GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Rita J. Will
GSEC Practical
Version 1.4b, Option 1

Firewall Rule Review

(Review and clean up of firewall rules)

Abstract

Far too often rules are loaded onto the firewall, ACLs are configured on the routers and no one goes back to review or clean up. Firewall rules are added and none removed, which puts the network and firewall at risk. [1]"*Security professionals often use the term "security erosion" to describe the condition whereby the security of a system decreases over time.*" Auditors check router, firewall configuration, and make recommendations to consolidate rules or ACLs wherever possible. However, there is still a need to review the policy and remove obsolete rules, services, reposition for performance, and policy compliance.

This paper explains the importance of regular reviews and clean up and suggestions for a process to do so and good practices to make the Rule Review easier. There are vendors offering automated products to assist with this type of review i.e. Lumeta. There are also vendors that offer to perform this task for you for a price, i.e. ESTec Security. Automated products and vendors services can help but they cannot substitute for the knowledge of the network, research, and customer interface. It is a tedious and thankless task and requires time and effort. Deleting rules could possibly break a connection and any outages could be costly. However, it is important that these reviews be performed carefully and regularly. Therefore, a process to continually clean up obsolete rules and ACLs should be in place. Proper documentation and a rule change process are also important when the time comes to remove an old rule.

Most examples refer to Checkpoint and Cisco PIX Firewalls, but apply to most any firewall product.

What is a Firewall Rule Review?

There are vulnerability assessments, to ensure that the firewall is not vulnerable to the latest exploits. There are official audits that check for vulnerabilities, firewall software configuration, and Security Policy. In addition, they make sure that the most recent patches are installed for the firewall software and OS. However, there is still a need for a Rule Review performed by the Firewall Administrator and/or Network Security Officer concentrating on the way rules are configured. Step through the firewall rules one by one to make sure that they are in the proper order. Check if the way the rules are written creates obvious holes,

[1] http://www.allasso.pt/base/docs/11031796360.pdf

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

such as vulnerable services or rules that have a range of ports or all port/all protocols. Check for obsolete rules, rules that should have been temporary, or rules that are no longer used. Ensure that proper paperwork is in place for contact information and purpose of the original rule. Try to consolidate rules when possible.

Reasons for the Rule Review

Suppose a request comes in that has a six-month exception granted by the Security Officer. It is a request to allow access to a vendor using an obscure port until the vendor can recode his application to use the Internet Proxy server on port 80 (http) or 443 (https). The firewall rule is implemented and if you are using Checkpoint Firewall, it is possible to enter text in the comment field "Added 5/6/03, delete on 11/6/03" or something similar to that. Six months later, will someone remember to go back and delete that rule when it is no longer needed? Is there enough information or history available about the rule to ensure it will not cause an outage if deleted. If you are using a PIX or router, there would be no place to put a comment. If there is no process to go back and cleanup, the rule/ACL could eventually be used to gain unauthorized access to your network. Suppose that rule is used to compromise an internal host and in the investigation, they find that the rule should have been removed two months ago.

In some cases, the chances are minimal that the obsolete firewall rule could be used for malicious access. It might have been configured with specific source and destination. This would greatly reduce the risk of unauthorized access. Removing that rule is still important for performance reasons. The more rules the firewall reads through to make a decision on a connection the more CPU processing required by the firewall. Large rule sets will cause performance and throughput degradation on most firewall products.

Many firewall products allow for grouping objects together such as hosts, networks, or services. Checkpoint has stated that using groups will cause more overhead for the firewall. Groups can also hide mistakes when implementing or changing policy. Objects can be added to groups inadvertently, groups might contain some obsolete objects, etc. When reviewing the policy it is important to review the contents of a group and if any obsolete objects are in that group. Checkpoint Firewall version 4.0 and above provides some assistance when cleaning up old objects. When attempting to delete old objects, Checkpoint alerts if the object is in a group or used in a rule and where.

