Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Auditing Sygate Personal Firewall 4.2

GSNA Certification Practical

Nicholas Shevelyov

February 2002

Version 1.2

GSNA Assignment 1 - Research in Audit, Measurement Practice and Control

1.1 Introduction

The personal firewall market has matured significantly in the last few years. The Big 3 Personal Firewalls as listed by Firewall Guide [1] are Zone Alarm, Tiny, and Sygate. I have chosen to audit the Sygate Personal Firewall 4.2 (Personal Firewall does Stateful Packet Inspection on every Remote TCP connection. Sygate® Personal Firewall also uses an algorithm to check Remote UDP and DHCP traffic to make sure that the communication is secure. [2]) running on a laptop connected to the Internet via a DSL modem. Keep in mind, this is a personal firewall meant to protect a system used by one person, it is not your typical corporate firewall protecting multiple assets. As a result, many areas important to a corporate firewall audit (including change control processes, corporate security policy, etc) are not applicable to this audit. Additionally, we will try to see if the firewall meets common criteria requirements that I will identify in the following sections.

The goal of the paper is to leverage a current standard of corporate firewall auditing while making improvements to that standard to better help audit a personal firewall. There is a lot of information available for auditing corporate firewalls, but not much of anything on Procedure audit personal firewalls. I will attempt to create a set of audit procedures applicable to most every personal firewall. Other users auditing any type of personal firewall can then repeat the audit procedure.

1.2 What is the current state of practice, if any?

I started off visiting Internet sites I have used in the past and that were related to auditing. These sites included http://www.isaca.org/, http://www.sans.org, http://www.securityfocus.com/, http://www.cert.org/, http://www.auditnet.org, http://www.infosecuritymag.com, and http://www.auditnet.org/ .While sites like http://www.auditnet.org/ offer documents on auditing firewalls[3] and www.securityfocus.com offered a good overview paper on auditing firewalls (http://www.securityfocus.com/library/2386)

The Sygate Help files are a useful reference and advertise features that should be audited in order to verify that they work as Sygate claims. Sygate Technical Support can also be contacted as a reference point, although inquiries were not replied to in a timely manner rendering the service less than useful. A search on Google for the term "Auditing Firewalls" yielded 35,400 results, the most relevant information being Lance Spitzner's document on auditing firewalls. Additionally, I have in my possession the SANS Track 7 manuals with book 7.2 dealing specifically with auditing routers and firewalls. Finally, I

---

[1] http://www.firewallguide.com/freeware.htm
[2] http://www.sygate.com/support/technotes/ssd_sms/SPFFAQ013.htm
[3] http://www.auditnet.org/docs/firewall%20audit%20program.txt

found that "Management Analytics Firewall Checklist"[4] to be the most valuable resource.

What I found was, although there is abundant amounts of information on Procedure audit corporate firewalls, there is no one "community accepted" current state of practise on Procedure audit personal firewalls, in fact I could not really find any information on what steps to take in order to audit a personal firewall. I will go into this fact in much greater detail in the following sections.

1.3 What is good and/or bad about the current checklists for corporate and personal firewalls.

The three documents I am using as reference (Stephen Northcutt's "Auditing Routers and Firewalls" volume 7.2 from SANS Track 7 – Auditing Information Systems, Lance Spitzner's "Auditing Your Firewall Setup[5]" and the "Management Analytics Firewall Checklist (M.A.F.C.")") are good resources for auditing corporate firewalls. Spitzner's document is presented much like a summery of best practices. Northcutt's manual is presented in a Power Point presentation format and has clear explanations on technical steps to take during and audit. The M.A.F.C. is presented as a series of checklist that focus on managing a firewall in a corporate environment (it does include functional tests, something I will address in the following sections). The strengths of these documents are as follows; If you were new to firewall audits Spitzner's document would be most useful. If you wanted technical steps for an audit Northcutt's would be best. If you wanted to incorporate firewall management into a security policy the M.A.F.C would be most useful. All documents are well done for their area of focus.

These resources are not fully applicable to home office environment personal firewall. Spitzner's document is a general summary that addresses auditing methodology, corporate firewall rule-bases, filtering and some auditing tools but provides no specific checklist to follow for corporate of personal firewalls. Northcutt's Power Point presentation provides the specific technical areas that should be part of a firewall audit, but does not provide a clear audit procedure checklist for firewalls. Finally, the M.A.F.C. document does provide a clear checklist of steps to take, but the vast majority of the document addresses firewall management related issues (control objectives, management decisions, etc.). For example a M.A.F.C. audit step is "Management is highly supportive of effective firewall protection." This is totally inapplicable to a personal firewall. The user is the administrator.

This is not to say that there are not certain similarities in auditing a corporate firewall and a personal firewall. For example, Spitzner states, "Did the firewall detect all of your scans, did it set off the expected alerts?" This is applicable for both a corporate and personal firewall. Northcutt states, "Do you have any specific requirements for how the firewall will operate"(with control outbound access)? It is important for both corporate and personal firewalls to control outbound access. The M.A.F.C. document states, "Technical safeguards include protection from outside attacks, inside attacks, and attacks directed

---

[4] http://www.all.net/books/audit/Firewall/manal/index.html
[5] http://www.enteract.com/~lspitz/audit.html

from within the firewall." This is applicable to both corporate and personal firewalls. The "Technical Specifications[6]" portion of the very broad M.A.F.C. document is the most relevant checklist I have found (for both corporate and personal firewall). It includes the following steps:

1. Technical safeguards include protection from outside attacks, inside attacks, and attacks directed from within the firewall.
2. The interaction of technical safeguards is well defined and understood.
3. Technical safeguards include automated response to many of the most common threats.
4. Technical safeguards provide for interface with automated intrusion detection systems or capabilities.
5. The firewall operates on highly secure operating systems.
6. The firewall does NOT consist entirely of a screening router.
7. The firewall properly separates a DMZ from the inside network and the outside network.
8. The firewall does not artificially limit the number of simultaneous sessions that can operate through it, or the limits are such that they are beyond any anticipated performance requirements.
9. The firewall is not artificially limited by the state information required to perform its function, or the limits are such that they are beyond any anticipated performance requirements.
10. The size of the access control file does not grow to extremes given the complexity of the organization's current or anticipated access control requirements.
11. Control of the access control file is adequate to assure that there are no windows of vulnerability as the access control information is changed.
12. No denial of service results during changes of access control information.
13. When access control information is changed, active sessions, which access controls should not permit, are terminated.
14. None of the attacks that have become widely known in the last months have worked against this firewall.
15. There is a systematic method for finding out about and updating the firewall to defend against new attacks.
16. IP packet forwarding is turned off.
17. Source routing does not operate through the firewall.
18. The recent packet fragmentation attack did not work through this firewall.
19. The firewall uses redundancy in the form of defense-in-depth to assure that no single attack or configuration error can bypass the firewall's controls.
20. All processes operating on all firewall computers at the time of the audit are known to be appropriate and appear to be operating properly based on the process status listing.
21. Traceroute through the Internet properly identifies routes including routes that cannot be verified as appropriate.
22. Widely used tests run from over the Internet or other similar networks do not reveal any firewall flaws.

