Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Secure Access of Network Resources by Remote Clients

Inadequately protected remote computers that access a corporate network may bypass IT safeguards and provide a back door for threats to the network. This paper will identify the threats that remote access poses to corporate network security including those involving hackers, malicious applications and the use of weak access and physical controls. Solutions for these security problems will be proposed using three paradigms; remote-based safeguards that are client-managed, remote-based safeguards that are centrally manag...

Copyright SANS Institute
Author Retains Full Rights

AD

SECURE ACCESS OF NETWORK RESOUCES BY REMOTE CLIENTS

G. Mac Donald
GSEC version 1.3
Submitted February 20th, 2002

Abstract:

Inadequately protected remote computers, that access a corporate network, may by-pass IT safeguards and provide a back door for threats to the network. This paper will identify the threats that remote access poses to corporate network security including those involving hackers, malicious applications and the use of weak access and physical controls. Solutions for these security problems will be proposed using three paradigms; remote-based safeguards that are client managed, remote-based safeguards that are centrally managed and network-based safeguards that are centrally managed. Both Host-based paradigms focus on protecting the remote client from security threats, which in turn, prevents the network from being compromised. The network-based paradigm does not attempt to safeguard the remote host, considering it to be unmanageable and untrustworthy. This "untrusting" model focuses on providing remote access without the client becoming a threat to network security. Each paradigm will be evaluated from a security, business and human resources perspective. This paper will argue that the "untrusting" solution is best able to meet the requirements from all perspectives. Not only is it the most secure but also the easiest to manage, cost effective, scalable and provides the client with increased performance and usability.

Introduction:

As the business utilization of Corporate Information Networks increases so does the requirement for these networks to be remotely accessible by employees, contractors and customers. Unfortunately remote access not only provides legitimate information services, it also creates an excellent opportunity for hackers and malicious applications. Viruses, trojans, and worms are unsuspectingly distributed through the ever-increasing use of email systems and web browsers. With increased network accessibility, and easily obtained tools, hackers locate and exploit vulnerabilities in access controls, passwords, firewalls, operating systems, and ports. The high rate at which these threats occur becomes evident by auditing any of a corporation's IDS/IPS systems (i.e. firewall logs, email filters, virus scanners).

Corporate IT departments have reacted to these pervasive threats by strengthening their perimeter defenses. Corporations have protected their networks from vulnerability probes and access attacks by configuring DMZ's and installing IPS systems (i.e. Firewalls). Networks have also employed filter systems and virus scanners to filter, scan, quarantine and delete malicious applications. IT personnel proactively view logs, scan for vulnerabilities and stay current on new methods of attack, so that defenses can be upgraded accordingly. These defense strategies might secure the network from direct attacks. But does it provide effective safeguards against backdoor attacks that could occur because of remote clients?

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

More and more businesses have remote computers accessing their network through VPN's and dial-in systems. These remote clients may be employees of the company and are working from home or "on the road". Other remote clients may not be directly under the corporations control; they could be corporate partners, customers or contractors. Unfortunately the remote users may be providing an un-secured backdoor into the corporate network. Due to inadequate safeguards and training, the remote computer may be susceptible to attacks from hackers and malicious applications. A compromised remote system might then be utilized to by-pass the networks defenses and cause a successful "backdoor" attack (See Appendix B).

Safeguarding the network from remote access vulnerabilities can present various unique challenges for the security professional. The IT department will have less control over the remote systems then the ones within the networks boundaries. Corporate IT security policies and procedures will be problematic to monitor and enforce. The remote system may not even be owned or configured by the company and the operator may not be even an employee.

Defining the Problem:

High Rate of Occurrence

According to the Security site DefCon "By 2002, approximately 19 million people will have the skills to mount a cyber attack." Recently hackers have seen an increase in the opportunities for compromising home computer systems. Cable-modem and DSL connections have become a popular method for home computers to connect to the Internet. Not only do these connections provide convenience and speed for the home user, but a constant connection. This 24 hour-a-day, often unattended, connection provides ample time for probes and attacks. The attackers job is also made easier by the numerous websites, books, chat rooms and news groups that provide how-to information, and downloadable tools, for the endeavor (see Appendix C). A search of the Internet can quickly demonstrate the ease of obtaining the means for performing probes, staging attacks and creating viruses. For example, a quick Internet search, utilizing Google, with the key phrase "hacking tools" returned over 14,500 matches.

Malicious application attacks have even a higher rate of occurrence then those of direct hacking. Viruses, trojans and worms are easily created and distributed. Basic knowledge of a scripting language, and the ability to "cut and paste", will allow a novice developer to create some very effective strains. These highly portable executables are then provided with ample opportunities of distribution through the highly utilized email and web browsing systems of the home user. CERT® recognizes the high risk of home systems being probed for vulnerabilities and being compromised with such mal-ware as trojans and viruses. [1] Malicious code may also infiltrate the remote client through inadequate safeguards while browsing the Internet.[2] JavaScript, Java and ActiveX all provide a more interactive experience for the user, however they also cause major security headaches.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Not only are remote systems vulnerable to compromise through their "connectivity" but also through direct physical access as well. Outside of the walls of the corporate buildings the remote computer and its data is also threatened by the lack of physical security and business continuity plans. Unattended remote computers run the risk of being compromised through theft, unauthorized access and inadequate backups. "FBI statistics indicate that one in eight laptop computers will be stolen and, in most cases, never recovered."[3]

Remote Risks to Corporate Information Assets

Threats to corporate assets, through remote clients, can be broken down into two primary types; connection-based and connectionless-based. Connection-based threats are arguably of higher notoriety and occurrence, port scanning and email viruses being two examples. Though this paper will focus primarily on connection-based threats the connectionless concerns will still be mentioned.