When responsible for a many firewalls with large rule bases, it is possible to make mistakes. It's possible to erroneously open up more than intended. Firewall Administrators are usually the last ones to be involved in a project and are usually under a crunch to get something done to complete the project. Many times that causes a hasty decision when implementing firewall rules. Therefore, it is necessary to go back and take a look at what is there, be familiar with the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

connections that are allowed, make sure that the company security policy is being enforced, and remove unused rules.

Firewall Rule Change Process

In a Network Security Office where more than one person is making firewall rule changes, there are going to be some difference in implementing rules and naming objects. Some administrators may not take the time to review previous firewall rules before implementing a new one. They may not review the order of the rules to select the best location for the new rule. The more users with the authority to change firewall rules, the more clean up required especially if there is no process in place. Maybe there is a request that the administrator misunderstood, maybe he felt pressured to put something in for an executive, or he missed that there is another rule that would have taken care of this new connection

With a process in place, all administrators are completing the changes in the same manner, and this will make the Rule Review easier. The following are suggestions for a Firewall Rule Change process.

Naming convention

One crucial part of the process is naming conventions for objects, groups, and networks. When creating object names, there should be written guidelines on how the company has decided to do that. Many times with several administrator each having their own preference on how to name objects, can make a firewall rule base confusing to administer. The standards should address how objects are named by identifying specifics for hosts, networks, service, and subnets so they are unique. The standards should also address when to use groups. Having a standard that makes sense and providing that to the new administrators will save time with the day-to-day changes as well as the Rule Review.

Research

Another part of the process, is researching the firewall rule request. Oft times requests are put in as a new rule and the administrator didn't research the request to make sure it is not going to open up a vulnerability that the requestor was not aware of. Also, review the rule base to determine if another rule might cover this connection or that it can be added to an already existing rule. Rule placement should also be considered. If the firewall is natting, it is important to check for any issue there before installing the new rule or change an existing rule. With a large rule base, research can be tedious, but there are tools that can help, depending on the firewall product and the platform. If running Checkpoint Management Station on a Unix platform, it is easy to parse through the rule base using a pearl script called "fwrules.pl" at http://www.geocities.co.jp/SiliconValley-Cupertino/8240/en/index.html. This script will take the "FWDIR/conf/rulebase.W" file and produce a text file that can

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

be searched through to find rules easily. The Checkpoint Gui's search option does not work as well or as efficiently as this script does on the raw file. For Cisco PIX, cut and paste the ACLs and nat statements to Notepad and search through.

Documentation

Documentation explaining when and why rules are created is important but often non-existent. Many times, the administrator receives an e-mail request; someone stops by the office with a special request, etc. Rules are created with no documentation. Administrators leave and they take the information about the firewall rules with them.

Firewall rule requests should have an official process through an online ticketing system or request form. Once a process is in place, rule request should not be accepted in any other manner. These should be stored with the Administrator as long as the rule exists on the firewall. This may require keeping hardcopies of the online ticket. Firewall rules could have a life of several years. The documentation should be there for any Administrator to refer to as needed. The documentation will have contact information of the requestor, their organization, and the reason for the request.

In addition to the documentation described above, Checkpoint has a place to put a comment on each rule. It is not a large enough field for contact name and information, especially if a rule has been consolidated with other rules. There is room enough for a request number, date, and initials of the administrator that created the rule. This would make it easy to locate the paperwork with the information needed to proceed. Cisco Device Manager provides a place for comments as well, where information to assist with locating the paperwork can be stored. Other uses for the comment field is to note that the rule is temporary and when it should be deleted.

Reports

Reports on the performance and usage of the firewall should be pulled and stored for approximately two months. These reports should include the firewall rules and their usage. This will come in handy when reviewing the rules to find those that are no longer needed. A regular backup of the rule bases should also be stored for 2 months.