---

[6] http://www.all.net/books/audit/Firewall/manal/tech.html

23. The /etc/services file contains only services in actual use on each machine within the firewall.
24. The /etc/inetd.conf file contains only services in actual use on each machine within the firewall.
25. Comments are not used to disable services; rather, those service entries are not within the files used to identify those services to the operating system.
26. All entries in all access control lists are known to be appropriate and have been individually verified as part of reviewing this checklist.
27. The password file has been examined for widely know inappropriate practices and no inappropriate or questionable entries are included within it.
28. Crack has been run against a copy of the password file and none of the passwords were successfully guessed.
29. Rsh and Portmapper functions are disabled on all firewall components.
30. Regular backups are done of all firewall components.
31. Copies of firewall backups are stored both on-site for rapid recovery and off-site for disaster recovery.
32. Backups are restored on a regular basis on machines designated for disaster recovery as a test of their proper operation.
33. Firewall files are cryptographically checksummed and those checksums are regularly verified.
34. Firewall files are stored on read-only media and a system of sound change control is used to make firewall alterations.

As you can see there are many steps here that do not apply to a personal firewall (for example Step 7, The firewall properly separates a DMZ from the inside network and the outside network.") In fact, although this is the most easily readable and applicable set of audit checklists for a firewall, it requires a great deal of change to be applicable to a personal firewall.

1.4 Resources I found to be most useful.

The documents I just listed provide a good source of reference in developing a firewall audit methodology. They will be leveraged in creating an audit process for the Sygate Personal Firewall 4.2. But in the end, the audit evaluation results (Pass/Fail) will be decided by the both objective results as well as the auditor's (me in this case) subjective view of the results. Each of the audit steps we take will be shown as either an objective or subjective test.

1.5 Why are current methods and techniques in need of improvement?

Current methods and technique are focused on corporate firewalls. They do no specifically address steps for a personal firewall. As a result I will use the most applicable steps from the M.A.F.C. "Technical Specifications" document and will make improvements to these steps so that the audit is better suited for a personal firewall. I will draw on audit steps from "Auditing Routers and Firewalls" volume 7.2 from SANS Track

7 – Auditing Information Systems, Lance Spitzner's "Auditing Your Firewall Setup[7]" to create the new/more applicable set of procedures for auditing a personal firewall. I will list which step originated from which resource (again by listing Auditor Influence in the audit step).

We also have to remember that Sygate does not have a configuration lock down feature. It allows the changing of its rule definition to an authorized user. This is an extension of a flexible operational philosophy; nevertheless, it makes audit results less and less useful past the actual audit date.

Intentionally Blank

---

[7] http://www.enteract.com/~lspitz/audit.html

1.6 Environment being audited.

Figure 1 gives us and idea of what our architecture resembles. This is a typical configuration, common in most homes with DSL connections. Although the firewall in Figure 1 looks like it is separate from the firewall in this layout, it is actually residing on the IBM ThinkPad itself.
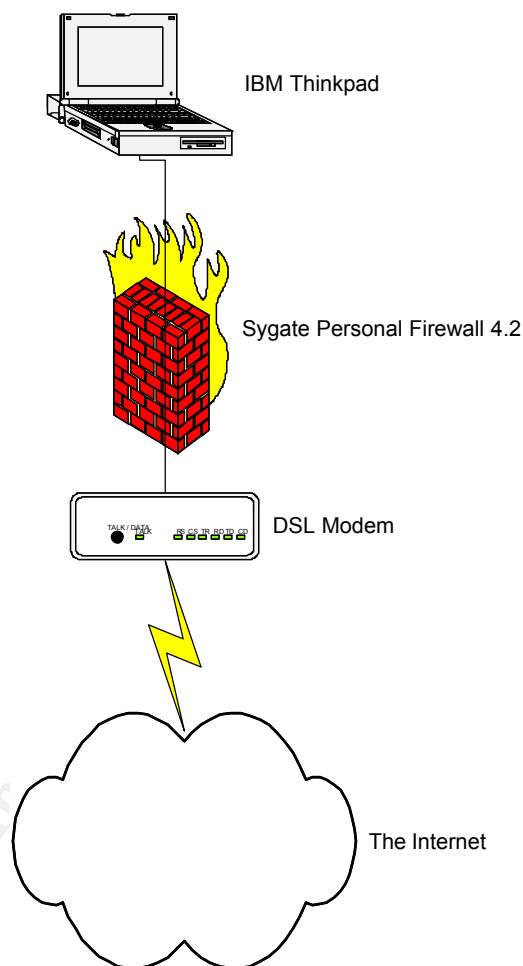

Figure 1 Visual layout of the laptop running the firewall and connected to the Internet via a DSL modem

1.6.1 Models for Controlling Access:

There are three models for controlling access. The three categories are as follows.

Mandatory Access Control: Authorization of a subject's access to an object depends upon labels indicating the subject's clearance as well as the classification of the subject.

Discretionary Access Control: Subjects have the authority to specify what objects are accessible. Access Control Lists (ACL) can be used in this scenario.

Non-Discretionary Access Control: Central authority determines the subject's access to certain objects based on a pre-defined security policy. Access may be based on a user's role (role-based) or the user's responsibilities (task-based).

In large-scale networks where personal firewalls are deployed to clients, these firewalls are usually centrally managed. The firewall rule sets are in most cases "pushed down" to the clients. In this case however, the personal firewall is independent of any central authority. The firewalls rule set is in this case purely a discretionary access control.
Typically, a laptop connecting to the Internet will have at least the following applications, and be required to run and utilize the following services and protocols.

1. Applications:

    - Web Browser (MS Internet Explorer or Netscape Navigator in most cases)
    - Email (MS Outlook in most cases)
    - A file sharing program (Not Recommended)
    - Firewall

2. Service:

    - DNS
    - DHCP
    - FTP
    - NetBIOS
    - Telephony
    - Simple TCP

3. Protocols

    - http (Web Access)
    - https (Web Access)
    - pop (Mail Access)
    - imap (Mail Access)
    - smtp (Mail Access)
    - ftp (File Transfer)
    - tcp (Web Access)

1.7 Final goal of the firewall

Conceptually, a firewall is meant to protect your computer resources from external

threats. In addition, as an ethical member of a community (the Internet) we are compelled to make sure our computer related resources are not hijacked and subsequently used in attacks on other web site, PCs, etc. As a result, controlling your computer related resources "is a good thing." In our case setting discretionary controls on the outgoing connections from the laptop may in fact require more of our time, but the added safety measures this brings is well worth the effort.

Rather than "allow all" traffic out, we will require that there be a specific rule to allow an application or protocol access out from the machine. An implicit "deny all" unless specifically allowed is always the best first rule in any firewall configuration. Being able to log firewall activity such as incoming and outgoing connections is also a desirable attribute. These come in particularly handy during an intrusion incident response or during a forensic portion of an intrusion. In summary, a firewall should protect your system(s) from malicious activity originating from the outside world, while also preventing you from doing harm to the outside world.

