few tenable solutions for enforcement of security policies on remote/mobile computers connecting to corporate networks. Some ways in which remote connections to the network have been provisioned until now include: Citrix/Terminal Services, corporate portals, VPN's, dial-up services, and Smart Cards/Tokens. Of these connections only corporate portals and Terminal services could truly offer secure connections. These connections are only secure as long as (and because) direct file access from the remote machines are not allowed.

Existing security measures can offer some protection from the threats introduced by remote connections just as they offer protection from other threats. Best practices application of host and network based intrusion detection, firewall protection, and virus protection at many layers in the network can greatly minimize risk from remote workstation vectors of attack. "Defense-in-depth,"<7> however, dictates that risk be further minimized by eliminating or mitigating the risk presented by these external agents.

Taking into account the upswing in virus, Trojan, and malicious code activity on the Internet today <8>, there is a great security need for an enterprise-wide, scalable and manageable solution to protect the corporate network from remote, wireless, mobile, home, and extranet computers by enforcing local protection measures on those computers before they are allowed to connect to the enterprise network or in essence "proxying" that connection through other means. Some of the solutions that start to address this need and will help corporate IT managers close the security holes described above are just now maturing.

III. Some solutions available today

Managed outsourced solutions: There are at least two companies today that offer an outsourced solution for managing secure external connections (Managed Security Service Providers - MSSP). The solutions discussed here are AT&T <www.att.com>, Fiberlink <www.fiberlink.com>, and IPass <www.ipass.com>.

They all employ Cisco or Nortel VPN hardware and software coupled with firewall software such as BlackIce defender from ISS <www.iss.net>, or Zone Alarm. <www.zonelabs.com> One or more management servers exist on their networks in order to enforce defined policies. Authentication can be managed through RADIUS or LDAP calls to databases that exist either on the MSSP network or the corporate network. Before a connection can be made, the VPN client, coupled with the personal firewall software and standard policies, must be installed or the connection will not be accepted.

If a user wants to connect to the corporate network they either use a dial-up connections to POP's provided by the solution provider or connect through existing connections to a provider and then authenticate to the VPN concentrator of the solution provider. After the initial connection is made, the latest software and policy code is downloaded to the client, if it is needed, and then the connection back into the corporate network is established. Appropriate firewall policies should be in place on the connection to the solution provider to prevent any unauthenticated access. The data transferred between the corporate network and the solution provider will not normally be encrypted so a private line or additional VPN sessions between those sites is recommended.

At this point the client is treated as if they were a normal client on the network and would have all access that their normal credentials afford them. All data transferred will be encrypted in the VPN tunnel first set up during authentication through the MSSP. If the firewall software fails or is tampered with, the connection is dropped.

Typically all application software would be loaded locally on the remote machine but other solutions would be possible such as web delivered or terminal services applications.

As a managed solution, any changes to software and/or policies are made by the service provider at the request of the corporate IT staff. Due, at least in part, to this outsourced arrangement the degree of granularity for the implementation of policy standard is somewhat

limited.

Enterprise locally managed solutions: Zone Alarm <http://www.zonelabs.com/>, Sygate<http://www.sygate.com>, ISS <www.iss.net>, and others.

Generally these solutions employ some sort of policy server tied to a combination of VPN, RADIUS, and Directory servers. Similar to the managed solution above, client software is deployed and loaded on each remote machine which both enforces defined policies and provides for encrypted connections to the corporate network.

Operation and functionality are much the same as the managed solution above, software is loaded on the remote machine and the machine at the other end of the VPN tunnel is treated as if it were a machine directly connected to the corporate network. The only real differences are that the policy servers, RADIUS, Directory servers, and all other equipment are located at the corporate network and are managed by corporate IT resources.

Enhanced corporate portal solutions: Novell <www.novell.com>, Yahoo <www.yahoo.com>, Ericsson <www.ericsson.com>, and PeopleSoft <www.peoplesoft.com>, just to name a few offer portal solutions that provide much of the functionality needed by remote workers via a web interface and either Java applications or applications delivered through terminal server connections.