Logs

Logs should be archived for as long as the disk space will allow. Checkpoint provides a utility that converts the logs in ASCII. This utility can be used in a script to compress those files using "gzip" and store the logs by date. Appendix A is an example of a script that a colleague wrote to dump logs to ASCII and store them compressed with "gzip" and named by date. They are then easy to view using "zgrep" on Unix. If using Windows, sort and view ASCII log files with Notepad and Excel. If file is not too large, MS Access can be used as well.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

There are some PIX log analyzers available on the Internet and from third party vendors; one example is at http://www.eventid.net/firegen/pixsample_report.htm where there is a sample report. It could be helpful when reviewing PIX logs or specific activity.

The Rule Review

Document

Document the progress and findings of the Rule Review possibly in a journal or spiral notebook, dedicated to the review. The Rule Review could take several weeks to perform and is impossible to do in one sitting. Especially when there are daily operations ongoing. Sometimes it is necessary to monitor a rule or activity for a time; the documentation will assist with keeping track of the progress.

Security policy

The first thing that an auditor would ask for is your security policy. This should be part of the Rule Review also. Make sure that there is a current security policy and that this policy is being enforced by the firewall. If they don't match, alter the Security Policy or alter the firewall rules. Altering the firewall rules could cause an unforeseen outage, so it must be done carefully using the process described later in this paper. Document the changes that are required from the Security Policy Review.

Rule usage

The next step is to run a report to find out the number of hits each rule is getting on the firewall. Some firewall products provide those reports to you by default, if not third party products and free tools are available on the Internet. For Example, Checkpoint does not offer a report that provides that information, however, there is a site http://www.phoneboy.com where you can find numerous tools and helpful information regarding Checkpoint firewalls and other Checkpoint products. From the Phoneboy website, there is a link to a script written by Peter Sundstrom called "fwlogsum" at http://www.ginini.com/software/fwlogsum/sample.html, which provides useful statistics about the firewall, and one of those is the rule numbers in the order of hits called "Rule Usage". Currently it produces the top ten rules used and their usage. This script could be changed slightly to provide the entire list of rules with the number of hits for each. It would be good practice to pull this type of report regularly and store it somewhere for the Firewall Policy Review. If changes are made to the firewall once per week, then this report should be pulled weekly. If changes were made daily, then it would be best to pull them daily. The reason is that with some firewall products, the rule numbers change when a rule is inserted. This will give you inaccurate results on the rule usage report. Therefore, it is important to take regular copies of the rule bases as well. This

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

way the rule usage report can be correlated with the rule bases for that date to determine the rule numbers at the time of the Rule Usage report.

Below is the “Rule Usage” section of a sample report from Peter Sundstrom fwlogsum script. What it is showing is that out of an example Checkpoint rule base the top ten rules used. This indicates that only two of the rules from the rule base were used during the period of this report. Rule 4 is used the most with 265 hits followed by rule 3 which had only 45 hits during the report period.

[2]Rule Usage: Top 10 of 2

Rule	Count	Of Total	%
Rule 4	265	85.48%	
Rule 3	45	14.52%	

This information is important for two reasons. It is important to know what rules are your “heavy hitters” because most firewall products start at rule 1 (or 0) and go through the list until it finds a match. If you have a rule that is being used heavily, as shown in the example above, it should be repositioned. Rule 4, which is handling 85.48% of the connections, should be moved above rule 3 or even in the first position, if possible, to decrease the processing required by the firewall to step through several rules to find a match.

The other use for this information is to find the rules that are not being used. That is why it would be helpful to pull a similar report periodically and store them for two months or more. This way you can refer back to those archives to determine how much the rule has been used. Keep in mind that each time a rule is inserted in the rule base of some firewalls that the rules below the insert are renumbered, so compare results to the rule base archives. In the example above it appears that Rule 1 and 2 were not used during this report period. This could mean many different things. Rule 1 could be the “stealth” rule that protects the firewall itself. Most times this rule would not be used unless someone was trying to connect directly to the firewall from outside or inside the network. Typically, this rule would be towards the top of the rule base. It could be that Rule 1 and 2 were just not used during this report. If that is the case, they should be repositioned, if it makes sense in the overall rule base. It’s possible that logging is not turned on for those rules since the report uses the log file to determine the “Rule Usage”. It could be that the rules are not needed and should be reviewed and deleted.