1.8   The Checklist

As stated in by SANS "For an audit to work, there must be a ruler.[8]" The ruler for my "new and improved" checklist is modelled after the (personal firewall applicable) audit techniques sampled from the "Management Analytics Firewall Checklist." Additionally, I will use the best steps from Stephen Northcutt's "Auditing Routers and Firewalls" volume 7.2 from SANS Track 7 – Auditing Information Systems, Lance Spitzner's "Auditing Your Firewall Setup,[9]" and audit steps I have found useful in the past. The goal of this audit is to compare "where we are" with the firewall's level of security as opposed to "where we should be." If the firewall passes the entire audit, then where we are is actually were we should be as well. If the firewall fails an audit step, the "Status" portion of the audit will list how it was determined that the firewall failed the audit and what steps need to be taken in order for the firewall to meet the audit requirements. These steps will fall under the heading of where we should be.

Each audit step will have a field stating it is an "Audit Checklist Step #" (to describe which step number this is) the Management Analytics Checklist "Technical Specifications" step I am using or an "Auditor Influence (to state whether it came from Lance Spitzner's document, Stephen Northcutt's manual or my own experience) and finally the "Date."(to understand when the firewall was in or out of compliance with this audit steps). The "Requirement" will list what we require of the firewall's security settings. The "Procedure" and the "Results" talk about Procedure conduct the audit step and what is the result. For the actual audit there will be an "Importance" description specifying why this audit step is important.

Either the "Objective" or "Subjective" boxes will be checked depending on whether I believe the audit steps fall under the general definition of objective or subjective results and whether the steps are considered objective or subjective by the audit from which I sampled the audit step. For example if I use an audit step from Stephen Northcutt's

---

[8] SANS GSNA v 1.2 audit procedures
[9] http://www.enteract.com/~lspitz/audit.html

"Auditing Routers and Firewalls" volume 7.2 from SANS Track 7 – Auditing Information Systems and the step is listed as subjective or objective in that manual, I will list it as such. What can be measured objectively? Output scans from a port scanner are objective.

How will you know it is out of specifications required? If, while the firewall is running, the output of a scan shows any open ports I did not specifically configure to leave open (this implies the firewall uses the implicit deny rule). This is binary output. The scan is either showing open port or it is not. This is strictly a pass or fail type of audit step. What can be measured subjectively? The consensus opinion on the usability of a console interface is a subjective assessment. The firewall console is out of specifications if it claims to be user-friendly but is difficult to navigate. The results are not binary in this case, but rather there are conditions that apply. For example, the 3rd party user auditing the usability of the firewall console felt it was difficult to navigate. This is a subjective opinion (a user with greater firewall console experience may say the exact opposite) where conditions (in our case the 3rd party's firewall console experience) apply.

And finally, "Pass" or "Fail" will be marked depending on how the firewall stands up to the audit procedure. Again, if the audit step is sampled from (for example) Stephen Northcutt's "Auditing Routers and Firewalls" volume 7.2 from SANS Track 7 – Auditing Information Systems I will audit the firewall against that step, and depending on how volume 7.2 decides if a system passes or does not pass, I will show the result accordingly. For every step that I feel requires a follow up to review the system logs, there will be s second portion to the audit step. So for example, if step 2 is to scan the firewall with a UDP scan, then step 2:2 will be to review the logs to see if they caught that scan.

How should this audit be conducted? Audits should ideally be conducted in a controlled environment. The test itself should be conducted in a secure area with little outside disturbances. This audit is being conducted primarily from my home office with two objective port scanning procedures being run within a small office environment.

1.9 Technical Requirements and Sygate Personal Firewall 4.2 Settings

These requirements will include firewall functionality (does the firewall actually do what it is supposed to do) and well as configuration and administration related topics.

Audit Checklist Step 1	M.A.F.C. Technical Objective Step 3	Date: / /
Requirement: Technical safeguards include automated response to many of the most common threats (outbound connections).		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 1:2	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: Verify the firewall logged un-authorized outbound connection attempt.		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 2	M.A.F.C. Technical Objective Step 22	Date: / /
Requirement: Widely used tests run from over the Internet or other similar networks do not reveal any firewall flaws (nmap SYN scan).		Objective Subjective
Procedure/Results: **Importance:**		**Pass** **Fail**

Audit Checklist Step 2:2	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: Verify the firewall logged the port scanning activity.		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 3	Auditor Influence: My Own Experience	Date: / /
Requirement: The Firewall protects against inbound connections. (Attempts by an outside machine to connect to the system).		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 3:2	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: The Firewall logs inbound connection attempts and subsequent results.		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 4	Auditor Influence: Lance Spitzner	Date: / /
Requirement: There is a method for notifying the system administrator when a critical event occurs that works consistently.		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 5	M.A.F.C. Technical Objective Step 28	Date: / /
Requirement: Administration of the Firewall is password protected.		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 5:2	M.A.F.C. Technical Objective Step 28	Date: / /
Requirement: Firewall logs invalid password attempts accessing the console.		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 6	M.A.F.C. Technical Objective Step 2	Date: / /
Requirement: The interaction of technical safeguards is well defined and understood.		Objective Subjective

Procedure/Results: Importance:		Pass Fail

Audit Checklist Step 7	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: The Firewall protects against connectionless protocol (UDP) scans.		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 7:2	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: The Firewall logs connectionless protocol (UDP) scans.		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 8	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: The Firewall protects against clandestine (FIN) Scans.		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 8:2	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: The Firewall logs (FIN) Scans.		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 9	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: The Firewall protects against vulnerability scanners (Nessus).		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 9:2	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: Verify the firewall logged the Nessus vulnerability scanning attempts.		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 10	Auditor Influence: My Own Experience	Date: / /
Requirement: The firewall blocks DoS attacks (large number of ICMP packets).		Objective Subjective
Procedure/Results: **Importance:**		Pass Fail

Audit Checklist Step 10:2	Auditor Influence: My Own Experience	Date: / /
Requirement: The firewall logs the DoS attack.		Objective Subjective

| **Procedure/Results:** | Pass |
| **Importance:** | Fail |

Intentionally Blank

GSNA Assignment 2 – Application of Audit Techniques to a Real World System

2.1 System to be audited

At this stage we begin to run the audit procedures outlined in Assignment 1. The system to be audited is an IBM ThinkPad T20 running Windows 2000 Sp 2 with Sygate Personal Firewall 4.2. The latest relevant Microsoft Hot-Fixes have been applied to this system.

2.2   What the purpose and primary role of the firewall?

The primary purpose of this firewall is to protect my personal and financial information while connected to the Internet via my DSL line. That means no outbound connections I don't know about and no inbound connections without my explicit permission. It means that my system should not give up information to port scanning activity or be susceptible to vulnerability scanners.

2.3   What is the risk to the system

I value the personal and financial information at $3000. With hackers shifting their focus in recent months to personal machines on DSL connections and the information on this laptop being worth $3000 to me, it is worth my time to protect this machine. (I define risk as the combination of likelihood and consequence of the occurrence of something going wrong).

Leaving my laptop connected to my DSL connection for 24 hours results in an average of 12 port-scans (from 12 separate IP addresses) from the outside per day. If I left my laptop on the DSL line 24 hours a day, 365 days of the year, I would face 4,380 (12scans per day) x 365(days per year)) port scan per year. As a result, my Annual Rate of Occurrence (ARO) (which is "a number that represents the estimated frequency in which a threat is expected to occur[10].") is 4,380. If 1 out of every 1,000 port scans leads to an extended attempt to break into my system, my laptop faces 4.3 potential break-ins per year.