These applications typically use 128bit SSL encryption and require authentication before access is granted. The authentication can also employ additional technologies such as tokens or fingerprint scans. Applications are then either delivered in the same 128bit session through the browser and/or within an encrypted terminal server session.

Data is typically kept on the corporate network but complimentary solutions that allow for data synchronization might be added to this solution.

Required software on the client PC would be a modern web browser and possibly a current terminal services client software package along with regular dial-up or broadband software for a connection to the internet.

This solution makes no attempt to secure remote machines but instead offers up corporate applications and data to authenticated users without allowing them direct access to those resources.

All or portions of this solution could be outsourced as well. Yahoo offers quite a complete package as part of an offering that can include consulting, software development, and even some hosted/managed arrangements.

Citrix/Terminal Server solutions Like the portal solutions above, this solution effectively

proxy's access to the corporate network with the terminal server. The remote client never has a real connection to the corporate network, but only directs the terminal server to act on its behalf.

All necessary software is loaded on and maintained on the terminal server and the only software needed on the remote computer is a terminal server client. It is also possible to offer up the terminal services through a web browser interface so that only a modern web browser with the necessary plug-ins is needed on the remote machine. The client must have a method of connecting either to the Internet and then the terminal server or via dial-up to the terminal server or terminal server network directly.

IV. **Pro's and Con's of solutions**

Outsourced Solutions:

Pro's Usability is a plus with these solutions because they offer what most outsourced solutions offer, namely fairly high levels of expertise at less than premium price as well as a solution that transfers a lot of the responsibility to the service provider. But there are other extra's offered with some of them. AT&T, for instance, offers a bundled dial-up internet connection with each subscription. Fiberlink has the added benefit of an auto-dialer that can dial POP's on 3 major carrier networks (AT&T, WorldCom, Qwest) in case of a local outage. This is especially beneficial for the road warrior because s/he only needs to enter in the area code where they are currently located and a whole list of numbers they can use are displayed. If the first number doesn't respond or is busy, then the next number is used until the user is connected. Another offering that is just coming out from FiberLink is an authentication module for the Palm, CE, and RIM platforms that allows a user to connect to the corporate network using encryption and the same credentials that they use for VPN and dial-up connections. These features add to the usability of the solution.

Scalability is a definite plus with outsourced solutions. You get the redundancy of the large networks and service organizations even if you don't have a large user base requiring these services initially, but it can grow to accommodate very large numbers of users. These solutions also offer some protection from the fast changing landscape of technology because they are service based and so can change with technology and are not an investment that might be outdated shortly after it is implemented.

The level of protection offered by managed solutions is probably greater than that of a similar solution built in-house. The NOC of the solution provider has staff on hand 24 hours a day, 7 days a week who are trained in the product and who are constantly monitoring your network for anomalies, updating signatures, and monitoring the Internet for new threats. It would be pretty hard to offer the same level of service with in-house staffing.

Typically these solutions are not available for fewer than 150 active users, or they are cost prohibitive. FiberLink, for example, starts out its managed services for 150 users minimum. However the costs are quite reasonable for large numbers of users at only a little more than the cost of regular dial-up Internet access.

Con's Manageability ends up in the con's column for a couple of reasons. First, all applications must be maintained or delivered to the remote PC with the proper configuration and settings to work with corporate back-end systems. This may conflict with settings already on the PC (i.e. a home based PC) and limits "ad-hoc" access from systems in public places or on client networks since they will usually not allow installation of software by users. It also significantly extends the necessary reach/responsibility of the corporate helpdesk and other support personnel and could entail a significant cost. Secondly, there is no direct control over policy settings or software versions. This can make reacting to new threats or changing situations more difficult. On the other hand, the responsibility for the policies and correct configurations lies with people who understand them very well and work with them every day. However, putting control of your network resources into someone else's hands is always hard to do.