In a connection-based scenario the remote system becomes the intermediary step to an attack on the network. Essentially attacks are possible by the remote system being seen as logically situated within the corporate network. After the initial authentication and connection process, the remote PC is considered a trusted member. Once within the network the remote PC circumvents the perimeter defenses (i.e. firewalls, filters and scanners). If hackers compromise the remote system it then be used to freely scan, enumerate and attack the network. Malicious applications can also by-pass the perimeter defense from this trusted source. These applications are freely passed through internal file transfers and vulnerable shares. None of these hacker or mal-ware exploits would be possible if not for the open ports, files and shares between the remote client and network.

Not all threats, involving the remote client, require a connection to the corporation. Hackers could gain information from the remote client that would allow direct access to the network. For example, planted software could record keystrokes or the hacker may crack cached passwords. This information can then be used to access the network directly, instead of doing it through the remote client. The remote system may also put corporate assets at risk by storing valued information on its local hard drive. Confidential and valuable files can be lost or exposed through system failure, theft and unauthorized direct access.

Solution Criteria:

In order to examine the proposed solutions to remote access vulnerabilities, it is essential that evaluation criteria be established. As with all IT security solutions there is a need to balance the requirement for a secure networking environment with the convenience and productivity of the employee, and the cost effectiveness for the organization.

For the protection of the corporate network, and its assets, security measures will focus on threats that have been deemed as occurring at a high rate. More specifically

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

safeguards will focus primarily on defending the network from hacking (see Appendix C) and the infestations by malicious applications (see Appendix B).

Budgeting for a particular network security solution can be quite complex. There will be obvious expenditures that may include implementation, licensing, maintenance, support agreements and training. Some costs will be more obscure and difficult to calculate, i.e. client training, increases in help desk support, compliance management, increases in technical issues, required system upgrades etc. The remote equipment may not be standardized or even owned by the corporation. The remote user, who may not be an employee, may require after hours help desk assistance, or other special considerations. As the remote access pool expands and diversifies IT staff will need additional training to cope with a larger array of problems.

A person's ability to easily utilize the remote PC is also an important factor. A complex procedure for the end user may result in compliance issues, need for increased training, denial of service and a higher number of service calls. This complexity, in turn, will negatively affect the productivity of the person's time on the computer.

Management issues will also need to be investigated: How costly and complex are the mechanisms for; implementation, updating, modification, support, auditing and logging? How flexible and scalable is the solution? Is it adaptable to different platforms? Is it adaptable to different groups i.e. contractors, home users and mobile users? Can it work well with various operating environments and applications? How complex will compliance management be and what level of compliance can be expected? Does the solution generate side effects that can be viewed as value added or detrimental?

Obviously the remote client situation is a complex problem with no perfect solution. However for this paper the proposed paradigms will utilize the following required and optional objectives, as well as discussing business and operational concerns:

<u>Required Security Objectives:</u>

- Prevent hacker's enumeration and attack of network by blocking access to ports and shares.
- Prevent the network infection by malicious applications.

<u>Optional Security Objectives:</u>

- Prevent exposing sensitive data through theft or unauthorized access of remote clients.
- Prevent data loss through backups
- Prevent network access through password compromise.

<u>Business Concerns</u>

- Implementation Costs
- Ongoing or secondary costs (i.e. maintenance, training, technical support)
- Allows (if not increases) staff productivity
- Reduces risks, to an acceptable level, cost effectively

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- How does it add value to the system?

IT Operations Concerns

- Ease of maintaining, upgrading and auditing
- Level of compliance management required
- Training requirements for IT staff and clients
- Support requirements
- Scalable
- Ease of implementation
- System requirements and level of platform dependency

Paradigms:

1.Remote Based Safeguards-User Managed

The main objective in this distributed solution is to protect the network by safeguarding the remote client. The idea being, that if the remote client isn't compromised then the network cannot be threatened through it. In this solution security is provided through host-based applications, policies and procedures, which are managed by the end user. The safeguards main purpose is to harden the client against direct threats from malicious applications and hacker attacks. Though the safeguards are all located and managed by the remote client, the IT team would still be involved in the implementation, training, support and compliance management. Without the involvement of the IT team, the effectiveness of implementation and maintenance could not be reliably guaranteed.

For this solution the paper will adopt the recommendations made by CERT web site in their recommendations for "Home Network Security". [4]

1. Use host based firewall
2. Turn off your computer or disconnect from the network when not in use
3. Keep all applications, including your operating system, patched
4. Use of strong access controls such as secure passwords *
5. Utilize virus protection software
6. Run software to filter email attachments *
7. Don't open unknown email attachments
8. Don't run programs of unknown origin
9. Disable hidden filename extensions
10. Disable Java, JavaScript, and ActiveX if possible
11. Disable scripting features in email programs
12. Make regular backups of critical data
13. Encryption of sensitive data *
14. No caching of passwords on PC *

(The papers author added the asteriated items. They are important considerations that were not mentioned in the list of CERT recommendations, due to it being a list primarily for home users and not network remote end points.)*

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Pros

In theory, at least, this solution meets all the required and optional security objectives: Items 1-4 are to prevent hackers from having means and opportunity to compromise the remote system. The client-based firewall prevents the unwarranted access of ports, which in turn prevents the footprinting, scanning, enumeration and unauthorized access of the system (see Appendix C). Turning off the computer decreases the window of opportunity for an attack. Patching and upgrading the OS with service packs diminishes the number of newly discovered exploits that can be used against the system. Strong passwords prevent unauthorized access through brute guessing.

Items 5-11 are to prevent the remote system from being infected with malicious applications.