Still, what is the likely-hood of a port-scan leading to an actual break in with financial losses incurred? Not that great but still worth keeping an eye on. I am not running IIS Web Server on the laptop so although that is a primary concern for a-lot of companies; it usually is not something to worry about as a home user. As a home user the greater threat is if the machine becomes infected with a Trojan (A Trojan is a program that you have sitting on your system that you are (usually) not aware of. When the right transmission is received the program goes into action and it can take hold of your computer, making it impossible for you to gain control. It can use your computer as a method of attacking another computer, or simply hand over all your information to a third party. Spy-ware is another problem. Spy-ware is defined as "spy-ware is any technology that aids in

---

[10] "The CISSP Prep Guide –Mastering the Ten Domains of Computer Security" p. 17

gathering information about a person or organization without their knowledge. On the Internet, spy-ware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spy-ware can get in a computer as a software virus or as the result of installing a new program. Data collecting programs that are installed with the user's knowledge are not, properly speaking, spy-ware, if the user fully understands what data is being collected and with whom it is being shared[11]." Trojans and/or spy-ware could result in identity theft and credit card fraud that would result in a cost much greater than $3000. As a result, the primary concern for a personal firewall should be outbound connections (especially those that I did not initiate).

2.4   Risk Priority-What I Expect The Firewall To Do

I need a firewall that will protect me from these potentially malicious intruders by doing the following:

1. Automated Response: Since this is my personal machine with my personal information on it, the number one priority is to make sure I am made aware anytime an outbound connection is attempted from my machine (which I have not specifically allowed). This is not just to protect my personal information, but also to make sure I am not unknowingly participating in a Denial of Service attack that may make my liable for resulting damage.
2. I want to know and have a record of when I am being port scanned for the most common ports. In case I need the proof when filing a complaint to an ISP.
3. Inbound Connections: A Firewall is meant to keep outsiders from getting in, so this functionality needs to be audited.
4. If an inbound connection occurs, I want proof in the logs.
5. I want to know when a critical event occurs, so some sort of paging notification should be available.
6. A password to access the firewall so that someone can't come up and make changes to my password is important and logs to prove an invalid password attempt.
7. Ease of use, in terms in navigating the firewall console.
8. I want to see how the firewall handles connectionless protocols (UDP).
9. Protection against exotic scans (FYN,)
10. Although Denial of Service attacks is not a big threat to a personal firewall, I would like to know the firewall would handle ICMP attacks.

2.5   The Audit Procedure –Most Relevant and Risky Steps

Sygate 4.2 settings for the laptop being audited should be set by configurations that are influenced by the auditors knowledge of Sygate 4.2 operational principles, W2K OS configuration settings, fundamental security principles, and good old trial and error checking.

---

[11] http://whatis.techtarget.com/definitionsSearchResults/1,289878,sid9,00.html?query=spyware

We should also ask ourselves "Do you have any specific requirements for how the firewall will operate[12]?" Our first step in auditing our firewall is defining what we expect. What do we want our firewall to do? Most of you should have this already defined in the form of a security policy. Make sure you have an understanding of these expectations before you verify your firewall setup. That way, when you are done with the process, you can compare the results to your expectations. Some of you may be in the situation where you don't know what to expect[13]. In our case inbound and outbound control access will take a precedent. That means "are you in control of what is coming into your system and what is going out of your system?"

Of all the resources that I reviewed, the M.A.F.C. document was the best suited as an audit procedure checklist and as a result, the M.A.F.C. document was the primary checklist used for my audit. But even as the best suited checklist, only a few of the steps were actually applicable to a personal firewall. As a result I chose the most relevant and riskiest steps from the M.A.F.C. procedures and combined them with the most relevant audit steps from my other resources. The result should be a set of audit procedures that suit personal firewalls.

Intentionally Blank

Personal Firewall Audit Checklist – In Order Of Risk To A Home

Audit Checklist Step 1	M.A.F.C. Technical Objective Step 3	Date: / /
Requirement: Technical safeguards include automated response to many of the most common threats (outbound connections).		**Objective** **Subjective**

---

[12] SANS Online Training Auditing Networks, Perimeters, and Systems slide 11

[13] http://www.enteract.com/~lspitz/audit.html

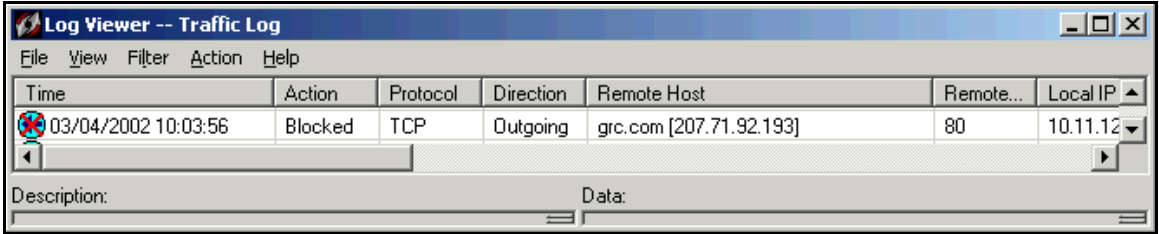[14] http://grc.com/lt/leaktest.htm

	Pass Fail
Procedure: 1. Download and install Leak Test from www.grc.com. 2. Leak Test will launch; click the "Test for Leaks" button. 3. A help window will pop up, click "OK" 4. A request for permission should pop up, click "No" 5. Leak test should come up with a Window saying it was unable to connect to the internet (as seen here below). **Results:** I define the most common threat for my personal firewall as outbound connections that I do not allow and/or am not aware of. I tested this by installing a Trojan Horse/Spy-ware simulation program called Leak Test. Leak Test is a safe and small (27k bytes), completely benign "chameleon utility" which can be used to simulate the presence and effect of Trojan horses, viruses, and adware/spyware running in your computer. It simply and quickly tells you whether it has been able to slip out past your firewall's outbound Trojan/Virus/Spy-ware protections and establish a standard TCP connection with the GRC server. [14] While connected to the internet I launched Leak Test and was unable to connect to grc.com. Sygate blocked the outbound connection and passed the test. **Figure 2 Sygate catches Leak Test's outbound connection attempt** **Importance:** Your Rule Base should specify which applications are making outbound connections, where they are trying to connect and why are they trying to connect. Allowing application to make these outbound connections without your explicit consent is a huge security hole. Information you did not wish to share could be sent out without your permission. Additionally, you do not want your system to unwittingly participate in any Denial of Service attacks (in the case your system has be turned into a droid).	
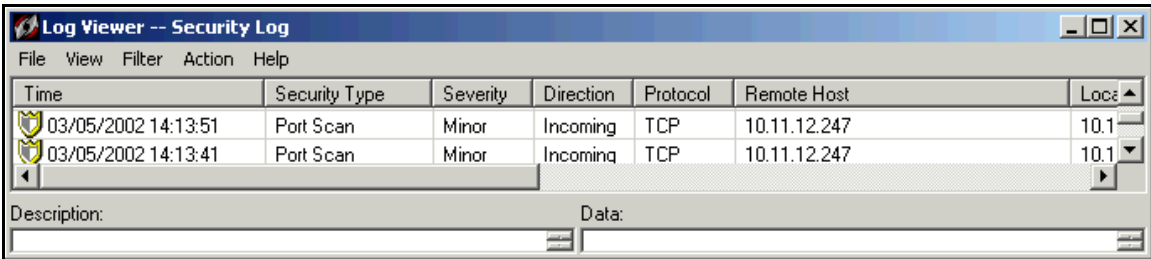
Audit Checklist Step 1:2	Auditor Influence: Stephen Northcutt	Date: / /