These solutions are probably not the right answer for offering secure access to partners or customers since they allow direct access to corporate networks and require a client and installed firewall software as well as application software on the remote PC. I would not be comfortable allowing access to potentially unknown individuals who are not under the control of the corporation.

Flexibility also ends up in the con column. In some ways this solution is ultimately flexible because any remote machine can run the same software and perform the same tasks as a LAN connected machine. However, since any new application software, updates, or policies must be installed on each local machine individually the speed of deployment, and therefore, the overall flexibility is reduced.

Locally Managed Solutions:

Pro's Scalability is a positive of a locally managed solution just as it is for a remotely managed solution. Although a local solution doesn't offer quite the scalability in infrastructure, it is still quite scalable in that the same back-end systems are used and those systems can be scaled upwards relatively easily to provide the same services to larger numbers of users.

Some other "pros" of this solution include the fact that capital investment in infrastructure results in a significant asset to the company that can add value. Also, as the high tech. industry continues to change and evolve you might be more insulated from the potential financial troubles of the service provider and you are not locked into a contract term that might not allow you to upgrade to the latest technology in a timely manner.

Con's One of the biggest con's in managing a secure remote access solution yourself is hiring qualified people to implement and manage it. This can be quite cost prohibitive if the number of clients served is small. However, if you already have qualified personnel on staff, the initial investment can be paid for quickly with the savings in monthly costs associated with a managed solution. Other manageability problems include the cost of managing and updating of the hardware and software systems on the local network as well as keeping support personnel trained and up to date on the necessary skills. Like the managed solution above, this solution also requires that all necessary applications be installed on the

remote machine and kept up to current standards of the enterprise. This is an additional support challenge and puts more demand on existing support systems.

Usability though positioned in the "pro" category for the outsourced solution, is in the "con" category when the solution is locally managed. One reason for this is the lack of an integrated phone dialer for remote users to use. Without the dialer and the national/global network support, all of the traditional usability problems of dial-up solutions are retained and the added complexity of the VPN and firewall software are added

As with the managed solution above, the flexibility of this solution is one of its "cons". While any applications used on the LAN can potentially be used remotely, the potential flexibility of this solution suffers because all applications and data on the remote machine must be managed and supported. Without any facility to remotely manage these workstations this solution ultimately lacks true flexibility.

With regard to the level of protection offered by this solution, installing and maintaining your own solution has some benefits. The entire solution is under the control of the company, keeping security responsibilities and data integrity responsibilities within the company. All passwords and authentication traffic are maintained on the local network, lessening the chance of compromise. However, since firewall policies and intrusion signatures must be maintained by internal employees whose responsibilities might span several areas, it is unlikely that the employee will be able to manage those policies and signatures as effectively as an outsourced company. Therefore, I think that this represents a "con" for this solution although not a strong detractor.

Corporate Portals:

Pro's Manageability is a strength of corporate portals. Since they are centrally managed and there are no client components other than a browser, the level of manageability is the best of any class of solution reviewed in this paper.

Corporate portals can often be quite flexible in that they are a configurable environment that each person can use in the way that works best for them. New content and applications can be added for the entire user base quite quickly by changing the server code in only one location. Because these are Internet based applications, they can be employed easily for the use of partners and customers as well, making their flexibility a real asset in some situations.

Portals can provide services for many individuals across the entire enterprise. They scale to large distributions very well since they are based on Internet technologies and require only a browser on the remote end making them a type of thin-client application.

The level of protection offered by pure corporate portals is very high. This is a completely different approach to secure remote access. External clients and all of the vulnerabilities that they represent never really enter the network. All clients are treated as untrusted. In this way, we don't really need to be concerned about the security posture of the remote client because we aren't allowing them access to the network.

