The Importance of Personal Firewalls and Anti-Virus software in the business environments.

By: Jason Kennedy

GIAC Security Essentials Certification (GSEC)

Version 1.4c

Option 1 – Research on topics in Information Security

March 21, 2005

Abstract

This paper will show the importance of using Personal Firewalls and Anti-Virus software on endpoint computers in the business environment. I will explain how utilizing Personal Firewalls and Anti-Virus software on endpoints will help achieve a Defense in Depth model and mitigate many risks and vulnerabilities that computer endpoints are exposed to in the business environment.

An introduction to the paper and the business environment will set the stage for importance of Personal Firewalls and Anti-Virus software in this environment. Personal Firewalls will be the first topic described and Anti-Virus will follow. I will be explaining several products, and also give some demonstrations as to how the products can mitigate important risks and vulnerabilities in a business environment. I will also recommend other products beyond the ones that I examine in detail. I will end with a conclusion, which will backup my writings on showing the importance of Personal Firewalls and Anti-Virus software in the business environment, how they will help achieve a Defense in Depth model by mitigating many risks and vulnerabilities.

Introduction

It seems as though everyone is connecting to the Internet these days, from browsing websites and checking email to connecting remote workers and offices to the corporate network. Internet usage is growing at a rapid rate world wide. With the phenomenal growth of the Internet, comes the unfortunate growth of Internet based attacks. These attacks that cause a disruption or denial of service are causing companies to lose an average of $2 million in annual revenue. [1]

Unfortunately the Internet is not the only source of attacks. In business networks attacks from internal employees are growing at an extremely large rate. According to an article from ComputerWorld.com, 80% of all corporate attacks originate from inside the company firewall.[2]

New computer viruses and worms are being designed and created everyday. Some are brand new and some are just new variants of old ones, improving on flaws in code with the hopes of the virus being able to be more effective in the wild for a longer period of time then the previous variant.

Corporate networks have malicious and non-malicious types of attacks coming

[1] Gonsalves, Antone. "Corporate Losses From Internet-Based Attacks Average $2M." CRN. 7 July 2004. 13 Jan. 2005 <http://www.crn.com/nl/crndirect/showArticle.jhtml?articleId=22104094>.

[2] Verton, Dan. "Security: IT Lockdowns." Computerworld. 1 Jan. 2002. 13 Jan. 2005 <http://computerworld.com/p100_2002/0,4639,STO66813,00.html>.

at them from multiple angles. Everyday there is a new type of malicious attack created, whether it is a software exploit, a virus, or a worm. Unsecured endpoints are easily exposed to possible theft of important information from the machines hard drive. Controls to mitigate these risks must be in place in order to protect the business core. This is where the importance of Personal Firewalls and Anti-Virus software comes into play. With the high abundance of this software available to us today, it is extremely important to utilize these products.

Many software vendors are now making centrally managed Personal Firewalls and Anti-Virus solutions for the business enterprise environment. With centrally managed Personal Firewall products, security administrators can quickly lockdown on an enterprise wide level, specific ports, protocols, services, and network based applications. Using centrally managed Anti-Virus solutions, security administrators can respond quickly to a virus or worm outbreak, effectively preventing possible major damage to the corporate network.

The extra layers of security that Personal Firewalls and Anti-Virus products provide will add to the depth of the company's overall security architecture and help mitigate many risks and vulnerabilities.

The Business Environment

The term endpoints as it will be used in this paper are defined as company owned desktop personal computers and laptops which connect to corporate networks. Endpoints are popular targets for many attackers looking to exploit vulnerabilities, infect them with some sort of malware or stealing information from the hard drive. Whether they are mobile endpoints or only connecting internally from the network, they have to be prepared to handle numerous threats. Perimeter firewalls and mail server Anti-Virus are very important components in a business network and often times represent the first line of defense. But to achieve a true Defense in Depth model, computer endpoint security needs to be addressed.

Hardware perimeter firewalls should not be expected to stop employee A from snooping in employee B's computer on the internal network. The Firewall ACL would grow so large and become extremely hard to manage or potentially be completely unmanageable in this granular of a design. That same perimeter firewall will most likely not catch the Trojan that is phoning home from employee C's computer through port 80 or 443, which are common open ports on the perimeter firewall for HTTP and HTTPS traffic. When mobile endpoints are using untrusted networks such as the Internet to connect remotely, the perimeter firewall is not expected to completely secure the endpoint from that untrusted network. Mail server Anti-Virus is not expected to catch a virus that employee D downloads from their web based email account onto their company owned computer. Personal Firewalls and Anti-Virus software on the endpoints are how you defense against scenarios like this. If you are serious about properly securing your network, you must add additional layers of security by installing Personal Firewalls and Anti-Virus software on computer endpoints to achieve a true Defense in Depth model.

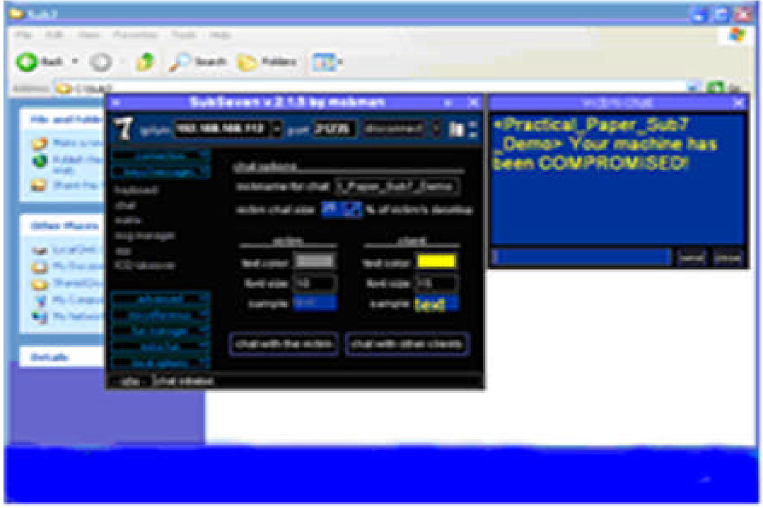
Business Environment: Personal Firewalls

Personal Firewalls take many of the same concepts of hardware firewalls and incorporate them into software which is then installed on computers to provide security. Personal Firewall products are increasingly being developed with more and more security features. Some products have the ability to work at multiple layers of the Open System Interconnection (OSI) model, providing inbound and outbound security controls that have the ability to become very granular and secure.

When a business owned computer is attached to the corporate network from inside the office, it is generally behind the company's hardware perimeter firewall. In most cases this is the first line of defense for endpoints connected internally to the network. If an endpoint is infected with a malicious program such as a backdoor Trojan or a worm that drains the machines resources and phones home to an Internet server, there is a chance that the first line of defense perimeter firewall will not protect against this scenario. It's typical for these types of malicious programs to operate over common popular ports, many of which are necessary for the company's Internet based services to operate, thus the ports are opened on the perimeter firewall, and communication to the internet is allowed. In order to mitigate a risk like this, Personal Firewalls can be installed on the endpoints. This will provide the ability to stop the communication of the malicious program from getting off the endpoint and to its parent server on the internet.

In the following example, in a lab environment I will use the SubSeven Trojan to show how easy it is to compromise an unprotected endpoint without a Personal Firewall installed. I will then show how a Personal Firewall can protect against a malicious program like this. In **Figure 1** on page 5 shows the attacker is using the SubSeven client to control and send chat messages to the SubSeven Server on the victim's infected endpoint.

(Figure 1)

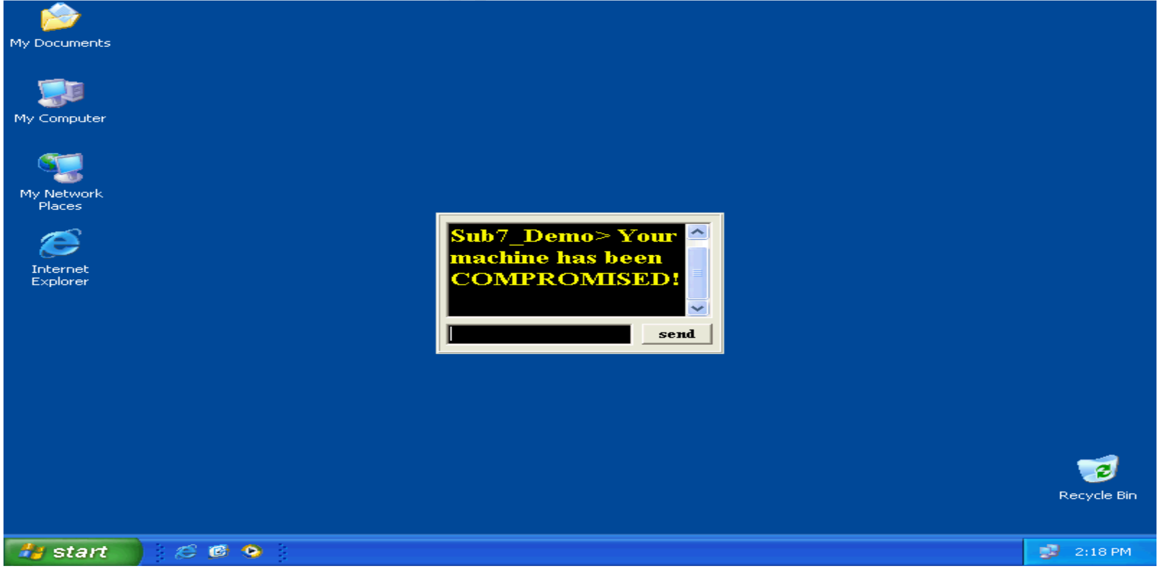


SubSeven v.2.1.5 by mobman

<Practical_Paper_Sub7_Demo> Your machine has been COMPROMISED!