[2] http://www.ginini.com/software/fwlogsum/sample.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

As mentioned above, this information may not be easily collected depending on the firewall product you are using. Cisco Pix logs can be sent to a syslog server and from there, create a script that will pull information about the source, destination and port activity, but it will not provide you with the rule/ACL that it used for that connection. Cisco has introduced a Gui that can be used for administration of PIX and other Cisco products. Cisco Secure Device Manager provides some statistical reporting as described at http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/ver31/user_gd/log/lrn02.htm#xtocid2, which can be helpful, but cannot provide the activity on each rule. When entering rules into the Device Manager or Secure Device Manager Gui, the rules are given numbers. However, the Gui converts those rules into ACLs and enters them into the PIX just as though it were done by command line. Therefore, you have a list of ACLs that are ordered in the manner chosen on the Gui. The Gui or the PIX will not indicate if the rules should be repositioned. For example, if a generic rule is hiding a more specific rule below. Therefore, the Policy Review should include inspection of the position of the ACLs not only for performance but also for logical positioning. In the case of the PIX, it would be necessary to review each rule and logs to determine which ACLs are being used and which are not.

Obsolete rules

Document the findings of the report review and the rules that are showing as not being used. Any rule that has not been used for a particular period should be reviewed thoroughly. First, make sure that logging is turned on for that rule since we are using the logs and archive rule bases to determine rule usage. If logging is turned on review the previous "rule usage" reports and the rule base archives to see if the rule has been used in the last two or so months. If logging is not turned on, turn on the logging, document in the comments logging is turned on, why, and the date that the rule should to be revisited. Document this in the findings with an explanation and mark on the calendar to revisit that rule in a week or two. How long to log the rule for usage, depends on what the rule is and the reason for the initial request.

Even if a rule is marked "temporary" and is overdue for deletion, review and the contact the originator before deleting as described later in this paper.

Review the logs

If there has been no activity, the next step is to check the logs for activity using the source, destination, and/or ports. This is important because the connection may be using another rule. There could be a more generic rule above or one using a group that includes the host or network. Checkpoint will verify the rule base to prevent the administrator from putting a rule in that hides a rule below. However, there could be a case in which a group is used containing the object or network and allows the connection. As mentioned above, the PIX will not verify the rules are logically positioned, so it will require a closer look.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The Checkpoint logs can be reviewed from the archived ASCII format mentioned in the Firewall Rule Change Process section. Scripts can be run after hours searching for specific source, destination, and port combinations and provide reports for review the next morning. Document the scripts, what they are pulling, and report names. One suggestion is to use the rule numbers for the report names.

The PIX has a different format than the Checkpoint for logging. Checkpoint will only log the Syn packet where the PIX will log each step of the transaction. The log files will probably be a little larger in order to get the information needed to determine which rules are being used. "Informational" level will provide an entry for each built connection and the teardown. If sending the logs to a Syslog server, it would be possible to grep through the logs and pull out only "built" connections for a specific IP address. As mentioned above, some vendor products provide reports that could assist in the analyses of the PIX log files. Below is a portion of a sample report from http://www.eventid.net/firegen/pixsample_report.htm.

The first portion of the sample report gives a count of the number of times the connection was built or torn down. This could be used instead of parsing through the Syslog entries for Source and Destination. However, with a busy firewall, this could be a very large report.

The second and third portion of the sample report shows the top 50 services and destinations used. This will assist with rule positioning. Compare these top 50 services and destinations to the ACLs and reorder the ACLs accordingly.