---

[14] http://grc.com/lt/leaktest.htm

Requirement: Verify the firewall logged un-authorized outbound connection attempt.	Objective
	Subjective
Procedure: 1. Open the firewall Traffic Logs and review for evidence of un-authorized out-bound connection attempts. **Results:** As the graphic below shows, the Firewall logged the un-authorized out-bound connection attempt to grc.com and shows that it was indeed Blocked. **Figure 3 Firewall Traffic Log showing blocked outgoing attempt.** **Importance:** If and application is making an out-bound connection attempt from your system your personal firewall needs to track this. As stated earlier, the primary focus of a personal firewall is to protect personal information form being sent out by a Trojan or Spy-ware. As a result, logging out-bound connection attempts (and their results) is important.	Pass Fail
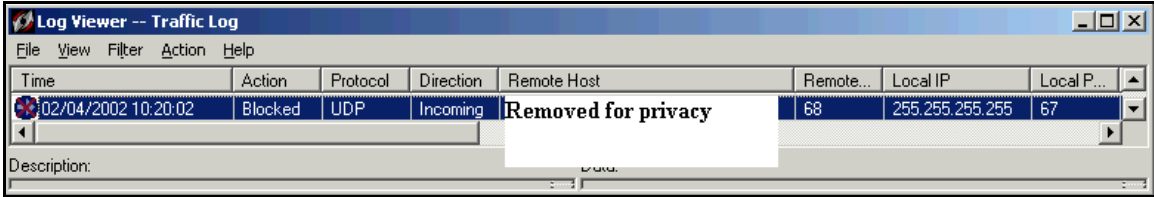
Audit Checklist Step 2	M.A.F.C. Technical Objective Step 22	Date: / /

	Objective Subjective
Requirement: Widely used tests run from over the Internet or other similar networks do not reveal any firewall flaws (nmap SYN scan).	**Objective Subjective**

Procedure:
 	
1. Download Nmap from www.insecure.org and install on a separate audit assessment box.
2. From the audit assessment box run an Nmap TCP SYN scan against the system running the firewall by typing nmap –sS –O –v (ip address of system running the firewall)(-sS TCP SYN scan: A "half-open" scan, as you never open a full TCP connection via the three-way handshake. A SYN is sent, and a SYN | ACK reply means the port is listening while a RST replay indicates a closed port. A SYN | ACK reply generates a RST to tear down the connection. This type of scan is harder to detect.)[15]
3. Save the results to a .txt file names "machine_name_SYN"
 	
Results:
 	
Port Scanning is the most widely used test across the Internet (although this may not be considered a threat by all administrators which is why it is subjective). With the Sygate 4.2 firewall running, I ran a TCP SYN Stealth scan using the command nmap -sS -O -v 10.11.12.145 which resulted in the following output:
nmap Syn Scan
  bash-2.04# ./nmap -sS -O -v 10.11.12.145
 	
  Starting nmap V. 2.54BETA25 (www.insecure.org/nmap/)
  Unable to find nmap-services! Resorting to /etc/services
  Host (10.11.12.145) 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 30 seconds
 	
Without the firewall running I got the following result:
 	
Adding TCP port 135 (state open).
Adding TCP port 139 (state open).
Adding TCP port 445 (state open).
The SYN scan took 0 seconds to scan 1523 ports.
Interesting ports on dhcp-145.xxxxx.com (10.11.12.145):
(The 1520 ports scanned but not shown below are in state: closed)
Port   State   Service
135/tcp open   loc-srv
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds
 	
Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
 Importance: While the firewall was running, Nmap could not find my host. The firewall passes the most common test ran across the internet.
	Pass Fail

---
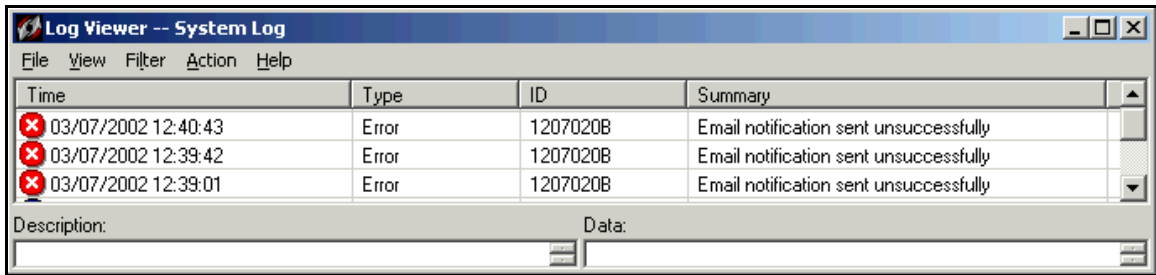
[15] http://rr.sans.org/tools/free_tools.php

Audit Checklist Step 2:2	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: Verify that the Sygate 4.2 logged the port scanning activity.		Objective Subjective
Procedure: 1.Open the firewall Security logs and review for evidence of port scanning. **Results:** Checking the Sygate 4.2 Security log files after I ran the nmap scan showed that the port scanning activity was indeed logged and Sygate gives me an description in the bottom left hand corner that says "Somebody is scanning your computer." **Figure 4 Sygate logs the port scan in the Security Logs** **Importance:** If someone is port-scanning your system you want to know about it. Again these logs can be used incase you decide to take action against the party initiating the port scans.		Pass Fail

Audit Checklist Step 3	Auditor Influence: My own experience	Date: / /
Requirement: The Firewall protects against inbound connections. (Attempts by an outside machine to connect to the system).		Objective Subjective
Procedure: 1.Create a share on the system running the firewall. 2. From the separate audit box: Type (for firewall running on a Windows 2000 platform, if another platform, use similar command) "NET USE \\Machine_Name\Share_Name" **Results:** The primary responsibility of a firewall is to protect your system(s) from outside machines trying to make un-authorized connections to your system. This is also known as inbound connections. The firewall should block these attempts. I attempted to make a connection to the IBM laptop from another system on a private network. The attempted connection was denied and received the following message. ![Exploring - Orion dialog box: \\Orion is not accessible. The network path was not found. OK] **Figure 5 Inbound connection attempt is unable to connect to my system** **Importance:** As previously stated, the primary goal of a firewall is to protect your resources from the "outside". Attempting inbound connections is a good example of this type of activity. To verify that the attempted inbound connection failed as a result of the firewall working properly and not as a result of a network failure I shut down the firewall and again attempted to connect to my system. With the firewall shut down I was able to connect to my system. This verifies that the firewall is protecting me from outbound connections.		Pass Fail