Figure 2 below shows the infected endpoint receiving the message from the attacker. SubSeven allows for several sneaky ways to get the Server executable on the victim's endpoint. It can be disguised as other programs to easily fool someone into executing it. The SubSeven Trojan can even be configured to utilize any port on the endpoint the attacker would like. A common open port on a perimeter firewall could easily be configured in the SubSeven Server. Using Zone Labs ZoneAlarm [3] Personal Firewall, I will show how to stop the SubSeven Trojan in its tracks.

(Figure 2)



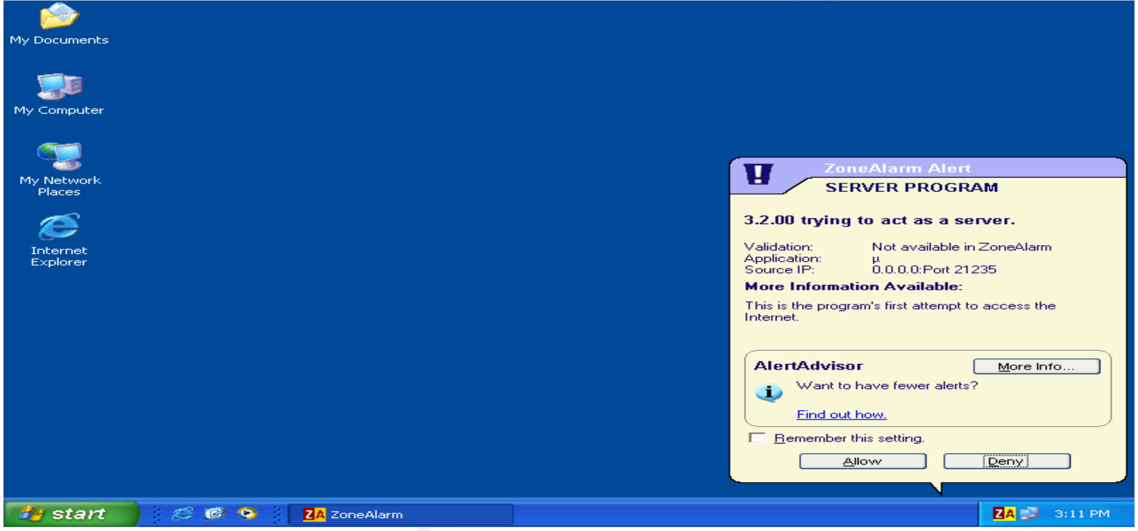
Sub7_Demo> Your machine has been COMPROMISED!

There are a couple of ways for ZoneAlarm to protect against a Trojan like this. If the attacker is on a network that is not trusted by ZoneAlarm, they will not be able to connect to the SubSeven Server on the victim's machine as the stateful

[3] <http://www.zonelabs.com/store/content/catalog/products/sku_list_za.jsp?lid=nav_za> (15 Jan. 2005)

firewall will block this inbound connection from the untrusted network. If the attacker was on a trusted network, like the same corporate network and ZoneAlarm was configured to trust the network or IP of the attacker, the Program Control feature of ZoneAlarm can catch the SubSeven Server on the infected endpoint trying to act as a server and accept connections. The SubSeven server can be configured to notify the attacker once it is ready to accept connections. The Program Control feature of ZoneAlarm will also catch this notification phone home process and give the ability to deny it. **Figure 3** on the next page shows the Program Control feature of ZoneAlarm catching the SubSeven Server trying to accept connections. By denying this connection, the infected user can effectively stop the attacker from communicating with the SubSeven Server.

(Figure 3)



ZoneAlarm Alert

SERVER PROGRAM

3.2.00 trying to act as a server.

Validation: Not available in ZoneAlarm
Application: µ
Source IP: 0.0.0.0:Port 21235

More Information Available:

This is the program's first attempt to access the Internet.

AlertAdvisor

Want to have fewer alerts?

Find out how.

□ Remember this setting.

Being able to provide security against a common threat like a Trojan is a huge plus. Personal Firewalls will provide this security on the endpoint, potentially saving unauthorized access to confidential information and exposure to the corporate network via the endpoint.

There are several scenarios where a Personal Firewall can provide protection and may need to be configured differently. In a business environment, it is important for security administrators to have control over how the Personal Firewall provides protection for their endpoints in these scenarios. Scenarios such as how the Personal Firewall should be configured when connected internally from the office to the internal network and how the Personal Firewall should be configured when the endpoint is connecting to the corporate network via the VPN.

This is where centrally managed Personal Firewall solutions come into play. With a centrally managed product, security administrators can configure the endpoint with a customized policy to fit the given scenario. Security administrators can configure the endpoint to protect against areas where the corporate network is vulnerable, such as little or no outbound traffic control out of the perimeter firewall.

Zone Labs offers their Integrity product [4] which provides enterprise endpoint solutions, with the same granularity of firewall protection as the company's Zone Alarm product.[5] Utilizing this enterprise solution, security administrators can centrally address unsecured endpoints. Unsecured endpoints in a business environment pose a great risk. Eric Ogren, a Sr. Analyst at the Yankee Group says "The weakest link in an enterprise risk management program is unsecured endpoints which expose vulnerabilities to the corporate network and drain IT productivity."[6] Integrity addresses these unsecured endpoints.

By using Personal Firewall products such as Zone Labs Integrity, mobile users connecting from an untrusted network to the corporate network via a VPN will now have firewall protection to secure the endpoint and thus better secure the corporate network from unauthorized access. It's no secret that unprotected mobile endpoint computers connecting to the VPN are increasingly becoming a high security risk to the corporate network. An unprotected PC can get hijacked within minutes of accessing the Internet.[7] If the unprotected endpoint is compromised or infected with a network worm, it is only a matter of time until that compromise or infection is propagated over the corporate network. Integrity features include port stealthing, which hides PC's from crackers looking to slither in a back door, and stateful firewall inspection, which opens ports only to authorized network systems. [8]

Personal Firewalls are increasingly becoming a necessary component to securing endpoints and thus better securing the corporate network. Many company's have security policies in place requiring the use of a Personal Firewall when connecting to the corporate VPN. Utilizing Personal Firewalls such as Integrity, security administrators can satisfy this security policy and provide many features that best meet the security needs of their network and endpoints.

By utilizing the port stealthing features of Integrity, an attacker's job will be that

[4] <http://www.zonelabs.com/store/content/company/corpsales/intOverview.jsp?lid=enthmintps> (21 Jan. 2005)

[5] Gambhir, Sahil. "Zone Labs Integrity 5.0." PCMag. 20 Sept. 2004. 21 Jan. 2005 <http://www.pcmag.com/article2/0,1759,1647643,00.asp>.

[6] Ogren, Eric. "Best-in-Class Security Solution Redefines Enterprise Network Protection with Increased Scalability, Support for 802.1x and security for Instant Messaging." ZoneLabs Press Release 18 Nov. 2003. 21 Jan. 2005 <http://www.zonelabs.com/store/content/company/aboutUs/pressroom/pressReleases/2003/pr_43.jsp>

[7] Acohido, Byron and Jon Swartz. "Unprotected PC's can be hijacked in minutes." USAToday 29 Nov. 2005. 23 Jan. 2005 <http://www.usatoday.com/money/industries/technology/2004-11-29-honeypot_x.htm>