Con's The usability of a corporate portal can vary greatly depending on the purpose and the implementation. They often rely on Java applets which are getting much

better but are not quite up to the level of standard programs in many respects. Since both the data and the application must be delivered to the client through a browser, slower speeds can be an issue depending on how much server side processing is employed. Also, since the applications are different from what users may be accustomed to, they may have trouble acclimating to them and additional training may be necessary.

The cost of portals can be quite high in comparison to other solutions especially for small numbers of employees. The development costs for individual applications are significant and probably not justifiable unless there is a relatively large user base that needs frequent remote access.

Citrix/Terminal Services

Pro's The terminal services solution is a very manageable solution because only a small client (or browser) is needed on the remote machine. Therefore, there are no issues with managing remote applications. The central applications on the terminal servers can also be more effectively patched and secured. Manageability is also enhanced because firewall policies can be greatly simplified since access is only needed from a relatively small number of terminal services hosts.

The usability of this solution is relatively high because the terminal services session functions as if the client was on the local network directly and it has the look and feel of a regular desktop computer. One of the largest usability downfalls of a truly secure terminal services solution is that local(in terms of the remote workstation) printing and file access is not available. For example, a salesperson at a remote client site could not print a document out and receive it at the client site. Another usability hurdle for some users is the confusion about which desktop they are viewing if a full terminal services session is provided.

The scalability characteristics of this solution are also good. Terminal servers can be deployed in a load balanced, fault-tolerant configuration and therefore can offer services to a few dozen on up to thousands of remote workers.

The level of protection afforded by this solution is a definite plus. As long as it is configured correctly and patches are kept up to date, the corporate network is effectively protected and insulated from remote machines. Another protection benefit to this solution is the fact that a very limited number of holes need to be opened in the firewall(depending on firewall architecture) since all access comes from just a few terminal services machines. A few challenges do exist with this solution since virus protection, host based intrusion detection, and host based firewalls are often not supported on terminal servers. This can be mitigated to some extent by careful configuration, placement, and monitoring of network based IDS systems and firewalls.

Con's I would classify the overall flexibility of this solution as somewhat of a con. In some ways the flexibility of the solution is good because nearly any win32 application can be used and the solution can be accessed from almost any remote machine. However, flexibility is hindered for non-windows client access and is also hindered for some file operations and printing as stated above. Non win32 applications are not supported. Also, any work done on the terminal server is not available when disconnected (i.e. on an airplane etc...).

V.Future direction

The future of secure remote access solutions appears to be a continuation in the directions that have been established today. Dial-up access of all types will likely continue to decline in favor of high speed access employing some combination of the solutions outlined above. However, the need for some sort of dial-up will not go away. Increasingly, dial-up service will be provided by traditional ISP's and others instead of by the corporation. Access to the corporate network will then be provisioned through one of the solutions outlined above.

Where VPN solutions are employed, personal firewall software will increasingly be required and will generally be managed in an outsourced arrangement. It appears that MSSP's who offer this type of service will continue to grow very quickly because of the value that they offer to the enterprise. There is also a move by software vendors of the firewall enforcement solutions to add enforcement of other 3rd party software and any associated policies such as virus protection software and associated signature levels and policies.

Terminal services and Portal solutions will continue to be viable and continue to grow as remote access solutions. Some of the most interesting solutions emerging combine Portals with terminal services access in order to offer a more flexible and useable solution than either class of product by itself.

My opinion is that terminal services and portal solutions will win out in the end for a couple of reasons. First of all, it proxies out user access to the network enabling secure connections without complex and confusing hardware and software. Secondly, because no applications exist on the remote user desktop, it is much easier to manage and extend for large numbers of users.

Direct VPN connections will probably always be necessary for some classes of remote users with specialized applications or non-standard operating systems.

<9 , 10>

VI.Conclusion

I have explored and discussed the problem as it exists today, evaluated the relative pro's and con's some of the solutions that are offered today, and explored the future direction that these and other solutions might take.