[3] Severity level 6 (Informational) details for the 172.17.250.4 firewall. Back to top

No	First Message	Last Message	Code	Message	Count
1	01/24/03 00:00:15	01/24/03 00:03:32	6-302013	Built outbound TCP connection nnnnn for outside:63.251.224.177/1521 (63.251.224.177/1521) to inside:172.18.10.99/nnnn (216.13.68.100/nnnn)	14
2	01/24/03 00:00:00	01/24/03 00:03:32	6-302014	Teardown TCP connection nnnnn for outside:63.251.224.177/1521 to inside:172.18.10.99/nnnn duration 0:00:01 bytes 86 TCP FINs	13

[3] http://www.eventid.net/firegen/pixsample_report.htm

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Top 50 protocols used for the 172.17.250.4 firewall. Back to top

No	Protocol	Connections	%	
1	53 - dns	65	28.5	
2	514 - syslog	50	21.92	
3	1521 - oracle	23	10.08	
4	139 - netbios	15	6.57	
5	1984 - big brother	14	6.14	

Top 50 Destinations for the 172.17.250.4 firewall. Back to top

No	Destination	Connections	Protocols
1	63.251.224.177	14	TCP/1521 – oracle
2	65.244.21.149	5	TCP/1521 – oracle
3	205.151.222.254	4	UDP/53 – dns
4	192.168.0.218	4	TCP/42 - ms wins,UDP/138 - netbios,UDP/161 - snmp,UDP/44787
5	10.42.0.164	4	TCP/2049 - nfs,TCP/22 - ssh
6	10.42.0.141	3	TCP/25 - smtp,UDP/138 - netbios
7	10.42.0.162	2	TCP/1521 - oracle,TCP/22 - ssh
8	12.129.129.149	2	TCP/1521 – oracle

Contact the initial requester

Once decided that a rule is a good candidate for deletion, the next thing is to get the approval from the originating organization. This is where the documentation for the original rule request is important. If documentation doesn't exist, there might be something in the comments field for that rule, or the subnet in the rule will give some idea as to where the rule change originated. Collect up the findings for the rule, contact the originator, and follow up with e-mail. E-mail follow up is needed for documentation purposes. The e-mail should include all the information collected about the rule, when it was last used, why it was created, who signed off on it, and/or the date of creation. The e-mail should also include the proposed date for deleting the rule, so they know when they need to respond.

NOTE: IP addresses are considered sensitive information and should not be sent in clear text in e-mail. We are assuming that e-mail is internal to the company, if not, encryption should be used.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Use change control
Before deleting a rule, it is imperative to get some sort of written approval to do so. Deleting a rule can be risky. The Change Control Committee would come in handy for this process. Having to go through a Change Control Process for each firewall rule change would be difficult, but for this type of change, it can be a good way to get the word out and for coverage if it causes an outage.

The Change Control Committee should consist of a representative from each organization or business unit. Submit the change control and clearly explain what will happen and the back out plan. It might make sense, depending on the rule being removed, to mention that it will be monitored for two days for any problems. Set up a script to watch for denies for that particular connection. Document that nothing was found and file.

Check logical order of Rules

After obsolete rules have been successfully deleted without incident, pull another report on rule usage. Make sure that the heavy hitters are towards the top of the rule base. For the PIX, review the ACLs and determine which ones will get the most activity by matching the ACLs with the PIX analyses reports either provided by CISCO or a third party vendor.

Check object groups

Also, check the rule base for the use of groups. It could be that the Firewall Change Process says, "Use groups only for objects of 5 or more". Check groups to make sure they still comply with the standards. An object could have been deleted which would make the group unnecessary. Since groups can cause performance issues, remove any groups as needed. Even though groups can be used when configuring the PIX using the Secure Device Manager or the Device Manager, the PIX configuration will not show the groups. Therefore, groups will not affect the efficiency of the PIX. However, the Device Manager should be cleaned of obsolete groups.