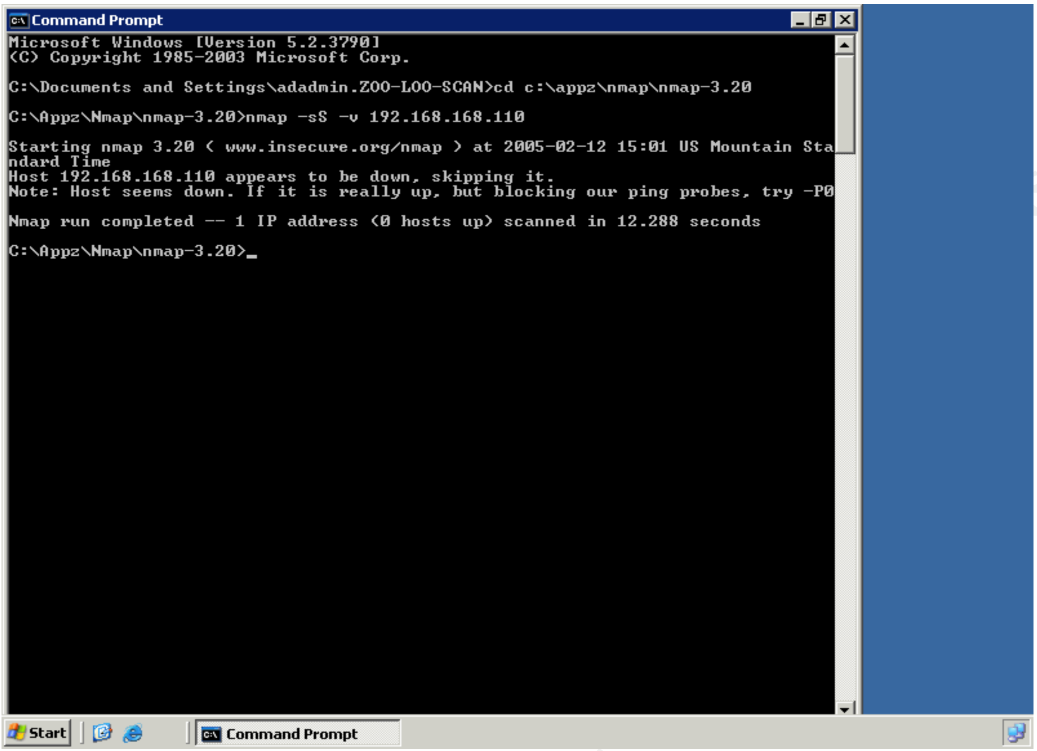
[8] "Security Exclusive: Zone Labs Integrity Burns Brighter." InfoWorld Issue 26 28 June 2004. 3 Feb. 2005 <http://download.zonelabs.com/bin/media/pdf/infoworld_int50.pdf>

much harder because their scan to fingerprint the endpoint can be skewed. Depending on the firewall configuration, the scan can show the endpoint as not online or not connected to the corporate network.

Gaining access or gathering fingerprinting information from a company's endpoint could potentially lead to a successful footprint of the corporate networks security posture. If that happened the attacker would be able to come up with a predetermined way to circumvent existing security controls that may be in place. Personal firewalls can prevent this from happening by securing the endpoint.

Nmap is an open source tool that can be used for security scanning. Information on Nmap can be obtained from http://www.insecure.org/nmap/index.html
In **Figure 4** below, I show a TCP SYN Stealth port scan in verbose mode using Nmap to scan an endpoint machine configured with Zone Labs Integrity Agent. The scan was initiated from a machine that is not defined as trusted in the Integrity Agents policy. As you can see in the Nmap scan results from **Figure 4,** the scan is showing that the machine is down. Integrity effectively prevented the scan from gathering information and the scan results came back as the host seems down. At this point, if the attacker feels the machine may possibly be alive and online, they would need to invest more time and effort into running additional scans to gather more fingerprinting information on this endpoint. Chances are good that the attacker will move onto a less secure machine that will respond to an initial scan. Being able to provide security against the numerous port scans that endpoints are exposed to on the Internet is a huge plus.

(Figure 4)

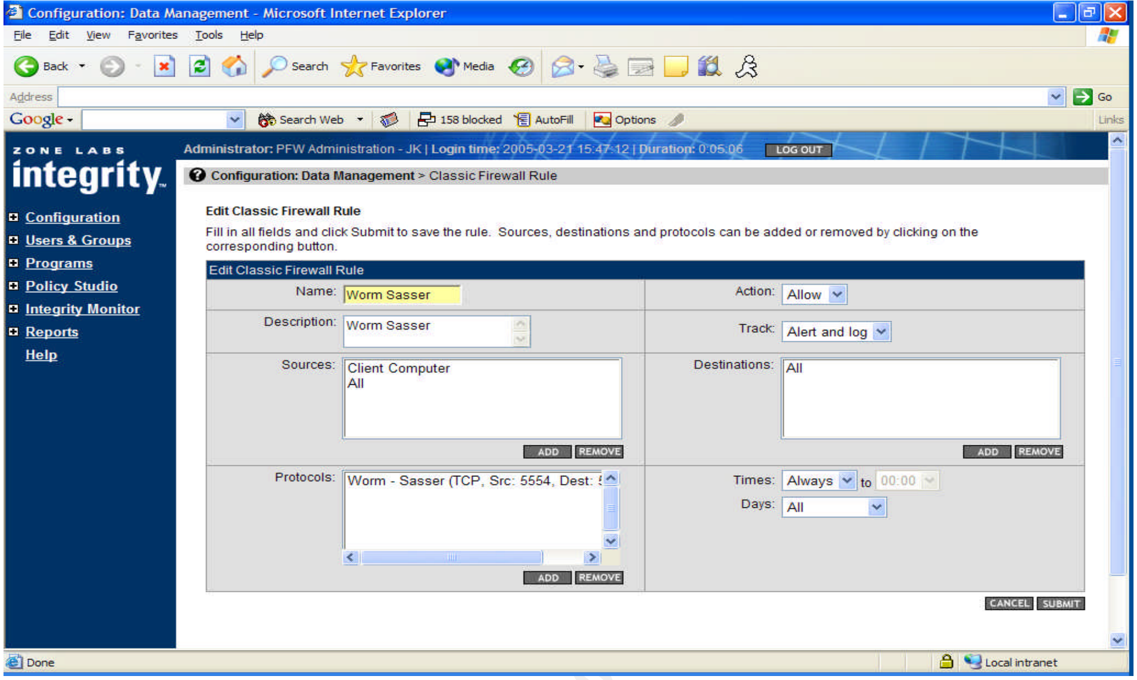


```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\adadmin.ZOO-LOO-SCAN>cd c:\appz\nmap\nmap-3.20

C:\Appz\Nmap\nmap-3.20>nmap -sS -v 192.168.168.110

Starting nmap 3.20 ( www.insecure.org/nmap ) at 2005-02-12 15:01 US Mountain Sta
ndard Time
Host 192.168.168.110 appears to be down, skipping it.
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0

Nmap run completed -- 1 IP address (0 hosts up) scanned in 12.288 seconds

C:\Appz\Nmap\nmap-3.20>_
```

Utilizing a centrally managed Personal Firewall product, security administrators can quickly deploy an enterprise policy to the endpoints, which can lockdown a port or executable that the worm uses in its signature. Being able to lockdown the propagating channel of a worm like this can potentially save the company a lot of money and unwanted media attention from the network being down and not able to provide service customers. **Figure 5** below and **Figure 6** on the following page show just how easy it is to deploy an enterprise policy using Zone Labs Integrity Classic Firewall Rules to effectively stop the Sasser worm in its tracks. Integrity classic firewall (CFW) rules are very similar to access control list rules found on routers and firewall rules from hardware firewalls. CFW rules give administrators the ability to set source/destination rules along with protocol and ports rules. CFW rules can also be applied to network based programs to provide a level of security in how that program accesses the network.

As shown in **Figure 5** below, first a CFW rule must be made in the Integrity administrator console with the appropriate source and destination values you want to apply the CFW rule to. Then add in the appropriate ports and protocols you want the rule to control. In the Sasser worm's case, we will want to use TCP Port 5554. The Action drop down menu box on this rule is set to Block and the Track drop down menu box to Alert and Log. By setting it to Alert and Log, alerts can be generated on the server that provides the ability to effectively log just how hard the network is being hit by this worm. **Figure 6** on page 10 shows the next step to lockdown Sasser which will be to apply the CFW rule to the enterprise policy. By clicking add, you will be able to select the CFW rule created in the first picture. After adding the rule in, simply click Deploy and upon the next client heart beat, the endpoint Integrity client will download the new policy and the rule will be in effect on the endpoint.

(FIGURE 5)


Configuration: Data Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address Go
Google Search Web 158 blocked AutoFill Options
Links
ZONE LABS integrity
Configuration
Users & Groups
Programs
Policy Studio
Integrity Monitor
Reports
Help
LOG OUT
ADD REMOVE
CANCEL SUBMIT
Done
Local intranet

Administrator: PFW Administration - JK | Login time: 2005-03-21 15:47:12 | Duration: 0:05:06

Configuration: Data Management > Classic Firewall Rule

Edit Classic Firewall Rule

Fill in all fields and click Submit to save the rule. Sources, destinations and protocols can be added or removed by clicking on the corresponding button.