Item 12-13 is more focused on securing the remote PC from the more direct "connectionless" threats. Even if the computer is not "connected", important information could be stolen, lost or compromised, due to the system not being adequately backed up and encrypted.

Initial costs of software are quite low. The virus scanner and firewall software purchase, to meet the "required security objectives", will be about $120/remote client. Remote based virus scanners can be downloaded from the Internet for about $50/copy and statefull, application aware, firewalls for $10 to $20 more. The professional personal firewall sold by ZoneAlarm will also filter out email attachments that have the ability to carry viruses.

The "optional security objectives" can be met by adding about another $100-$200 to this solution. Effective encryption software can be downloaded from the Internet for free and many backup solutions will cost between $100 and $200. All in all the direct setup costs for this solution would be $150-$300 for each remote access point. At least at first glance this solution appears to reduce risks, to an acceptable level, cost effectively.

Cons

Though this model theoretically fulfills the "required security objectives" in an applied security environment it consistently fails. The end user cannot be expected to have the experience, training or inclination to meet all the rigorous standards for maintaining a secure system. It is unrealistic to expect that 100% of the clients will be able to meet the technical challenge 100% of the time (see Appendix B).

This model requires the end user not only to have a high level of technical knowledge but also a desire to comply with procedures and policies. For example, all remote users must be willing to sacrifice the "fun side" of web browsing since active code would be prohibited. All remote users must never get frustrated with the firewall popping up and blocking their remote activities. They would also need to be sophisticated enough to realize that "htm" attachment isn't really from their best friend telling them about a hot stock tip! Though compliance management can be implemented for the end point, at what cost? (See Appendix A) One also needs to realize that the level of non-

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

compliance will be compounded by non-employee utilization, i.e. corporate clients, employee's friends and family.

With this solution there appears to be a low startup cost, however there are many hidden initial and ongoing expenditures that need to be identified (see Appendix D). During the remote user setup additional software licenses may need to be purchased. If the remote user is an employee who uses a different computer at work then at home, two licenses will be required for each essential application. This model will also have increases in costs and technical challenges associated with substantial compliance management, remote audit procedures and staff/employee training. The help desk's calls could increase dramatically and the support staff will need to be more diversified in their knowledge. Since the remote systems will be running OS's and applications that may be more diverse and different then what staff are accustomed to within the network. Extended hours of technical support may also be required, as the remote points will generally be utilized outside of business hours in the evening or in different time zones.

One of the important business related concerns is the decrease in employee's work productivity. Some of the employee's time must be diverted from productive work for the purposes of performing security and technical duties. The remote user will require time to maintain the software, download and apply patches, update virus definition files, perform threat recognition and handling as well as manage encryption key archives, passwords and backup strategies.

2.Remote Based Safeguards-Centrally Managed

This solution is similar to the "Remote Based Safeguards-User Managed" paradigm in that it attempts to protect the network's resources by safeguarding the remote client. However this paradigm recognizes the problems with the remote user controlling the safeguards. Though host based security is still utilized there is a shift to having them centrally managed by the network. This method reduces the compliance and training problems by reducing the remote user's involvement. In this model remote base security applications are configured and controlled from the network. The network also may utilize network based applications and scripts that perform security functions remotely.

As in the first solution host-based firewalls and virus scanners are utilized, however this time they are controlled by network centric management systems. Many of the same companies that have produced personal security products have also developed client/server solutions. "PGP Desktop Security V7" by Mcafee, "ZoneAlarm Integrity" by ZoneLabs and "CyberArmor Suite" by InfoExpress are all firewalls that reside on the remote client but are controlled by a network based server/management console. The network-based server components manage and configure the remote firewalls. IT Security policies and configurations are centrally defined then distributed to the remote hosts. The server then enforces the policies while the remote hosts are connected to the network. Each of these products, though the same in its basic objective, provide additional and different security features; PGP's product performs file encryption and

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

ZoneAlarm's product filters the riskier types of attachments from the email. ZoneAlarm's product also checks for any suspicious changes to important system files, five integrity checks are performed on important system files before the server allows the remote client to connect to the network (i.e. MD5, file name registry, size and description). Enterprise versions of virus scanners are also available. Virus definitions are downloaded from a network based server to the client during connection. Though these new definitions are pushed after the connection is made the network can scan the remote system while establishing a connection.

System Updates, system patch installs, virus updates, data backups and registry settings can all be remotely managed through networked based scripts and services. For example login scripts can upload and apply system updates to certain versions of windows. Network based backup applications are able to perform remote backup services for the client, downloading files to the secure network environment at regular intervals.

Pros

The obvious benefit to this approach is that it removes many of the end user compliance issues that were so evident with client managed safeguard model. The user's level of technical ability and security compliance is greatly diminished. As such the need for client training and compliance management is also greatly reduced.

Upgrades and installations are server initiated resulting in a standardized implementation that requires less time from both the end user and IT technical staff. Once the servers, scripts and network centric services are configured they will push updates and enforce policies without further need for intervention. When policies or installations require modification the IT staff performs the changes from a centralized point and then pushes the changes to the distributed agents.

Cons

Though this solution diminishes the need for user security awareness and compliance it does not eliminate it. For example, there will still be requirements to use strong passwords, maintain proper configurations of Internet browsers and to safeguard confidential files. This diminished role may work against the security of the system in several ways. The end user may perceive the remotely enforced security applications and policies as invasive and attempt to circumvent them. The automated systems may also breed a false sense of security for the end user resulting in a diminished level of caution.