Audit Checklist Step 3:2	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: The Firewall logs inbound connection attempts and subsequent results.		Objective Subjective
Procedure: 1. Open the Firewall logs and verify that the Firewall logged in inbound connection attempt: **Results:** Blocking against inbound connections is the primary goal of a firewall, but being able to review the logs of such activity is also necessary. I reviewed the Sygate 4.2 logs after I failed to make the inbound connection in the previous audit step. (Due to the size of the graphic I am unable to show all the categories the firewall log addresses, but I will describe them here). The log showed me the Time the inbound attempt occurred, the action taken, the protocol used, the direction of the traffic (inbound/outbound), the IP address of the remote host (I removed the actual IP address for privacy), The port the remote machine used to make the connection attempt, the local IP address, the port on the local machine that the outside machine tried to initiate the connection on, the application (if any) that was involved in the activity, the time the inbound attempt began, the time the inbound attempt ended, and finally the rule that prevented the inbound attempt from being successful. This is what the Sygate 4.2 logs showed me: **Figure 6 Sygate caught the inbound connection attempt in the logs** **Importance:** Logs are important to what is going on with your firewall in general and especially for incident response forensics. If your firewall fails and there is a compromise to your system, having the logs to tell you what happened and when it happened is critical. If the firewall does not fail, you still want to know where the inbound attempts are originating, what time, etc. This will help in case you decide the contact the offending IP address' ISP and file a formal complaint. The ISP will request the log information to validate your complaint. If the ISP can verify that one of their users is trying to "hack" other systems, the ISP will in some cases cancel the offending users internet service.		Pass Fail

Audit Checklist Step 4	Auditor Influence: Lance Spitzner:	Date: / /
Requirement: There is a method for notifying the system administrator when a critical event occurs that works consistently.		Objective Subjective
Procedure: 1. Configure the notification function on the firewall. (In Sygate's case it is the Email notification option). 2. From a separate audit system, launch a vulnerability scan against the system IP address running the firewall. 2. The Firewall should send an email notification to administrator (in this case my pager). **Figure 7 Email fails to be sent** **Results:** Although Sygate attempted to send the email, it was sent unsuccessfully as seen in Figure 7. Although this function has worked for me in the past, this system is having problems and will require further troubleshooting. So although this is usually a working feature it has failed the audit step at this time. **Importance:** If your system is being attacked you will want to know about it. You can't always be right in front of you firewall console, that's why it is very useful to have your firewall page you when an un-authorized event occurs.		Pass Fail
Audit Checklist Step 5	Auditor Influence: M.A.F.C.	Date: / /
Requirement: Administration of the Firewall is password protected.		**Objective** **Subjective**

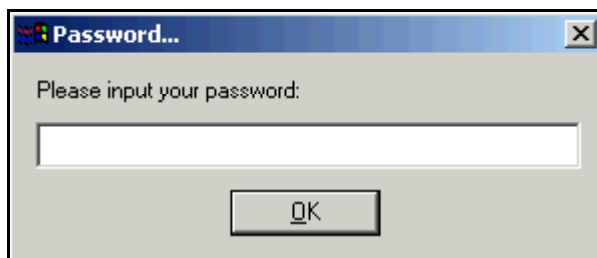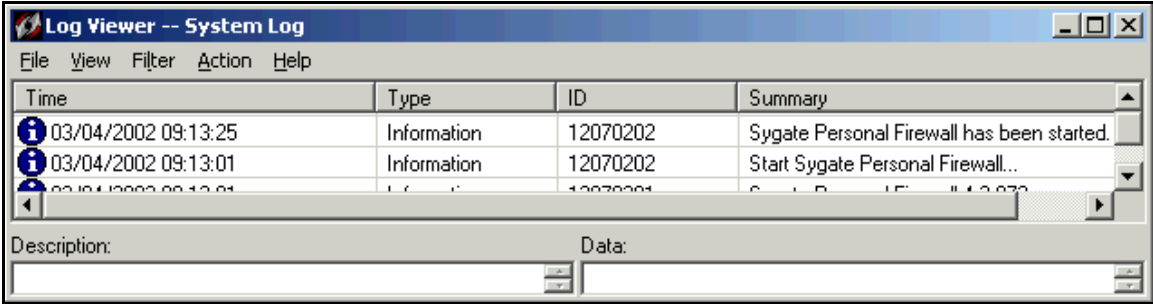|	
Procedure: 1. Launch the firewall to see if it prompts you for a password in order to access the console. **Results:** I attempted to launch Sygate 4.2 and was prompted with the following screen seen in Figure 2: **Figure 8 Password Prompt** To test Sygate's password protection I typed in an incorrect password which resulted in the following screen shown in Figure 3: **Figure 9 Splash Screen showing that the password is rejected** I hit OK and again attempted to launch Sygate. This time when I was prompted for a password I entered in the correct pass-phrase. The Sygate 4.2 administration console started up. **Importance:** Passwords are a fundamental part of security. Your could have a well configured firewall, but if you allow anyone to make changes to that configuration then you are opening yourself up to a big risk. As stated in Tina MacGregor's SANS article **"Password Auditing and Password Filtering to Improve Network Security"** [16]Passwords are often the first line of defense (in some cases the only line of defense) in a network environment or standalone system	**Pass** **Fail**
Audit Checklist Step 5:2	**M.A.F.C. Technical Objective Step 28**

Audit Checklist Step 5:2	M.A.F.C. Technical Objective Step 28	Date: / /

[16] http://rr.sans.org/authentic/improve.php

Requirement: Firewall logs invalid password attempts accessing the console.	Objective
	Subjective

Procedure:	Pass
1. Launch the System Logs to see if Sygate logs invalid password attempts to access the firewall console.	Fail
Results:	
I purposefully tried an invalid password to access the password protected firewall console. Checking the System logs showed no invalid attempts.	

Figure 10 System Log shows no invalid attempts, just the system starting

Importance: If someone is trying to access your firewall console directly from the laptop, you want to know about it. The Sygate firewall should really log invalid password attempts but it does not. The firewall fails this audit step.

Audit Checklist Step 6	M.A.F.C. Technical Objective Step 2	Date: / /
Requirement: The interaction of technical safeguards is well defined and understood.		Objective Subjective
Procedure: 1. Find an individual with little or no firewall experience. 2. Verbally guide the user on how to launch the Firewall console. 3. Verbally guide the user through adding a Firewall rule. 4. Verbally guide the user through deleting a Firewall rule. 5. Verbally guide the user through opening the Firewall logs. **Results:** This is a purely subjective assessment, but having used multiple personal firewalls over the last few years my opinion is that the Sygate 4.2 user interface is both simple to navigate and has well defined functions. **Importance:** If the user is unable to navigate the firewall configuration tools, how can they be expected to configure a firewall effectively. An intuitive GUI and a well-defined set of functions is critical to an application be distributed to the retail buying public.		Pass Fail