Edit Classic Firewall Rule

Name: Worm Sasser

Action: Allow

Description: Worm Sasser

Track: Alert and log

Sources: Client Computer
All

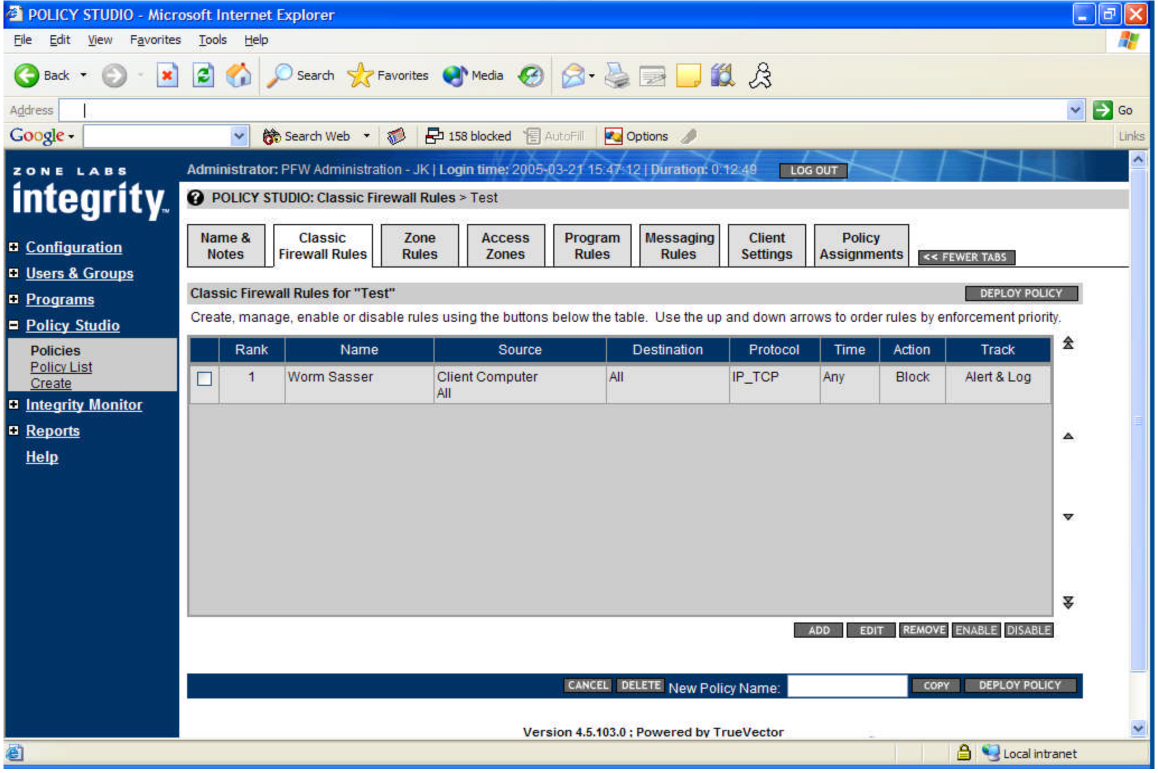
Destinations: All

Protocols: Worm - Sasser (TCP, Src: 5554, Dest: 5

Times: Always to 00:00

Days: All

(FIGURE 6)



Administrator: PFW Administration - JK | Login time: 2005-03-21 15:47:12 | Duration: 0:12:49

POLICY STUDIO: Classic Firewall Rules > Test

Classic Firewall Rules for "Test"

Create, manage, enable or disable rules using the buttons below the table. Use the up and down arrows to order rules by enforcement priority.

	Rank	Name	Source	Destination	Protocol	Time	Action	Track
□	1	Worm Sasser	Client Computer All	All	IP_TCP	Any	Block	Alert & Log

Version 4.5.103.0 ; Powered by TrueVector

Zone Labs Integrity offers multiple firewall clients for the endpoints. These different Personal Firewall clients give security administrators more options in how they want to secure their endpoints.

The Integrity Agent, which is a client with a non-configurable user interface, allows centralized control over endpoint security policies. These policies can be completely transparent to the end users.[9] A client like this can come in handy for users who are not well versed in firewall configurations. With the Integrity Agent being transparent to the end users while providing security to the endpoint, this is a huge plus to a company as the Agent will not interfere in the users daily job functions. Users that are not well versed in firewall configurations will not have the ability to play around and potentially lock themselves out of network resources.

The Integrity Flex client offers a user interface much the same as the commercial ZoneAlarm product from Zone Labs. Users do have the ability to configure the Flex client's personal policy, while at the same time the client can be centrally managed and have enterprise policies deployed to it. Several scenarios to configure the Flex client are possible. Security administrators can make it so the Flex client merges the user's personal policy and enterprise policy together and lets the most restrictive rule setting apply of those policies. It can be configured to have the enterprise policy enforced always, which would disable the users personal policy, or it can be set to allow the personal policy to become active once it is disconnected from the corporate network. By allowing the personal policy to become active once disconnected from the corporate network, this works well with mobile users who may need to configure the firewall to meet their needs while traveling or working from home.

Personal Firewalls allow security administrators not only to protect their endpoints while connected to the Internet or from an untrusted network to the corporate VPN, but also provides security on the internal network. While any reputable Personal Firewall can provide security on the internal network, it is easiest for security administrators to have the ability to centrally manage this process.

With a centrally managed product like Integrity, security administrators can effectively prevent internal malicious attacks or curious snoopers from accessing and browsing other endpoints on the corporate network. Some users may have sensitive information stored on their machine that they are using for a project, or possibly store customer information on their machines for easy access. If this information was compromised it could do damage to the company. The endpoint must also be secured from internal attacks. Security administrators can get very granular with firewall rules and security zone settings on the endpoints. If NetBIOS file sharing traffic is not allowed, a policy can be deployed to block that traffic while on the internal network. If all

[9] "Integrity Product Family." Zonelabs Enterprise Products – Integrity Agent <http://www.zonelabs.com/store/content/company/corpsales/familyOverview.jsp?lid=enthmintprdfam>. (3 Feb 2005.)

communication of endpoint to endpoint on the internal network is not allowed, a policy can be deployed to raise the trusted zone security settings to high, which will hide all machines from each other. Classic firewall rules can be deployed allowing authorized traffic to and from trusted servers so the users can still perform their daily work. If there is a group of users or a whole department that performs sensitive job functions, security administrators can deploy a custom policy to the users to effectively create a bubble network between the group and the rest of the corporate network, stopping attacks or snooping from others on the network. A bubble network is a network or LAN that is isolated from the rest of the corporate network.

Peer to Peer file sharing programs open up a number of big risks to a company. Risks such as possible unauthorized access, data compromise, viruses, worms, and legal liability. These programs are also typically high bandwidth hogs on the corporate network, which can slow down legitimate network needs of other hosts. Orthus Information Security Solutions, in their top ten vulnerabilities list rates file sharing programs as number seven out of ten most often exploited internet system security flaws. [10] On an unprotected endpoint, with some of file sharing programs currently available, attackers can have an uncontested inbound connection to the victim's endpoint. This could potentially be exploited and critical information stored on the endpoints hard drive could be exposed to the attacker. A Personal Firewall could stop an unnecessary inbound connection to the endpoint thus stopping an exploit of the file sharing program installed on the endpoint. Centrally managed firewalls could even go as far as locking out Peer to Peer file sharing programs from running at all by blocking their ports and or executables. This can potentially not only save the company from security risks that the endpoints are exposed to, but also from legal issues in regards to copyright infringement from downloading copyrighted music and movies.

Netcat is a network utility which reads and writes data across network connections, using the TCP/IP protocol.[11] Netcat provides numerous features, including the ability to spawn a process such as a command prompt on a remote machine. Netcat can be set to listen on common open ports to avoid detection by administrators. This can do serious damage if the machine is not secured. Using this popular utility against an endpoint with a Personal Firewall installed can make it quite hard to successfully execute any of the Netcat commands that may be used maliciously to compromise the endpoint.

Many tools available to so called hackers, crackers and script kiddies for reconnaissance, fingerprinting, and compromising of an endpoint can be prevented with Personal Firewalls. Many of these tools provide legitimate purposes for security and network administrators. To ensure the endpoints do

[10] "Top Ten Vulnerabilities" Orthus Information Security Solutions < http://www.orthus.com/ttvuln.html>. (5 Feb. 2005.)

[11] "The GNU Netcat project" Sourceforge.net <http://netcat.sourceforge.net/>. (10 Feb. 2005.)

not fall victim to these tools when used for malicious purposes, it is important to secure the business endpoints with Personal Firewalls.

In a lab environment, I can relatively easily gain access to an unprotected machine using Netcat. I installed Tiny Personal Firewall [12] on the machine and now it is a whole new ballgame. I was unable to connect to the machine any longer with Tiny Personal Firewall running. On the machines console, Tiny recognized the inbound connection attempts. Unless I allowed Netcat to accept connections, I will no longer be able to gain access to this machine using Netcat. It would take a big chunk of time and resources to find a way around this as Tiny is a very secure and powerful Personal Firewall product.