Client/server solutions have a higher implementation cost then the distributed versions. These costs may include server and client licenses, annual renewal fees, and ongoing support fees and insurance for upgrade renewals. For example the ZoneAlarm "Integrity" firewall product is $4500/100 clients plus $17000 for the server and a 13 % renewal fee.[5] There will also be indirect costs associated with this solution. Even though the remote client is no longer in charge of security systems an unexpected or

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

misunderstood behaviour may elicit their concern. Technical support may be required when the security applications prevent a user from performing an activity, warns or reacts to an attack or causes performance issues.

Bandwidth/Connection performance may also be negatively affected with the increase of network/client security maintenance overhead. For example, policies are being pushed to the client, MD5 settings are being checked on critical files, information downloaded to the network for backup purposes and service packs uploaded and installed on the client.

Due to compatibility issues, this solution will also place restrictions on the remote PC's hardware, Operation System, software configurations and platform. Once a particular firewall and virus server has been purchased the remote system will need to be compatible with it. Many firewall and virus solutions will only work in a Microsoft windows environment. For example ZoneAlarm is only "compatible with Microsoft Windows 95/98/Me/NT/2000 and XP".[6]

3.Network Based Safeguards-Centrally Managed

Unlike the distributed paradigms this centralized model does not secure the network by attempting to safeguard the remote PC. In this model the remote client is considered unmanageable and consequently untrustworthy. The objective of this model is to provide adequate services to the remote clients while preventing them from attacking, infecting or in other ways compromising the security of the corporate assets.

Technically this solution has two essential components; on the remote PC there is a thin client agent, while on the network side a secured application server. The only required installation at the remote point is an operating system, a thin client agent and a secure connection service (i.e. VPN or dial-in applet). No other applications are required on the remote PC including the need for a; firewall, virus scanner, encryption software, service packs, backup routines or office applications such as an email client, word processor or spreadsheets. All security related applications and business software is located within the corporate network, on the secured application server.

Both Microsoft and Citrix have developed Terminal Server technology that was designed as an application server, though a Web Server such as IIS may also meet the requirements. Once in place the remote client accesses all the required business related applications through the thin client technology. The thin client agent intercepts mouse movements and keystrokes from the user and forwards them to the appropriate applications that reside on the network based application server. The server returns nothing more then screen refreshes to the remote user. The remote user is opening and manipulating data by utilizing the server's CPU, memory and hard drive (see Diagram 1)

The Application Server is secured on the Internet side with the use of a network switch. The Application Server has also been equipped with a host-based firewall and virus scanner. The Application Server protects the corporate network, from the outside, by

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

utilizing a different NIC/switch connection and separate firewall policies. This separation prevents any packets from the outside ending up within any other part of the corporate network (See Diagram 1). The Application Server's firewall rules are configured to be very restrictive for connections with computers outside of the corporate network. The only ports that accept traffic from the "outside" are those utilized for Terminal Server traffic. These required ports are further configured only to accept the required terminal server protocol from authorized thin clients. Nothing else is open to the outside world including shares, ports or null sessions. If a hacker has compromised a remote client his techniques will be ineffective in penetrating the server (see Appendix C).

Malicious application infiltration from the remote client will also be prevented. All direct malicious application transferal methods between the remote client and server have been virtually eliminated. The ports open between the two points will only accept certified terminal server protocol or traffic and there are no shares open. Infection cannot occur through the transfer of data or files, since no files are shared between the two points. The files are opened on the network side and then only viewed and manipulated through strictly controlled input/output traffic.
Even though the Application Server is equipped with functioning virus scanners and filters, their need is reduced by the fact that there is no "trusted" communication to the remote point.

The Centralization of this model makes the optional security safeguards easier to accomplish and manage as well. The Application Server can easily be audited for problems and upgraded to prevent vulnerabilities by IT staff. With important corporate files being stored within the network, confidentiality and availability issues are easily resolved. Files, data and applications are backed up by the same network system as all other centralized assets. Sensitive files are no longer threatened from the remote computer being accessed by un-authorized personnel or being stolen.

<u>Pros</u>

This model provides, with a high level of certainty, that security procedures, policies and applications will be effectively managed. This certainty comes from the centralization and professional management of the safeguards. The end user is no longer required to follow complicated and annoying procedures, nor are they responsible for configuring and maintaining security applications. With the dramatic reduction in the need for end user involvement in security comes a dramatic decrease in issues involving compliance management. This method acts totally separate, and transparently, of the remote PC. The remote user will not perceive any evasive amount of control over their computing environment or activity. The remote user is permitted a freedom on their computer that the other solutions would prevent.

Direct and indirect costs of this solution are less then those of both previous solutions (see Appendix D). Microsoft's Terminal Server license and software is sold for less then $1000 and a client license less then $100. Additional money can be saved by not

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

having to purchase security and office applications for the remote locations. There will also be substantial indirect savings with this method as well. Since remote users are not greatly involved in security procedures the need for compliance management and employee training is greatly reduced. The users requirement for help desk support should also decrease.

Sensitive data is also more tightly controlled and receives a higher rate of protection. Since files are kept within the confines of the company they are more secure. When a user closes his email or a confidential file it's not sitting on the remote PC's hard drive, it's stored safely on a network-based file system. The network now takes care of the backups and scanning of the files for corruption. If a person's remote system is stolen or otherwise compromised there will be no confidential data to be viewed or stolen. The end user will no longer have to be concerned about encryption systems or key management.

Most security solutions deteriorate remote PC performance due to resources being required for security overhead. However this solution actually increases the performance for the remote PC. Remote resources are not involved in the business and security application processing. Since the application processing occurs on the server, processing will occur at the server's speed. For example a client could sit at home utilizing a 486dx2 computer with Dos 6.2 but be running the application at the processing speed of a Pentium 4. Network usable bandwidth will also increase since the thin client is only involved in what is required for input and output data (i.e. screen refreshes, keystrokes and mouse movements). The remote user will actually see a performance increase in opening emails, files and application processes. One example of this concept is Citrix's terminal server product independent Computing Architecture (ICA).