The problem is a significant one. Many otherwise relatively secure organizations have no effective security in place for their remote access solutions. Often organizations have been relying on VPN's and/or virus protection as a security mechanism. These are good technologies but are not adequate to protect the enterprise.

Portal solutions, terminal services solutions, and VPN solutions have been employed for some time to attempt to secure remote access connections to the corporate network. Up until recently, it has been very difficult to adequately secure VPN connections with personal firewall solutions and policies. Solutions are now being offered to secure this VPN access in a dynamic and manageable way. These solutions can be employed as either internally managed solutions or a solution managed by an application service provider. These make dynamic user VPN connections much more secure by requiring firewall installation and policy enforcement before a connection is allowed and dropping the connection if the firewall is shut-down, unloaded or policies are changed.

Like many technologies, the best solution is probably a combination of solutions in certain circumstances and for certain numbers of users.

The best all-around solution is probably a combination of Portals and terminal services because of its security footprint and its usability and flexibility. Depending on the portal technology deployed, it may be an expensive solution to employ for a small number of users.

VPN access with an MSSP enforced security infrastructure is also a compelling solution but the difficulties in supporting the remote machines makes it a harder solution to employ. It still has an important place, however, for employees in special roles or those who need access to specialized applications from remote connections.

Internally managed VPN's with an enforced security infrastructure are solutions that are only appropriate for organizations with a need for a large number of remote users and those who can afford the full time security and infrastructure personnel required to manage this solution. Even for those organizations, a higher level of security may be obtained by using an MSSP who specializes in the intricacies of the products and stays abreast of new vulnerabilities threatening their clients every day.

Because the best solution for most companies will be a combination of technologies, most of the technology vendors and service providers out there will continue to thrive for the near future. However, since the best set of solutions for the majority of remote corporate users is a combination of a portal and terminal services, these solution vendors will continue to gain market share.

The need for remote access for corporate workers is poised to increase rapidly in the coming years due to the enabling technologies of home broadband access, high speed wireless access, and the increasing presence of the Internet in every corner of our lives. With these remote connections comes increasing risk to corporate digital assets. It is important that we as security professionals continue to understand and evaluate both the risks and the possible solutions for mitigating those risks so we can employ the best technologies available in order to protect our companies and/or clients.

VII.References:

1. Yasin, Rutrell. "Enterprises Enhance Broadband Security." *InternetWeek.* 18 June 2001 <http://www.internetweek.com/newslead01/lead061801.htm >

2. Bartlett, Michael. "Workers Can't Wait To Go Mobile – Study." *WashingtonPost.com Newsbytes.* 18 Mar. 2002 <http://www.internetweek.com/newslead01/lead061801.htm>

3. Lyman, Jay. "Home Is Where the Hacker Is." *E-commerce Times.* 29 Jan. 2002 <http://www.ecommercetimes.com/perl/story/16035.html>

4. Mitnick, Kevin. "Microsoft hack wasn't espionage." *SecurityFocus Home News.* 5 Nov. 2000 <http://online.securityfocus.com/news/112>

5. Oh, Jenny. "Broadband Opens a Back Door." *The Industry Standard* 11 Dec. 2000 <http://www.thestandard.com/article/0,1902,20467-0,00.html>

6. Girard, John. "Mobile and Wireless Security: Worst and Best Practices." 20 Sept. 2001 <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2815059,00.html>

7. Rasmussen, Scott. "Centralized Network Security Management: Combining Defense in Depth with Manageable Security." *SANS Information Security Reading Room*. 29 Jan. 2002 <http://rr.sans.org/practice/central_netsec.php>

8. "CERT/CC Statistics 1988-2001." *CERT Coordination Center.* 19 Feb. 2002 <http://www.cert.org/stats/>

9. Leyden, John. "Future trends in secuity – 3i survey." *The Register* 28 Jan. 2002 <http://www.theregister.co.uk/content/55/23848.html>

10. "Security: Market Trends." *IT-Director.com* 26 Feb. 2002 <http://www.it-director.com/article.php?id=2633>