Some Personal Firewalls such as Tiny Personal Firewall gives the ability to generate alerts when a program's MD5 checksum has changed. When an alteration to the program happens, the MD5 checksum will change. This can be a heads up that a program has been potentially infected with some sort of malware. Some viruses, worms and Trojans can alter an installed program with malicious code. The user will continue to run the program without knowing what is actually happening in the background. After installing Microsoft's Service Pack 2 for Windows XP, Tiny Personal Firewall came back to alert me that SVCHOST.exe MD5 has been changed and replaced with a new one. It gave me the ability to allow the new SVCHOST access or deny it. In this case I did allow it as this was a valid change from Service Pack 2 being applied. However, if I did not previously run an update and this was a malicious change, not having a Personal Firewall installed would have potentially opened up a backdoor or given the malicious program the ability to do whatever it was coded to do. This could be countless things. Having the ability to get as granular as checking MD5 checksums is a huge plus for a Personal Firewall product. This can give a heads up that the machine has been infected and or compromised can save the company money from any damage that may be done or information that could potentially be stolen off of the endpoint.

802.11 Wireless Networks are becoming extremely popular. This technology makes it easy to connect computers in a network without the need of running cables. Many businesses are starting to deploy Wireless Local Area Networks (WLAN's) in their offices for the ease and convenience of connecting their endpoints into the network. Unfortunately though, many companies are not thinking through proper security controls to implement a secure WLAN. Hackers using the war-driving practice can sit in the parking lot and access the network via unsecured wireless devices. [13] Many tools are available to help so called

[12] <http://www.tinysoftware.com/home/tiny2?s=5375286922904117117A0&&pg=content05&an=tf6_home> (15 Feb. 2005.)

[13] Hausman, Kirk, Diane Barrett, and Martin Weiss. Security+ Exam Cram
Indiana: Que Publishing, 2003

war-drivers identify a wireless network and potential vulnerabilities of that network. These tools can provide war-drivers access into the network and then other tools can be used to do normal network level hacking to successfully compromise unprotected endpoints on a wireless network. Company owned mobile endpoints may be used to connect to hot spots and other wireless networks such as in hotels or airports in order to gain access to the internet and then the company VPN. Unprotected endpoints connected to a wireless network are open targets will be compromised. Compromising an endpoint on a wireless network can potentially lead the attacker beyond the endpoint and WLAN it is connected to and into the core company network. Securing endpoints on a wireless network require several factors, such as encryption for the data being transmitted through the air. But without having Personal Firewalls on the endpoint, the value of that encryption goes down dramatically. An attacker could gain access to the unprotected endpoint and have access to the data directly from the endpoint rather then using a wireless network sniffer to grab it. Personal Firewalls provide a crucial layer of defense in protecting endpoints connected to the wireless network. Attackers will often move on or drive onto easier targets when they are faced with endpoints having firewalls enabled. Chances are they will easily be able to find another target that is unprotected relatively quickly.

Exploits in computer software and Operating Systems are very common. These exploits could allow attackers to execute code remotely on an endpoint and have complete remote control of the machine. Known exploits will sometimes lead to worms coded specifically to take advantage of the exploit. It is important to keep both installed software and Operating Systems up to date with the appropriate patches, hot fixes and services packs. It is also important to have a Personal Firewall installed to have the ability to mitigate some of these exploits before patches are released. By the Personal Firewall blocking unsolicited inbound requests and recognizing outbound access attempts, the chance for the flaw to be exploited are mitigated. If the machine happened to be infected by a worm taking advantage of the exploit, the outbound traffic controls of the Personal Firewall product could generate an alert when the worms tries to propagate outbound to the next victim and provide the ability to deny outbound access. This is an important feature of Personal Firewalls that can potentially save a great deal of money to the company in that they would be able to more effectively keep a worm outbreak under control on the network. Imagine having a large network with several thousand endpoint computers and having to fight a powerful network worm taking advantage of a zero day exploit that is propagating extremely quickly across the network. Having a mitigating control like a Personal Firewall in place to stop this before causing extreme damage is an absolutely huge positive.

Microsoft now offers a built in Firewall for some of their Operating System products. Microsoft has turned on the built in firewall by default in Service Pack 2 for Windows XP. [14] By Microsoft doing this, it is just another reminder how of crucial utilizing Personal Firewalls to secure endpoints. Microsoft's Windows Firewall can be turned on for any network connection on the endpoint with just a few clicks of the mouse. It only offers inbound protection, so there are still risks such as a malicious program phoning home could get off the endpoint and to the internet. However, some protection is better then none. In an Active Directory environment, Administrators can control the built in Windows Firewall settings through Group Policy. [15] Wireless users can very easily turn on the firewall to provide a crucial layer of security for the endpoint connected to the WLAN. Or security administrators can enable the firewall and configure it as needed through Group Policy settings. It is a move in the right direction by Microsoft and will provide users who are not well versed in firewall configuration some level of protection that can defense against numerous inbound attacks. In my testing with Microsoft's Windows Firewall against common inbound access attempts, it faired well. I believe Microsoft's built in firewall to be adequate protection against most common inbound access attempts.

If a company's only firewall is the perimeter firewall, what happens if that firewall is compromised? The attacker could potentially have uncontested access to all endpoints on the network. Eventually security administrators will be tipped off of the compromise of the perimeter firewall, either by reviewing logs or possibly when the vendor releases a patch for vulnerability and upon reviewing what the patch fixes; you discover you have been exploited. At this point even though the exploited vulnerability has been secured preventing the attacker using it for access again, chances are the attacker has been able to compromise several endpoints. The attacker could potentially infect them with a backdoor that could still allow access back into the network, through an alternate means of how they originally gained access. By having a second line of defense with a Personal Firewall which adds to the Defense in Depth security model, the risk of something like this from happening is mitigated.

In today's world, the ability for users to quickly access information is imperative. Many computer endpoints in the business environment today are storing sensitive information such as customer information or company initiatives directly on the endpoints hard drive, enabling for fast access to users or access while not connected to the network. On top of this, many of these computers are used by remote users with the need to have a mobile endpoint such as a laptop. These machines typically connect to untrusted networks in order to gain access into the company VPN. Information Security is often times overlooked in this scenario of unprotected laptops storing sensitive information and connecting their machines to untrusted networks. An unprotected endpoint with sensitive information stored on it being compromised and having the information virtually

[14] "Some programs seem to stop working after you install Windows XP Service Pack 2." Microsoft Knowledge Base. <http://support.microsoft.com/kb/842242>. (11 Feb. 2005.)

[15] "Managing Windows XP Service Pack 2 Features Using Group Policy" Microsoft Technet. 1 Aug. 2004. 15 Feb. 2005 <http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/mangxpsp2/mngwfw.mspx>.

stolen from the machine is the equivalent to having the endpoint physically stolen. Other issues are that the information could be altered or deleted by an attacker. Stopping and thinking about having the sensitive information potentially stolen, altered or deleted, what is really happening are all three aspects of the information security bedrock principles: Confidentiality, Integrity, and Availability [16] have the ability to easily be compromised in this situation. California law now requires companies to notify customers if their personal information has been stolen. This notification to customers along with breaching any or all of the Confidentiality, Integrity, and Availability principles of Information Security has the makings to be extremely costly to a business. A way to greatly mitigate against this from happening is the use of Personal Firewalls on the endpoints. Personal Firewalls will provide the layer of defense that can deter unauthorized access to an endpoints and potential breaching of the Confidentiality, Integrity, and Availability of the information stored on the endpoint.

Most Personal Firewalls offer many features and configuration options to secure endpoints and add another crucial layer of defense to a company's overall Defense in Depth model. After assessing the network for risk and vulnerabilities, Personal Firewalls can be used to effectively mitigate those risks and vulnerabilities to an acceptable level, making your corporate network that much more secure. By having Personal Firewalls on the endpoints, the perimeter firewall is not the only means of firewall protection for the endpoints on the network.

Aside from the Personal Firewalls written about in this paper, there are a few other products that I have found to provide solid security features that can mitigate against the attacks and vulnerabilities that I have described in this paper. These products will also effectively add to the Defense in Depth model of the corporate network. Sygate offers both centrally managed enterprise solution and user managed Personal Firewall products.
Sygate Secure Enterprise product can be found at:
http://www.sygate.com/products/sygate-secure-enterprise.htm
The Sygate Personal Firewall Pro product can be found at:
http://www.sygate.com/products/sygate-personal-firewall-pro.htm
Kerio Personal Firewall product can be found at:
http://www.kerio.com/kpf_home.html

There are numerous websites that allow you to run Personal Firewall security tests. Some of these tests could show if one product performed better in an area in which the corporate endpoints are most vulnerable, but the other product you are testing does not perform as well in securing this area. These tests could help decide which product best meets the endpoints and network security needs. Since some of these sites test the Personal Firewalls ability to catch outbound access attempts, Microsoft's Windows Firewall may not fair well on a

[16] SANS Institute. Track 1 – Security Essentials Volume 1.2. SANS Press, November 2004.

test. Some sites you could use to help you decide which product best meets the security needs of your organization are:
https://secure1.securityspace.com/sspace/index.html
http://www.pcflank.com/about.htm
http://scan.sygatetech.com/
https://grc.com/x/ne.dll?bh0bkyd2

Business Environment: Anti-Virus

There are dozens of reputable mail server Anti-Virus products out there that get the job done. Administrators can do a great job using these products to prevent viruses and worms from propagating through their corporate email system and onto endpoint user's machines. But there are a number of other transmission vectors a virus or worm can take to infect the endpoint. Anti-Virus software installed on the endpoints provides security against these other transmission vectors, enabling another line of defense on the endpoints and contributing to the overall Defense in Depth model of the company's security architecture.