> *"On the server, Citrix ICA has the unique ability to separate application logic from the user interface. On the client, users see and work with the application's interface, but 100 percent of the application executes on the server. And with ICA, applications consume as little as one-tenth of their normal network bandwidth…. ICA is optimized for connections as low as 14.4 Kbps. Only mouse clicks, keystrokes and screen updates travel the network to generate exceptional performance."* [7]

Platform dependency is also greatly reduced. The terminal server clients are quite flexible on what they can be installed on. While the remote software for solutions involving remote security applications had fairly strict hardware and OS requirements, this solution does not. For example, a Citrix client agent can be installed on a various remote platforms but connect to the same Application Server. Citrix provides clients for legacy windows systems, current Microsoft products, Unix, Linux and even some hand held appliance operating systems.[8]

<u>Cons</u>

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Work productivity becomes more closely associated with the connection to the network. Emails, data and applications are all located in the network. If a connection cannot be made critical work and productivity will be greatly affected.

The terminal server solution was discussed with technical support staff of ZoneLabs and they were able to think of only one problem with it.[9] If the remote computer is left vulnerable it could become compromised with hacker utilities that could perform screen captures. The captured information would allow the hacker see confidential information or learn the users password/access information. This was the only vulnerability that they could come up with. Safeguards against both vulnerabilities can be implemented. For the password vulnerability the system could be hardened by providing the remote client with either a one time password device such as a token or provide them with a biometric device such as finger print reader. The solution for the file confidentiality problem can be to control what files can be viewed from the Terminal Server. In other words classified files would be restricted from terminal server sessions.

Discussion:

Research for this paper resulted in copious amounts of information related to securing network assets by safeguarding the remote access point. Searches for information on a centralized approach, however, resulted in absolutely no literature. Lack of documentation resulted in several companies and technicians being contacted to assist in the evaluation of the centralized paradigm (see Acknowledgements). These contacts have resulted in numerous discussions, as well as several technical teams testing the concept. From the results of the testing I've concluded that the model is a valid, real world, approach to the problem. My conviction is reinforced by the fact that this is the basic concept that web sites utilize all the time. Web sites permit and rely on connections with remote clients that they have little "trust" in. For example neither my "hotmail" provider or my bank's web site requires my computer to be "secure". When I go to my hotmail account the web server has protected itself against the remote PC. My bank allows me to view my confidential information as well as execute transactions. Surely if the "Network Based Safeguards-Centrally Managed" is a cost effective and secure approach for these organizations it can be considered a valid paradigm for corporate networks!

The "Network Based Safeguards-Centrally Managed" paradigm has the characteristics of a security solution that can actually be effective. The solution does not have unrealistic expectations of personnel nor does it equate security with increases in cost and decreases in productivity.

The "untrusting" solution doesn't have unrealistic, clouded or impractical expectations of the end user. High levels of security compliance are neither required nor expected from the systems user. Any security solution that involves technical security solutions, high rates of threat occurrence and a requirement for end user compliance is flawed and will fail. The solution is also "real world" in that it recognizes the need for the end user to be productive in their work without understanding the technology they are utilizing. The

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

most valuable asset of any company is it's employees. When large amounts of user time are required to learn and comply with complicated security procedures then production is lost and an asset wasted.

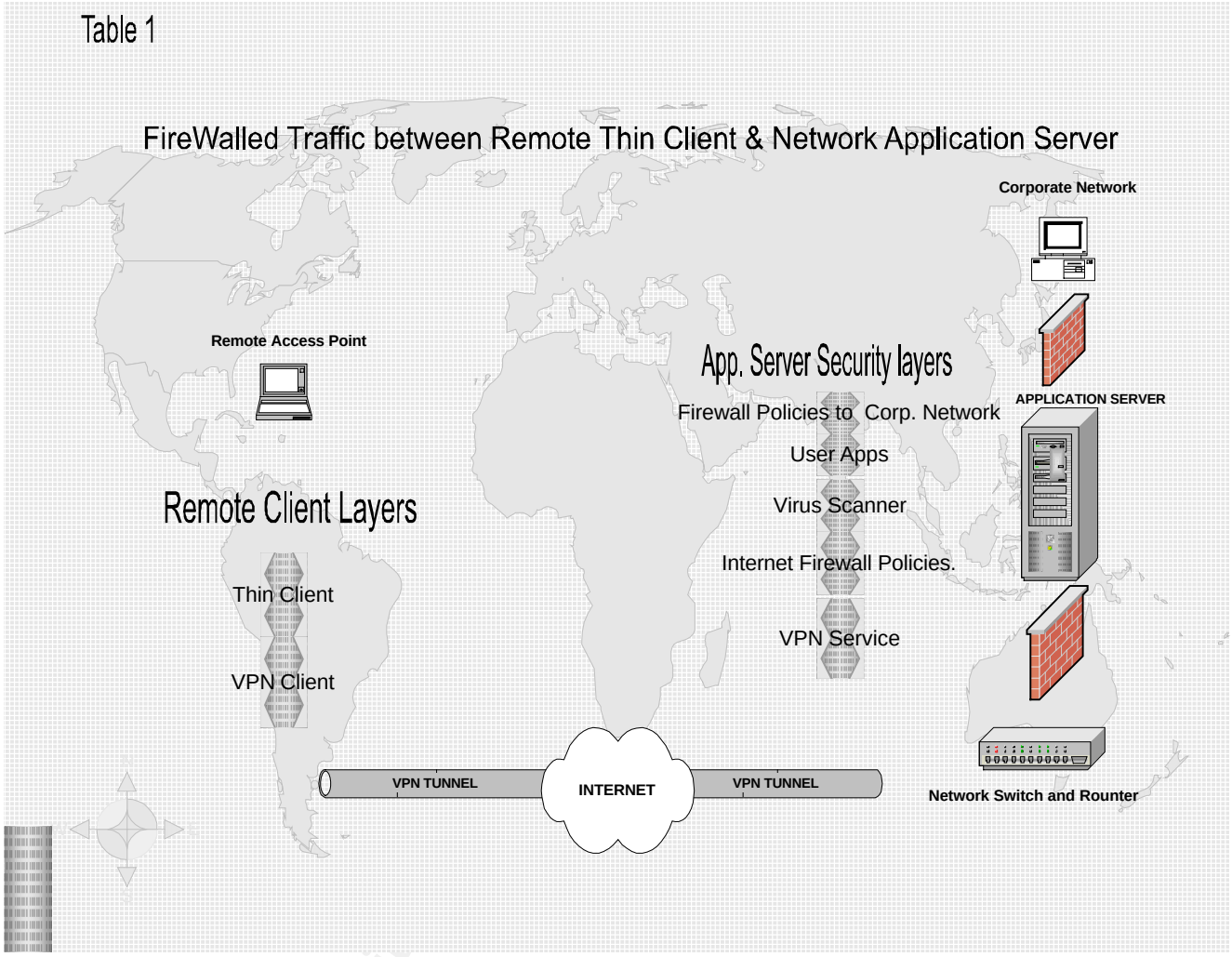
Conclusions:

For an information security solution to be acceptable it must cost effectively reduce risks to an acceptable level while allowing the productivity of the system. Of the three paradigms this paper examined, for the safe access of network resources from remote clients, the only one that met these criteria was the "Network Based Safeguards Centrally Managed" solution. This solution requires the least amount of compliance from the remote user, and as such is the most consistent and reliable in its implementation of security policies and procedures. Not only was this approach the most secure it was the most cost effective and actually could result in less requirements for technical support and an increase in system performance.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Diagram 1:



(Diagram is original work by papers author)

Appendix A: (Non-compliance Case Studies)

This appendix describes cases that the author has been directly involved in during his 8 years in the IT profession. These situations are included to demonstrate non-compliance behaviour and how punitive measures could cost more then the asset that they are intended to guard. Please note that while the situations are true and accurate, including costs, the names of companies, locations and people have been altered.

<u>Situation 1: High valued low-tech employee</u>

Mr. Im Busy is the Director for Western United States for the company XYZ. This position requires Mr. Busy to travel regularly throughout his extensive territory. During his travel Mr. Busy spends his days meeting with regional managers and his evenings

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

completing the day's paper work. This paper work involves connecting remotely to the head office to transfer files and access emails.
Mr. Busy just recently negotiated the annual financial quotas for his territory for the 2002 fiscal year. He has contracted himself, and his team, to generate slightly over $3 billion in new business within the next twelve months. Three years ago, before Mr. Busy took the territory over, the Western United States was consistently and substantially "behind plan". In some years the territory was sometimes as much as 60% behind expected revenues. Since Mr. Busy directed the region the revenues have been consistently "over plan". In the last two months alone Mr. Busy's territory has been 196% above plan for that time period. In the last two-month period Mr. Busy was expected to generate approximately $300 million of new business, he generated slightly over $800 million.
Mr. Busy, though a valuable asset to the company is very non-compliant with security procedures. Though very bright, he has very little ability and patience when it comes to computers. He views "wasting time with complicated computer procedures as a cost of millions of dollars in company time!" He has, on numerous occasions, had to call for technical support on such simple procedures as copying a word document to or from an email. And on a regular basis re-writes documents because he is not able to find where they have been saved.
Mr. Busy has been offered computer training and has also been given a list of computer security procedures he is expected to follow. Needless to say these procedures are not being followed both for lack of ability and lack of interest.
If Mr. Busy were released from the company several costly things would occur. First of all the company would loose a very valuable asset in the form of an employee that has been responsible for generating literally hundreds of millions in corporate profits. Secondly the employee would take legal action for loss of expected income. The company would settle with the employee quietly as to not effect the company's reputation and stocks. Thirdly Mr. Busy has many valuable contacts and customers that would leave the company with him.

Situation 2: High tech Contractor

One of the company's I consult for is involved in production of construction materials from raw wood products. The company has over a dozen mills and each of these mills has been outfitted with highly automated systems. The machinery is all leading edge technology controlled with leading edge proprietary computer systems. These computer systems are on the corporate network to facilitate remote management, automated data collection and analysis. The contractors that have installed all this equipment are located in Germany and need to be called on a regular basis for remote maintenance and management of these very sophisticated systems. Due to the contractors concerns over confidentiality they are not willing to inform us on their level of compliance with our remote security procedures. The systems that the contractor controls are essential to the business and must be maintained on a regular basis. One estimate from management is that if the contractor could not promptly deal with problems remotely that the downtime would generate a loss of $60,000/hour.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

When management was asked if they would ever consider banning the contractor from connection to the network their response was one of questioning my understanding of "The Business".

Appendix B: (Incident Case Study)

This appendix describes an incident that the author had been directly involved in. Please note that while the situations are true the names of companies and people have been altered.