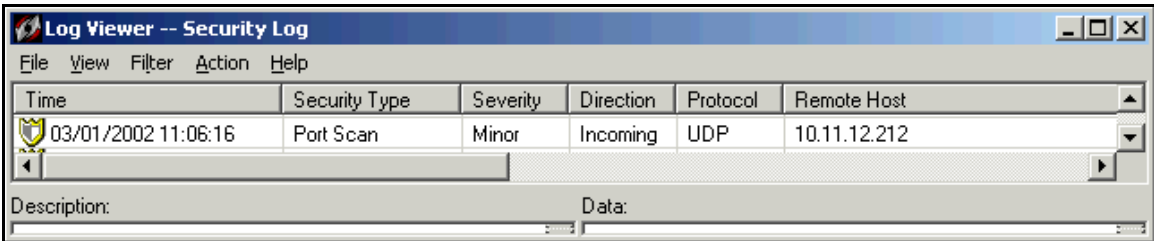| Audit Checklist Step 7	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: The Firewall protects against connectionless protocol (UDP) scans.		Objective Subjective
Procedure: 1. Download Nmap from www.insecure.org and install on a separate audit assessment box. 2. From the audit assessment box run an Nmap TCP UDP scan against the system running the firewall by typing nmap –sU –O –v (ip address of system running the firewall)(-sU UDP scans: Nmap sends a 0 byte UDP packet to each port on the scanned machine. An ICMP unreachable reply means the port is closed.)[17] 3. Save the results to a .txt file names "machine_name_UDP" **Results:** I ran the Nmap UDP scan against the firewall and it passed the test as Nmap was unable to find the host much less any open ports. **nmap UDP Scan** **bash-2.04# ./nmap -sU -O -v 10.11.12.145** **Starting nmap V. 2.54BETA25 (www.insecure.org/nmap/)** **Host (10.11.12.145) 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 30 seconds** **Importance:** You would expect the primary focus of the firewall would be to protect against TCP connections (a connection oriented protocol) but being able to protect against UDP scans (a connectionless protocol) is also valuable.		Pass Fail

---

[17] http://rr.sans.org/tools/free_tools.php

Audit Checklist Step 7:2	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: The Firewall logs connectionless protocol (UDP) scans.		Objective Subjective
Procedure: 1. Check the Security logs to see if the firewall picked up on the UDP scan. **Results:** The Sygate firewall logged the scan as seen here in the Figure 11 screen shot. **Figure 11 Sygate Logs the UDP scan** **Importance:** As with previous scans, we want our firewall to log scanning activity.		Pass Fail
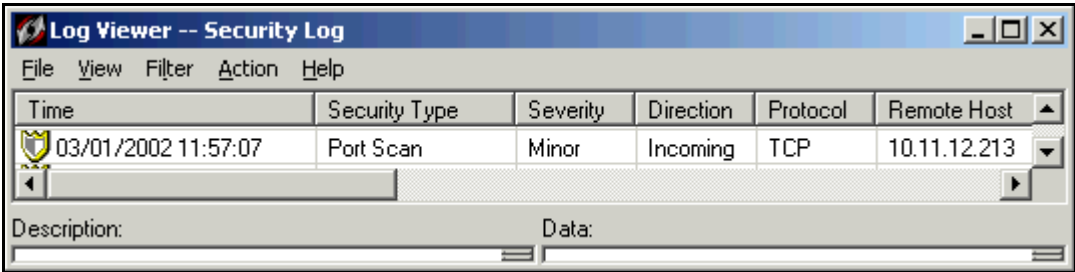
Audit Checklist Step 8	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: The Firewall protects against clandestine (FIN) Scans.		Objective Subjective
Procedure: 1. Download Nmap from www.insecure.org and install on a separate audit assessment box. 2. From the audit assessment box run an Nmap TCP FIN scan against the system running the firewall by typing nmap –sF –O –v (ip address of system running the firewall)(-sF These scans are useful in testing the ability to scan through a firewall/filtering device undetected. These scans are recommended for experts.)[18] 3. Save the results to a .txt file names "machine_name_FIN" Startup **Results:** I ran this scan and Sygate caught it and reported it as a UDP scan in the logs. **nmap FIN Scan** **bash-2.04# ./nmap -sF -v 10.11.12.145** **Starting nmap V. 2.54BETA25 (www.insecure.org/nmap/)** **Host (10.11.12.145) 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 30 seconds** **Importance:** As stated at http://www.insecure.org/nmap/nmap_doc.html#frag " There are times when even SYN scanning isn't clandestine enough. Some firewalls and packet filters watch for SYNs to restricted ports, and programs like synlogger and Courtney are available to detect these scans. FIN packets, on the other hand, may be able to pass through unmolested. This scanning technique was featured in detail by Uriel Maimon in Phrack 49, article 15. The idea is that closed ports tend to reply to your FIN packet with the proper RST. Open ports, on the other hand, tend to ignore the packet in question. As Alan Cox has pointed out, this is required TCP behavior. However, some systems (notably Microsoft boxes) are broken in this regard."		Pass Fail

[18] http://rr.sans.org/tools/free_tools.php

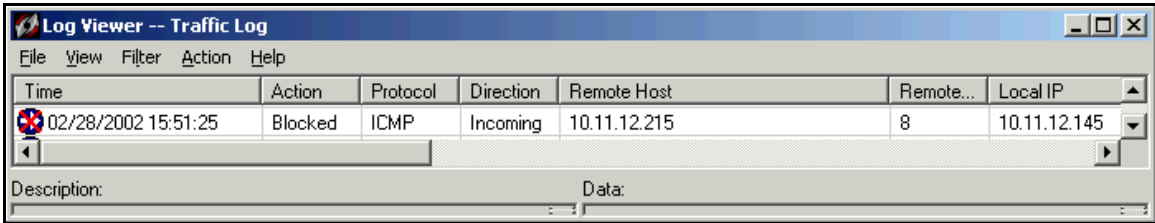| Audit Checklist Step 8:2	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: The Firewall logs (FIN) Scans.		Objective Subjective
Procedure: Check the security logs for the FIN scan. **Results:** I reviewed the Security logs and although Sygate logged the scan, it was unable to differentiate between a UDP and FIN scan. So although it blocked and caught the scan, I think it could have done a better job listing the scan as something other than the generic UDP. **Figure 12 Sygate sees a FIN scan as a minor problem and a UDP scan** **Importance:** I think when someone scanning your machine makes the effort to use a FIN scan; the firewall should have a method of noting that there is something different here. Sygate does not and as a result fails this audit-logging step.		Pass Fail

Audit Checklist Step 9	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: The Firewall protects against vulnerability scanners (Nessus).		Objective Subjective

Procedure:
1. Download Nessus from www.nessus.org and install the back-end and front-end portion.
2. Connect client to Nessus host server.
3. Configure Nessus client for target IP.
4. Execute the Nessus scan.
 	