Web based email services give the users the ability to open a web browser, go to URL on the internet and have full access to their personal email through the web browser interface. Unless the endpoint is configured with Anti-Virus software, the potential for virus or worm infestation on your network is very high with users being able to access these web based services. Many companies employ security policies against users accessing web based email services from company owned machines or while connected to the corporate network. However that does not always stop all users from violating company policy and accessing the services anyway. It is possible to block domain names on the perimeter firewalls or proxy servers to prevent access to the services, however with new web based email services popping up seemingly daily, and just about every ISP offering web based access it would take full time employees to investigate these domains and set rules to block access to them. Most companies do not have the resources and funding to do this.

When security administrators have their mail server Anti-Virus configured correctly and with the most up to date virus definition files, it will block known viruses at the email gateway entry point preventing them from being delivered to users mailboxes. For proactive security reasons, some businesses will even flat out block all email attachments inbound from the Internet with the exception of common business file extensions such as .doc, .xls, and .ppt. In this scenario, a user who wants to see a video clip or get a music file from their friend to help pass the time while at work will not be able to have it emailed to their work email mailbox. When this happens, a user will most likely search for alternate means of being able to get those files. They will likely turn to a web based email service where they can have the file sent to an account and then easily download it to their machine. It's possible the file from their friend is legitimate, and it is also possible it contains a hidden virus. These email inboxes are usually full of SPAM and emails with attachments, often containing viruses. Oftentimes users will be curious about other attachments from emails in their inbox. If the machine is not protected with Anti-Virus, the user will be infected. Depending on the virus or the worm that was contained in the attachment, there is a high chance the virus or worm will propagate to other machines on the network. If the endpoint has Anti-Virus installed on it, it can prevent an infection in this scenario.

Instant Messaging (IM) is becoming an increasingly popular vector for computer viruses and worms to be transmitted. While email is still the primary vehicle for viruses and worms, the fact that IM is a real-time communication technology makes it a dangerous threat. [17] It is an easy task to transmit a virus or worm via IM. A few clicks of the mouse and it is sent off to a friend on the other end of the IM chat service. Viruses and worms have the ability to do many different actions. The developers are often sneaky in the means of disguising the virus or worm. Companion Viruses can attach itself to legitimate programs and create different file extensions. [18] When the victim executes the file, the virus or worm will then infect the endpoint. Many users are tricked into this type of transmission vector think they are receiving a legitimate file from a friend or coworker. It is possible the friend or coworker is acting maliciously and purposely sending it and it is also possible they are on a computer without Anti-Virus and unknowingly sent the virus thinking it was a legitimate file. None the less, if Anti-Virus software was installed on the endpoints, chances are the virus or worm would be deleted or quarantined, which would stop it from spreading and causing productivity issues on the endpoint and possibly the corporate network.

In a growing number of cases, viruses have started using instant messaging as a supplement to other channels of infection, like email. [19] Anti-Virus vendors are catching onto this though and doing the necessary things to make sure Anti-Virus software will play a role in protecting against the Instant Messaging transmission vector.

Peer to Peer file sharing programs which are extremely popular with internet users are fertile grounds for transmission of viruses and worms. Like web based email services, there are countless Peer to Peer file sharing programs available on the internet. These programs create new risks which can cause damage to endpoints and corporate networks. Many companies employ security policies against using these programs on their endpoints and networks. As most know this will not stop everyone. There will always be a number of users who utilize these programs regardless of company policy. It's not uncommon for someone to download a file such as a MP3 from a file sharing network thinking they are

[17] Moore, Cathleen "IM viruses: The next big threat?" Infoworld. 11 Feb. 2005. 21 Feb. 2005 <http://www.infoworld.com/article/05/02/11/HNimvirus_1.html>.

[18] Pastore, Mike and Emmett Dulaney. Security+ Study Guide Second Edition California: Sybex Inc., 2004

[19] Saunders, Christopher "Report: IM Viruses on the Rise." instantmessagingplanet. 1 Oct. 2003. 23 Feb. 2005 <http://www.instantmessagingplanet.com/security/article.php/3086291>.

only getting a MP3 they wanted. But what they are really downloading is a virus. Like IM, many viruses are now being created to directly target Peer to Peer file sharing programs. A search on most any known music artist on a file sharing network will turn up hundreds to thousands of results. The likely hood for hidden viruses or worms transmitting is very high over Peer to Peer file sharing networks.

With Peer to Peer file sharing, the transmission of virus and worms is like a domino effect. One person will download the virus or worm thinking it is a legitimate file, and then they will share it out for others to download from them and so on and so forth. The dominos continue to fall, and the virus and worms continue to travel to new hosts to infect. There will always be a handful of users that try to use Peer to Peer file sharing services. If just one virus or worm is downloaded from there, it can spell disaster for the network if the other machines are also unprotected without Anti-Virus. Mitigating the risks and vulnerabilities of virus and worm transmission through Peer to Peer file sharing programs can be achieved by using Anti-Virus software.

Physical media such as CD's, Floppy disks, and Flash drives are also ways for virus and worm to be transmitted. It's common for a user to carry some sort of media with them so they can have access to their files while at another computer. While at home, a user could download a virus from a Peer to Peer file sharing program or an illegal software download site thinking they are getting a legitimate file and then save it to their flash drive or other media and bring it back into the office. If the endpoint computer does not have Anti-Virus installed, when the user executes the file, the endpoint will become infected. Physical media is oftentimes passed around or shared. The chances of someone encountering a virus or worm on an unprotected machine are very high. If the virus or worm is copied to the physical media, and then given back to someone else in the company to copy the file onto their machine, they will become infected also. Having a layer of defense in Anti-Virus on the endpoint will provide security against an infection over a transmission vector like physical media.

With so many transmission vectors available today for computer viruses and worms, it is important to have all bases covered. Above I described several ways of virus and worm transmission. By having Anti-Virus installed on the endpoint, you will have the ability to mitigate against endpoints being infected by those transmission vectors. If there is no Anti-Virus installed, viruses and worms have the ability to cause serious damage that will likely result in a dollar loss to the company.

In a lab test environment, on a machine using Grisoft's AVG Network Edition Anti-Virus [20] and Trend Micro's PC-Cillin products[21], I tried to infect the test machine with the SubSeven Trojan. Both AVG and PC-Cillin detected and deleted it very quickly. If the machine was not protected by Anti-Virus, it would

[20] <http://www.grisoft.com/us/us_avg_ml.php> (25 Feb. 2005)

[21] <http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/overview.htm> (25 Feb. 2005)

be compromised with a backdoor, and the attacker would have numerous features at their fingertips as to how they want to control the SubSeven Trojan server on the infected machine. My personal email account generally gets numerous SPAM emails with viruses included as attachments sent to it. I saved one of the attachments that PC-Cillin informed me was the vbs.loveletter.var virus to the hard drive of another test machine with AVG Anti-Virus installed. On this machine I tried to infect it with the vbs.loveletter.var virus that was sent to my inbox. The AVG Anti-Virus recognized this and deleted it very quickly. Without Anti-Virus, my test machines would be infected with a backdoor in SubSeven and a mass emailing worm in vbs.loveletter.var. In a business environment, this could cause a huge impact. An attacker will have many options at their fingertips using the SubSeven Trojan. If the machine is unprotected, the attacker will essentially have full control over the endpoint. Even though the company mail servers have Anti-Virus installed, they could potentially be overloaded with an uncontrollable load of email attempts from the infected endpoints, which could result in a denial of service. Email is an important key to many businesses in this day and age. A company's Email infrastructure must be protected. Not having Email service online could potentially be devastating to a company. Having Anti-Virus installed on the endpoints will provide a layer of defense and provide security for the endpoints and company's email infrastructure.

Anti-Virus is such an important piece of securing endpoints and adding to the Defense in Depth model that Bank of America is now recommending all clients that use their Online Banking services to have Anti-Virus installed. A businessman who banks with Bank of America has sued them for negligence in not alerting him about the existence of Coreflood, which is a form of Trojan horse that opened a back door to his machine and allowed an attacker to transfer $90,000 to a bank account in Latvia. [22] If the user would have had Anti-Virus installed, it would have caught this Trojan, preventing the attacker from gaining access and transferring the money. This type of scenario is what businesses face when securing their endpoints. There are so many different Trojans, viruses, and worms out there that are targeting them. The potential for a compromise is extremely high should the endpoints not be secured with Anti-Virus. In a business environment, should an endpoint have been infected like the machine of Bank of America's customer, the attacker in control of that endpoint could potentially have access into the corporate network and retrieve highly classified information ranging from bank and financial records to company confidential and restricted information. By using Anti-Virus which adds a layer of defense on the machine, the chances of this type of attack to compromise the endpoint with a Trojan is mitigated.