Party in through the back door

Mr. TJ is a Vice President for the company ABC. The corporate email system of ABC Inc. is protected against distributing malicious applications through a multi-layer approach. First the mail server has all incoming and outgoing email attachments scanned for viruses. Secondly all incoming emails are filtered for attachments that are executable. If an attachment has the ability to be activated it is not sent to the email recipient, instead it is quarantined. The quarantined attachment is only forwarded to the intended recipient if it is requested and required for business reasons. The purpose of the filter system is to prevent network infiltration from viruses that have not yet been isolated and defined for the virus scanning system. Another layer of defense against the viruses is the ongoing corporate education and virus awareness program.

Mr. TJ has met all the policies and security requirements for remote access into the company. He has installed a personal firewall and virus scanner. He is also diligent in keeping the virus scanner up to date and is careful in what attachments he opens.

One Sunday morning, early January 2002, Mr. TJ is sitting at home utilizing is home PC. Mr. TJ has two Outlook profiles one for his home Internet mail and one for his corporate mailbox. He goes to his ISP mailbox through the outlook client and finds a letter waiting for him with the subject title "new photos from my party". Mr. TJ opens the letter to find the attachment "www.myparty.yahoo.com". Mr. TJ perceives this to be a hyperlink that has been sent to him by a trusted friend. Mr. TJ is also not concerned about going to this site since he has also been careful to follow IT security instructions able disabling his browser from executing active scripts from web sites. Mr. TJ double clicks on "the party attachment" several times but no web page appears. Mr. TJ thinks very little about it, assuming a broken link he continues reading his other email. After reading mail from his ISP mail box Mr. TJ opens his VPN to work. Once connected to work through the VPN he opens the outlook application with his corporate profile to check for work-related email.

Unknowingly Mr. TJ's infected outlook has just released the mass-mailing worm "Win32.MyParty.A"[10] into the corporate network. At the time a virus definition had yet to be released for this attachment so neither the remote hosts personal virus scanner nor the corporation's detects it. The worm spread quickly through the company even though the perimeter defenses were ready to deal with an attachment of this sort. Any email coming from the Internet would have been filtered before it had reached the mail system. Mr. TJ had complied with all policies that Cert and his IT department had

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

required and the Corporations front door had a multi-layer defense yet this worm cost numerous days of recovery and substantial embarrassment.

Appendix C: (Hacking Procedures)

1. FOOTPRINTING
   Objective: Target address range, namespace acquisition, and information gathering.
   Technique: Open source search, whois, DNS transfer
   Tools: www.networksolutions.com/whois, www.arin.net/whois/dig, nslookup www.samspade.org

2. SCANNING
   Objective: Target assessment, identification of most promising system Compromises.
   Technique: ID ports, shares and OS, map network thru ping sweeps and port scans
   Tools: fping, nmap, fscan, siphon, queso, superscan, netviewcmd

3. ENUMERATION
   Objective: Assess identified recourses (i.e. ports, share, OS) for vulnerabilities
   Technique: List user accounts, file shares, applications, services running, ports open
   Tools: null sessions, DumpACL, sid2user, NAT, Legion , banner grabbing, netcat

4. GAIN ACCESS
   Objective: Informed attempt to comprise target network or system.
   Technique: Password stealing & guessing, file share brute forcing, password file grab & Crack, buffer overflows
   Tools: tcpdump, L0phtcrack, legion, tftp, pwdump2, bind, retina

5. ESCALATE PRIVILEGE
   Objective: Gain system control, examine privileged information, modify system
   Technique: Exploit target vulnerabilities, crack weak passwords of privileged accounts
   Tools: john, L0phtcrack, getadmin, sechole

6. PILFER
   Objective: Obtain privileged information on systems, personnel, clients, trade secrets
   Technique: Text search engines, view names of files , scan databases
   Tools: rhosts, LSA Secrets, registry, cybercop, various text search engines

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

7. COVER TRACKS
   Objective: Prevent detection of system compromise and its method or source
   Technique: Clear all audit trails logs and hide tools and exploits of vulnerabilities

8. CONTROL/OWN SYSTEM
   Objective: Continue eavesdropping for information, access other systems, launch attacks on other systems
   Technique: Install software and create accounts that will allow future access, Remote control and the ongoing capture of information
   Tools: Trojans, rogue user accounts, scheduled scripts, install remote Control Services, remote.exe, VNC, BO2K, keystroke loggers
   (Source: Hacking Exposed [11])

Appendix D: (Budgets for Solutions)

This appendix prepares a budget for each of the proposed paradigms. The submitted budgets examine the primary costs with what it would cost to maintain the solution for one year for a small company with 20 remote clients and a mid-sized company with 100 remote clients. These budgets do not examine the hidden costs.

1.Remote Based Safeguards-User Managed

First year implementation costs:	Qnty:	20 users	100 users
Host based firewall application:	1/user	$1000	$5000
Host based virus scanner:	1/user	$1000	$5000
Encryption Software:	1/user	$0	$0
Additional Office App. License: *	1/user	$10000	$50000
CD writer for data backups:	1/user	$2000	$10000
Blank CD's weekly data backups:	52/user	$1000	$5000
First year Total:		$15000	$66000

Annual Maintenance Costs:	Qnty:	20 users	100 users
CD writer replacements:	20%	$400	$2000
Blank CD's weekly data backups:	52/user	$1000	$5000
Yearly Total:		$1400	$7000

Total Costs by End of 2nd fiscal year:	$16400	$73000

*Note: If the remote user is an employee, who uses a different computer while at work, an additional software license will be required for all remote office/business applications. (i.e. one license for work based computer and one for remote)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

2.Remote Based Safeguards-Centrally Managed

First year implementation costs:	Qnty:	20 users	100 users
Client for firewall:	100(min)	$4500	$4500
Client virus scanner:	1/user	$1000	$5000
Firewall Server application:	1/netwk	$17000	$17000
Virus Scanner Server App:	1/netwk	$3000	$3000
Additional Office App. License: *	1/user	$10000	$50000
Encryption Software:	1/user	$0	$0
Dedicated PC for Svr Apps:	1/netwk	$2000	$2000
First year Total:		$27500	$81500