Results: Nessus is software, which will audit remotely a given network (or system) and determine whether malicious intruders may break into it, or misuse it in some way. Nessus found zero security holes and zero security warning. That is a pass in my book.
`Nessus Scan Report`
`------------------`
 	
`SUMMARY`
 	
` - Number of hosts which were alive during the test : 1`
` - Number of security holes found : 0`
` - Number of security warnings found : 0`
` - Number of security notes found : 1`
 	
`TESTED HOSTS`
 	
` 10.11.12.145 (Security notes found)`
 	
`DETAILS`
 	
`+ 10.11.12.145 :`
`. List of open ports :`
`  o general/udp (Security notes found)`
 	
`. Information found on port general/udp`
 	
`   For your information, here is the traceroute to 10.11.12.145 :`
`   ?`
 	
`------------------------------------------------------`
`This file was generated by the Nessus Security Scanner`
Importance: A vulnerability scan will tell you what exploits are available for specific ports.
		Pass
		Fail

Audit Checklist Step 9:2	Auditor Influence: Stephen Northcutt	Date: / /
Requirement: Verify the firewall logged the Nessus vulnerability scanning attempts.		Objective Subjective
Procedure: 1. Open Firewall Security logs to verify that the vulnerability scanning activity was in fact caught by Sygate. **Results:** Sygate did in fact log the Nessus scans and showed it as a Port Scan of Minor Severity: I am failing the Sygate firewall for this interpretation of a vulnerability scan. I consider a vulnerability scan a bigger threat than a port scan (my opinion), but Sygate considers the severity to be the same. As a result it fails this audit step. **Figure 13 Sygate logs the Nessus vulnerability scan** **Importance:** A port scan is similar to a knock on the door; a vulnerability scan is more like looking for an open window in the house to break into. I think Sygate's logs should reflect this higher risk.		Pass Fail

Audit Checklist Step 10	Auditor Influence: My Own Experience	Date: / /
Requirement: The firewall blocks Denial of Service (DoS) attacks (large number of ICMP packets).		**Objective** **Subjective**
Procedure: 1. From 5 separate machines that have network connectivity and would be able to ping the system running the firewall (if the firewall was not running) type "**ping.exe my systems firewall address -l 65500 -n 10000**" **Results:** This causes the Windows machine to send ten thousand very large (64 kbyte) "ping" packets to the machine at the specified IP. This is 655 megabytes of data. This doesn't generate a high-speed stream because the "ping" command waits for a reply before trying again. But if many machines are all pinging at once, the result is cumulative and can be significant: Although performance was a bit more sluggish on the laptop, the firewall blocked the large ICMP packets. **Importance:** Although the risk of a ICMP DoS attack is minimal for a personal system, the fact that this type of attack gets so much press against public web sites I though it would be interesting to see how Sygate reacted. Basically I wanted to know how Sygate handles ICMP. If I had more machines sending the ICMP packets performance would become so sluggish the system would be knocked "offline" for all intents and purposes.		**Pass** **Fail**

Audit Checklist Step 10:2	Auditor Influence: My Own Experience	Date: / /
Requirement: The firewall logs the DoS attack.		Objective Subjective
Procedure: 1. Open up the Traffic Log file to see what Sygate said about the ICMP packets. **Results:** The logs were full of what you see below, Protocol ICMP with the three remote hosts that were used in the attack. **Figure 14 Sygate logs the ICMP packets Dos attack** **Importance:** As previously stated, a DoS attack on a personal machine is very unlikely, still the possibility exists that someone may take a disliking to you and try to launch an assault.		Pass Fail

2.6 Evaluating the Firewall

Evaluating this firewall we focused on verifying that relevant control objectives were being met (the firewall was controlling what came in and out), to identify where there were significant weaknesses (are there any hole in Sygate 4.2 that we were not aware of when we started this process) and to substantiate the risk that may be associated with such weaknesses (if there is a problem with Sygate 4.2, what types of threats does it pose).

Given the audit steps taken, the results posted by the Sygate Personal Firewall 4.2 were solid. We frequently read about personal firewalls not measuring up to the standards they advertise. In this case Sygate 4.2 met the audit challenges most firewalls will face on a regular basis. It protects the system from inbound connections, monitors outbound connections, provides log data on activity, notifies the administrator via pager when a critical event has occurred, starts automatically, auto-checks for updates, has a user-friendly console and is password protected. This is a solid foundation. However, the Sygate firewall failed in several logging audit steps. For example, although Nessus found nothing during the scan, Sygate interpreted a Nessus vulnerability scan as a minor threat. I would have rated it as a higher threat than minor. Also, it failed to log invalid password attempts to access the firewall console and interprets Nmap UDP and FIN scans with the same log results. I think it could have been more sophisticated in interpreting these results. The email notification feature failed on me, so although it has worked in the past it is sensitive and needs a thorough review to see why it is broken.

All in all, as a personal firewall independent of a central console controlling configurations, Sygate 4.2 shows itself to be reliable and easy to work with. It takes into account the applications, services, and protocols addressed in section 1.4.1 of this document.

2.7   Audit Evaluation

The guidelines for auditing listed in Part 1 of this document effectively evaluate the related features advertised by Sygate. This covers the firewalls initial action immediately after an install (it denies all then requires explicit rules to allow that traffic) as well as the permissions and filtering rules that follow. The port-scanning portion of the audit challenged and finally validated Sygate's ability to defend against some very basic scanning, although more intricate techniques were not used against the firewall and as a result can be considered a drawback to a firewall audit. This would be particularly true if we were auditing a commercial corporate firewall Another shortcoming could be see by my assuming a scenario where there has not been any malicious tapering by an authorized user. I also do not take into account the countless things that can go wrong based on user error.

This brings up the point mentioned in section 1.3. Sygate does not have a configuration lockdown feature but has a set of rules that can be changed by an authorized user. This is necessary for a personal firewall but it renders audit results obsolete in a rather short

period of time. Audit results that were true on one day could very well be changed the next day. If you have a rule denying the use of Netscape outbound connections on the day of the audit, then an authorized user knowingly or even unknowingly changed that setting to allow outbound connections, your audit results would be very different indeed.

Finally, a personal firewall sits on top of an OS. If the OS has security holes the firewall is also compromised. As a result, a systems overall security cannot be assessed by just its firewall being audited. The OS needs to be audited as well to give the system a full security assessment. An in-depth review of the OS security logfiles is as necessary as reviewing the firewall logs.

As a result, an audit of the Sygate 4.2 can tell you whether the firewall is protecting your system at the present time based on the criteria I have specified. It cannot tell you how secure your configuration will be next month (assuming configuration changes). This results in the need to repetitive audits. Additionally, this audit cannot tell you if your OS is undermining your security measures. A broader audit of both the firewall and the OS would be required for that type of assessment.

Reference:

Management Analytics. "Management Analytics Firewall Checklist" (Aug.13, 2001) URL: http://www.all.net/books/audit/Firewall/manal/index.html

Gibson, Steve "Leak Test: Procedure use Version 1.X" (Nov. 03, 2001)
URL: http://grc.com/lt/howtouse.htm

Gibson, Steve: "Leaktest.exe"
URL: http://grc.com/files/LeakTest.exe

MacGregor, Tina "Password Auditing and Password Filtering to Improve Network Security" SANS Institute http://rr.sans.org/authenticate/improve.php

Northcutt, Stephen. Track 7 "Auditing Information Systems, Volume 7.2 Auditing Routers and Firewall" (2001) SANS Institute

Spitzner, Lance "Auditing Your Firewall Setup" (Dec. 12, 2001)
URL: http://www.enteract.com/~lspitz/audit.html

SANS Online Training Auditing Networks, Perimeters, and Systems

Control Objectives for Information Technology (COBIT) Audit Guidelines – July 2000, IT Governance Institute

http://rr.sans.org/tools/free_tools.php

 http://www.sygate.com/support/forms/ssreq_form.htm

http://www.sans.org

http://www.auditnet.org/

http://www.firewallguide.com/freeware.htm

http://www.nessus.org