An unprotected endpoint is likely to become a zombie. A zombie computer is a

[22] Marlin, Steven "Bank of America to Install Encryption Software." Informationweek. 18 Feb. 2005. 23 Feb. 2005 <http://www.informationweek.com/showArticle.jhtml?articleID=60402074>.

computer that has been compromised and infected so it can be used for malicious purposes. It's common for zombie computers to be infected with worms that will propagate to other machines. It is possible for the worms to be coded to launch an attack on an Internet site or server on the same day, causing a Distributed Denial of Service (DDoS) attack. By having numerous computers attacking the internet site or server, it makes it harder to stop the attack because the attack is being launched from multiple machines across the globe. An example of this would be the Blaster worm which targeted Microsoft's Windows update site. The target Internet site or server will not be the only one who feels the negative impact from the DDoS attack. The company's network bandwidth is going to take a hit also, which can potentially cause some sort of Denial of Service attack on the company network as well as the Internet site or server the worm is targeted to attack.

Zombie computers are growing at a huge rate. Some sources have put the number of zombie PC's operating worldwide as high as two million. [23] Many zombie PC's are infected with viruses and worms that have their own built in Simple Mail Transport (SMTP) engines which will provide a means for the virus or worm to spread via email. Unless the machine is secured, chances are other attackers will start using the machine for malicious purposes also. Many attackers are installing SMTP engines on zombies to use them to SPAM email boxes across the world allowing the attackers to remain anonymous as the SPAM is not tracked back to them. Infected zombies in a business environment will create havoc on the company network. Due to the loads of SMTP email being sent outbound from the zombie machines to the network gateway, there will be network latency or possibly Denial of Service conditions being felt on the company's network from this high load of traffic. Having Anti-Virus installed on these machines would be able to stop these machines from being infected in the first place and becoming zombies.

IRC bots are also growing in at a huge rate. IRC bots are similar to zombie machines, but the machine is remotely controlled by the attacker via an IRC channel. Attackers often have numerous bots in their control creating botnets. A botnet is a group of machines that an attacker has access to and can remotely control each of them. [24] These botnets are often times used for creating a DDoS against an internet site or server. Having updated Anti-Virus software on endpoints can prevent the machine from having any malicious software installed on it, potentially making the endpoint into a bot, or IRC bot.

Many Anti-Virus vendors are now offering centrally managed products. There is great need for security administrators to be able to control the risk of viruses and worms on their endpoints and networks.

[23] Tynan, Daniel "Zombie PCs: Silent, Growing Threat." PCworld. 09 July 2004. 25 Feb. 2005 < http://www.pcworld.com/news/article/0,aid,116841,00.asp>.

[24] "Know your enemy: Tracking Botnets." Honeynet.org < http://www.honeynet.org/papers/bots/> 13 Mar. 2005 20 Mar. 2005

Symantec offers its AntiVirus Corporate Edition[25], which gives administrators numerous features and the ability to centrally manage the Anti-Virus client on the endpoint. Symantec System Center enables centralized configuration, deployment, policy management, and reporting, and allows administrators to audit the network to determine which nodes are vulnerable to virus attacks. [26] Administrators can keep virus definition files up to date rather then relying on the user to update their Anti-Virus software.
Infected clients are cleaned quickly and efficiently via an on-demand, enterprise-wide virus sweeps initiated from the centralized console. [27]

Having the ability to quickly respond to a new virus or worm outbreak is crucial to a networks stability and performance. Using Symantec System Center, administrators can force a Live Update to occur immediately on single or multiple clients, minimizing the response time to fast spreading threats. [28] Having Anti-Virus software installed on all endpoints is a key piece in providing overall network security. Nimda, Code Red, SQL Slammer, and the Melissa viruses are all examples of showing why it is important to have Anti-Virus software installed and the ability to centrally manage the Anti-Virus client on the endpoints. These viruses caused havoc on countless networks across the world. By having a centrally managed Anti-Virus product, security administrators could quickly keep a virus outbreak under control by deploying updated virus definition files.

Centrally managed Anti-Virus products bring a lot to the table in adding another layer of security to the corporate networks defense in depth model. The features of a product like Symantec AntiVirus Corporate Edition would allow security administrators to better mitigate and control an outbreak such as Nimda, Code Red and the Melissa viruses.

Computer viruses and worms can cause serious problems for a business. If a corporate owned endpoint is infected with a virus or worm, it can cause loss of productivity for the user who uses the infected machine. The cost of having a technician re-image the unprotected infected machines can become a huge expense to a company. If the virus or worm is able to propagate across the network, there is potential for serious damage to the corporate network which can result in a high dollar loss. Utilizing Anti-Virus software on the endpoint can save a lot of time, headaches, and dollars by catching viruses and worms before the damage is done to the endpoints and the corporate network. Computer

[25] <http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155> (20 Feb. 2005)
[26] "Symantec AntiVirus Corporate Edition." Symantec Enterprise Security. <http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155>. (21 Feb. 2005.)
[27] Laity, Chad "SYMANTEC ANTIVIRUS CORPORATE EDITION V8.1." ccmagazine. 29 Mar. 2004 25 Feb. 2005 <http://ccmagazine.com/Reviews/ReviewDetails.asp?ID=540>.
[28] "Symantec AntiVirus Corporate Edition." Symantec Enterprise Security. <http://enterprisesecurity.symantec.com/content/displaypdf.cfm?pdfid=276&EID=0>. (22 Feb. 2005)

viruses and worms must be taken seriously and as a risk to the company. Providing Anti-Virus to mitigate the risk is extremely important. Without it, you are opening up your business for extreme challenges and financial loss.

The goal of many network administrators is to have a 99-100% up time. Without having Anti-Virus on endpoints in the network, this goal will not be obtained. Viruses and worms have the ability to knock an unprotected network out for days, and potentially weeks. The cost of having the network down for this period of time could be devastating to a business. On top of having the financial loss of the network being down, there will be costs in the cleanup effort. Help desks will be swamped with calls, and technicians will be backed up with using removal tools to repair the endpoints or perhaps having to reimage the machine depending on the damage the infection caused. The potential for an amazingly high total of financial loss is possible from some viruses and worms. Computer Economics reported the total economic cost for the Code Red and Code Red II to be more then $2 Billion. [29] This is an absolutely scary damage cost figure. Having mitigating controls in place to protect against a loss of this magnitude is extremely important to a business. If a larger percentage of computers across the globe utilized Anti-Virus software, I would estimate the economic cost of this virus to be much less. Unfortunately as virus designers become more knowledgeable and more vulnerabilities are found, there will be viruses and worms designed that will have the ability to be even more damaging then a $2 Billion dollar loss economic cost. With security administrators realizing the need to have a layer of defense in Anti-Virus on their endpoints, the chances for a damage loss to the company is greatly reduced.

Anti-Virus on endpoints provides another layer of defense against a clear and present risk of viruses and worms. It will provide protection in areas that another layer will not. As shown in this paper, there are numerous transmission vectors a virus or worm can be spread through, all which are present in the majority of businesses today. When a transmission vector like this is utilized, Anti-Virus on the endpoint can effectively stop the initial infection and potential propagation and dollar loss. Endpoints are the primary target for virus and worm infection on a corporate network. By having Anti-Virus installed on the endpoints, the most crucial base in defending against viruses and worms is covered and a layer of defense is added to the Defense in Depth model of the businesses network overall network security architecture.

There are several reputable Anti-Virus software vendors. Besides the ones mentioned in this paper, others that I have found to offer a good product in that it is easy to work with and can detect numerous types of viruses and worms are:
McAfee:
http://www.mcafee.com

[29] Delong, Daniel F. "Code Red Virus Most Expensive in History of Internet." NewsFactor. 9 Aug. 2001 25 Feb. 2005
<http://www.newsfactor.com/perl/story/12668.html#story-start>.

Computer Associates:
http://ca.com/

Trend Micro also offers House Call, which is a solid online Anti-Virus scanner. By going to the URL, through a web browser you can scan a machine for viruses and worms. This can come in handy if a Retrovirus, which attacks or bypasses the Anti-Virus installed on a computer, [30] has infected a machine and caused the installed Anti-Virus product to become inoperable. House Call can be found here:
http://housecall.trendmicro.com/

Conclusion

A Defense in Depth model is the best way to approach securing a network. Defense in Depth is often represented by an example of an onion. An onion is composed of multiple layers. In order to get down to the core, multiple layers would have to be penetrated. A layered design like this should be incorporated into the design of the company's network security architecture. The more layers that are created, the harder it would be for an attacker or for worm to penetrate the core. This core could represent many things, but ultimately it is the critical assets that the company wants to protect and guard most from the outside.