Annual Maintenance Costs:	Qnty:	20 users	100 users
Annual Firewall Maint. Fee:	13%	$600	$600
Yearly Total:		$600	$600

Total Costs by End of 2nd fiscal year:	$38100	$82100

*Note: If the remote user is an employee, who uses a different computer while at work, an additional software license will be required for all remote office/business applications. (i.e. one license for work based computer and one for remote)

3.Network Based Safeguards-Centrally Managed

First year implementation costs:	Qnty:	20 users	100 users
Terminal Server Client:	1/user	$2200	$11000
Terminal Server App Svr:	1-2/netwk	$1050	$2100
Firewall on Terminal Svr:	1-2/netwk	$50	$100
Virus Scanner on Terminal Svr:	1-2/netwk	$50	$100
Additional Office App. License: *	0/user	$0	$0
Dedicated PC for Svr Apps:	1-2/netwk	$3000	$6000
First year Total:		$6350	$19300

Annual Maintenance Costs:	Qnty:	20 users	100 users
Annual Firewall Maint. Fee:	na	$00	$00
Yearly Total:	$00	$00	

Total Costs by End of 2nd fiscal year:	$6300	$19300

*Note: If the remote user is an employee, who uses a different computer while at work, no additional software license will be required for use of the office/business applications.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Footnotes:

1. Carpenter Jeff, Dougherty Chad, Hernan Shawn. "CERT® Advisory CA-2001-20 Continuing Threats to Home Users". July 23, 2001. URL:http://www.cert.org/advisories/CA-2001-20.html

2. CERT/CC. "CERT® Advisory CA-2001-20 Continuing Threats to Home Users". July 23, 2001. URL: http://www.cert.org/advisories/CA-2001-20.html

3. Smith Joel, "Service finds stolen laptops", USA Today, October 24, 2000. URL: http://www.usatoday.com/life/cyber/ccarch/ccjoe038.htm

4. CERT/CC. "Home Network Security" No revisions date available. URL:http://www.cert.org/tech_tips/home_networks.html#Iv

5. Smith Jason, Technical Sales, ZoneLabs Inc.

6. ZoneLabs. URL: http://www.zonelabs.com/

7. Citrix Systems Inc: URL:http://www.citrix.com/products/clients/ica/technology.asp

8. Citrix Systems Inc: URL: http://www.citrix.com/products/

9. Morgan Justin, Level 2 Technical Support, ZoneLabs Inc.

10. Computer Associates Virus Information Center, "Win32.MyParty.A", January 06, 2002. URL: http://www3.ca.com/solutions/collateral.asp?CT=65&ID=1323

11. McClure Stuart, Scambray Joel, Kurtz George, "Hacking Exposed", Corel Ventura Publishing, Third Ed, 2001. Info. From inside of back cover

Bibliography:

Carpenter Jeff, Dougherty Chad, Hernan Shawn. "CERT® Advisory CA-2001-20 Continuing Threats to Home Users". July 23, 2001. URL:http://www.cert.org/advisories/CA-2001-20.html

CERT/CC. "CERT® Advisory CA-2001-20 Continuing Threats to Home Users". July 23, 2001. URL: http://www.cert.org/advisories/CA-2001-20.html

CERT/CC. "Home Network Security" No revisions date available. URL:http://www.cert.org/tech_tips/home_networks.html#Iv

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Computer Associates Virus Information Center, “Win32.MyParty.A”, January 06, 2002.
URL: http://www3.ca.com/solutions/collateral.asp?CT=65&ID=1323

Citrix Systems Inc: URL:http://www.citrix.com/products/clients/ica/technology.asp

Citrix Systems Inc: URL: http://www.citrix.com/products/

Frato Mike, “Firewalls at Your Service”, November 12,2001.
URL: http://www.networkcomputing.com/1223/1223f34.html

Hawkins Dana, “Data on home computers not necessarily your own”, February 28, 2000,
URL: http://www.usnews.com/usnews/nycu/tech/articles/000228/nycu/work.htm

Krutz Ronald, Vines Russell Dean,” The CISSP Prep Guide”, pub John Wiley & Sons, Inc.

McClure Stuart, Scambray Joel, Kurtz George, “Hacking Exposed”, Corel Ventura Publishing, Third Ed, 2001

Shirley John, “A Guide to Managing Remote Users”, April 10,2000
URL: http://www.networkcomputing.com/netdesign/1107remote-full.html

Smith Joel, “Service finds stolen laptops”, USA Today, October 24, 2000. URL: http://www.usatoday.com/life/cyber/ccarch/ccjoe038.htm

Smith Jason, Technical Sales, ZoneLabs

Tweney Dylan, “ Are Home PCs a Backdoor Into Your Corporate Network?” August 02,2001
URL: http://www.business2.com/articles/web/0,1653,16680,FF.html

ZoneLabs. URL: http://www.zonelabs.com/

ZoneLabs, “ New Threats, New Solutions: Enterprise Endpoint Security”,
URL: http://www.zonelabs.com/pdf/IntegrityOverview_final.pdf

Contacts & Acknowledgements:

The following people provided either technical input or laboratory testing for the solutions provided in this paper.

Morgan Justin, Level 2 Technical Support, ZoneLabs Inc.

Roger (not permitted to supply last name) Level Two Technical Support, Microsoft Canada

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Smith Jason, Technical Sales, ZoneLabs

Storkey Peter, Senior Technician for Exchange & Connectivity Services, (Not Permitted to provide corporation name or address)

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**