Perimeter firewalls and mail server Anti-Virus also provide very important layers of protection for the core. But if these layers of protection can be circumvented by attacking or infecting an unprotected endpoint, their value is not as high as it would be if they had additional layers of protection to fall back on. Personal Firewalls and Anti-Virus add crucial layers of protection, thus creating Defense in Depth. Having perimeter firewalls and mail server Anti-Virus for protection at the perimeter point, and then more layers of security on the endpoints, you achieve a model that makes an attack harder to execute. Unprotected endpoints are the downfall to many organizations in terms of their security architecture. Since perimeter firewalls and mail server Anti-Virus are such important layers of protection for the company, you should also think in the terms that their mini versions, Personal Firewalls and Anti-Virus are also just as important to secure the endpoints of the network. If an attacker targeting endpoints bypasses the perimeter firewall layer of defense, and then hits another layer of defense in the Personal Firewall, this is depth that can ultimately prevent an attack. The same holds true with Anti-Virus. If a virus or worm is targeted for endpoints but can not get in through the company mail servers and other transmission vectors they may take, the next layer of defense, endpoint Anti-Virus is there to provide protection.

Utilizing Personal Firewalls and Anti-Virus together create a somewhat synergistic affect in that they work well together to improve endpoint security. If one were missing, the less secure the endpoint would be and potentially the

[30] Pastore, Mike and Emmett Dulaney. Security+ Study Guide Second Edition California: Sybex, Inc., 2004

less secure the network would be. Where one product might have a weakness, the other may have the ability to provide security to make up for it. An example of this would be a network worm or a zero day exploit, where the Software vendor has not yet been able to release a patch or in the case of a worm, the Anti-Virus vendors that have not yet of released a virus definition file that can protect against this. But if the endpoint has a Personal Firewall installed on the machine, it could potentially stop the propagation of this worm by providing the ability to prevent unauthorized outbound access and also the ability to lockdown an executable or file that the worms uses as part of it's signature. Another example would be if a virus or worm were developed to specifically attack a Personal Firewall. By having Anti-Virus installed, this virus or worm could be detected and prevented from attacking the installed Personal Firewall. An example of a worm that was created to take advantage of software firewalls is the witty worm. This worm targeted several firewall products and did some damage. Taking away one layer, either the Personal Firewall or the Anti-Virus protection will take away from the overall Defense in Depth model, making your endpoints and network more vulnerable.

The phrase "more is better" is especially true in the context of a Defense in Depth model for the overall network security architecture of a business environment. When an attacker targets a specific area of a network for an exploit, and finds this area to be properly secured, they will most likely move onto another area. The next area they move onto should also have a layer of protection and so on and so forth. At some point in the process the endpoints will be targeted. The need for layers of protection on the endpoint is extremely high. When the endpoints are secured with Personal Firewalls and Anti-Virus software, they contribute to the Defense in Depth model, protecting the business core. Imagine an attacker having to work past layers of security at level. If every level in the network is secured, the chances to catch or prevent an attack skyrocket. Endpoints are an important level that is often times most vulnerable to an attack. Not having the endpoints secured makes an attack all that much easier.

A business that secures their endpoints with Personal Firewalls and Anti-Virus software should look at these products as an investment to the company. These products have the ability to greatly reduce and mitigate many risk and vulnerabilities that could potentially lead to high dollar losses and disruption of the service the business provides. By having these mitigating controls in place, the business has a significantly better opportunity to continue doing its business without the major impact they would be facing if they did not have Personal Firewalls and Anti-Virus on their endpoints. This is the importance of Personal Firewalls and Anti-Virus in the business environment.

In this paper I have explained and showed several risks and vulnerabilities that unprotected endpoints are exposed to. I showed how Personal Firewalls and Anti-Virus software can effectively mitigate these risks and vulnerabilities thus showing the importance of using them in the business environment. Unfortunately there are countless other risks and vulnerabilities in the wild that were not documented in this paper. The good news though, is that there are products to help prevent your business from becoming a victim. Those products are Personal Firewalls and Anti-Virus software.

List of References

Gonsalves, Antone. "Corporate Losses From Internet-Based Attacks Average $2M." CRN. 7 July 2004. 13 Jan. 2005 <http://www.crn.com/nl/crndirect/showArticle.jhtml?articleId=22104094>.

Verton, Dan. "Security: IT Lockdowns." Computerworld. 1 Jan. 2002. 13 Jan. 2005 <http://computerworld.com/p100_2002/0,4639,STO66813,00.html>.

<http://www.zonelabs.com/store/content/catalog/products/sku_list_za.jsp?lid=nav_za>. (15 Jan. 2005)

<http://www.zonelabs.com/store/content/company/corpsales/intOverview.jsp?lid=enthmintps>. (21 Jan. 2005)

Gambhir, Sahil. "Zone Labs Integrity 5.0." PCMag. 20 Sept. 2004. 21 Jan. 2005 <http://www.pcmag.com/article2/0,1759,1647643,00.asp>.

Ogren, Eric. "Best-in-Class Security Solution Redefines Enterprise Network Protection with Increased Scalability, Support for 802.1x and security for Instant Messaging." ZoneLabs Press Release

18 Nov. 2003. 21 Jan. 2005
<http://www.zonelabs.com/store/content/company/aboutUs/pressroom/pressReleases/2003/pr_43.jsp>.

Acohido, Byron and Jon Swartz. “Unprotected PC’s can be hijacked in minutes.” USAToday
29 Nov. 2005. 23 Jan. 2005
<http://www.usatoday.com/money/industries/technology/2004-11-29-honeypot_x.htm>.

“Security Exclusive: Zone Labs Integrity Burns Brighter.” InfoWorld Issue 26 28 June 2004. 3 Feb. 2005
<http://download.zonelabs.com/bin/media/pdf/infoworld_int50.pdf>.

“Integrity Product Family.” Zonelabs Enterprise Products – Integrity Agent
<http://www.zonelabs.com/store/content/company/corpsales/familyOverview.jsp?lid=enthmintprdfam>. (3 Feb 2005.)

“Top Ten Vulnerabilities” Orthus Information Security Solutions
< http://www.orthus.com/ttvuln.html>. (5 Feb. 2005.)

“The GNU Netcat project” Sourceforge.net
<http://netcat.sourceforge.net/>. (10 Feb. 2005.)

<http://www.tinysoftware.com/home/tiny2?s=5375286922904117117A0&&pg=content05&an=tf6_home>. (15 Feb. 2005.)

Hausman, Kirk, Diane Barrett, and Martin Weiss. Security+ Exam Cram
Indiana: Que Publishing, 2003

“Some programs seem to stop working after you install Windows XP Service Pack 2.” Microsoft Knowledge Base. <http://support.microsoft.com/kb/842242>. (11 Feb. 2005.)

“Managing Windows XP Service Pack 2 Features Using Group Policy” Microsoft Technet. 1 Aug. 2004. 15 Feb. 2005
<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/mangxpsp2/mngwfw.mspx>.

SANS Institute. Track 1 – Security Essentials Volume 1.2. SANS Press, November 2004.

Moore, Cathleen “IM viruses: The next big threat?” Infoworld. 11 Feb. 2005. 21 Feb. 2005
<http://www.infoworld.com/article/05/02/11/HNimvirus_1.html>.

Pastore, Mike and Emmett Dulaney. Security+ Study Guide Second Edition
California: Sybex Inc., 2004

Saunders, Christopher "Report: IM Viruses on the Rise."
instantmessagingplanet. 1 Oct. 2003. 23 Feb. 2005
<http://www.instantmessagingplanet.com/security/article.php/3086291>.

<http://www.grisoft.com/us/us_avg_ml.php>. (25 Feb. 2005)

<http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/overview.htm>. (25 Feb. 2005)

Marlin, Steven "Bank of America to Install Encryption Software."
Informationweek. 18 Feb. 2005. 23 Feb. 2005
<http://www.informationweek.com/showArticle.jhtml?articleID=60402074>.

Tynan, Daniel "Zombie PCs: Silent, Growing Threat." PCworld. 09 July 2004. 25 Feb. 2005
< http://www.pcworld.com/news/article/0,aid,116841,00.asp>.

"Know your enemy: Tracking Botnets." Honeynet.org
<http://www.honeynet.org/papers/bots/>. 13 Mar. 2005 20 Mar. 2005
<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155>. (20 Feb. 2005)

"Symantec AntiVirus Corporate Edition." Symantec Enterprise Security.
<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155>. (21 Feb. 2005.)

Laity, Chad "SYMANTEC ANTIVIRUS CORPORATE EDITION V8.1."
ccmagazine. 29 Mar. 2004 25 Feb. 2005
<http://ccmagazine.com/Reviews/ReviewDetails.asp?ID=540>.

"Symantec AntiVirus Corporate Edition." Symantec Enterprise Security.
<http://enterprisesecurity.symantec.com/content/displaypdf.cfm?pdfid=276&EID=0>. (22 Feb. 2005)

Delong, Daniel F. "Code Red Virus Most Expensive in History of Internet."
NewsFactor. 9 Aug. 2001 25 Feb. 2005
<http://www.newsfactor.com/perl/story/12668.html#story-start>.