Obsolete objects

The Rule Review will identify obsolete objects for deletion. These can be deleted without a change control approval. Prior to Checkpoint Version 4.0, it was necessary to review the rule base for an object before deleting. However, as mentioned above, Checkpoint 4.0 and above alerts the administrator that the object is being used in a rule or group before it completes the delete. Beware of groups of services. It is far too easy to slip a service into an existing group and put the network at risk.

On the PIX command line configuration, IP addresses are used in the ACL, and are not saved as objects; therefore, there are no objects to remove. However, if using one of the Device Managers, objects are created and should be cleanup as needed form the management device.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Consolidate rules

The research from the initial Rule Review will identify some rules that can be consolidated. Take another look and to see if there are any others. For example, if a rule has several sources going to the same destination or visa versa.

Summary

Firewall Rule Review is looking at the configuration, position, and clean up rule bases. Should be done on a regularly because of "*security erosion"* which is caused from improper maintenance of the firewall and putting the system at risk.

Reasons for the review:

- Obsolete rules can be used to obtain unauthorized access.
- Rule position can improve the performance of the firewall
- Use of groups can cause performance issues
- Improper configuration of a rule can put the firewall and/or network at risk

Firewall rule change process can help:

Standards and processes for firewall rule changes will assist the administrators to make the changes in a uniform manner.

- Naming standards for objects (hosts, networks, groups, services, etc)
- Research the rule change request and what it means to the environment
- Process to review existing rules for possible consolidation
- Implement a formal process for requesting firewall rule changes
- Document rule changes and requestor information
- Compress and store logs in easy to read format such as ASCII
- Archive statistic on firewall rule usage, performance, and copies of the rule base.

Firewall Rule Review:

- Needs to be performed by someone with knowledge of the environment (technical and political)
- Document the progress
- Check firewall rule usage reports and logs to find obsolete rules
- Contact requestor and use Change Control Process to delete obsolete rules
- Check for logical order of the rules
- Check rule placement for performance
- Check for obsolete groups and objects
- Consolidate rules where possible

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix A

Below is a script used in a Checkpoint environment that will save the logs to a directory named as the month and then in a file named with the date. They are saved in ASCII using the "logexport" utility provided by Checkpoint and then compressed using "gzip".

This script also runs the "fwlogsum" mentioned on page 5 of this paper, which analyzes the logs and provides helpful statistics about the firewall.

```
#!/bin/sh

FWDIR="/opt/CPfw1-41"
PATH=".:/usr/local/bin:/usr/ccs/bin:/usr/sbin:/usr/bin:/usr/opt/SUNWmd/
sbin:/opt/CPfw1-41/bin:/opt/CPrt-41/bin"
MONTH=`date +%b`
/opt/CPfw1-41/bin/fw logswitch
FIRST=`ls -tral /var/opt/CPfw1-41/log/[0-9][0-9]$MONTH*.log | tail -1 |
head -1 | awk '{print $9}'`
BASEFIRST=`ls -tral /var/opt/CPfw1-41/log/[0-9][0-9]$MONTH*.log | tail
-1 | head -1 | awk '{print $9}' | sed -e 's/\.log//'`
LOGTODO=`echo $FIRST | sed s/:/_/g |cut -d\/ -f6 `
MYDATE=`date +%d%b%Y`
HOUR=`date +%H`

if [ ! -d "/checkpoint-oldlogs/$MONTH" ]; then
  mkdir -p /checkpoint-oldlogs/$MONTH/ascii
fi
if [ ! -d /checkpoint-oldlogs/$MONTH/ascii ]; then
  mkdir /checkpoint-oldlogs/$MONTH/ascii
fi

/opt/CPfw1-41/bin/fw logexport -n -i $FIRST -o /checkpoint-
oldlogs/$MONTH/ascii/$LOGTODO 2> /dev/null
/usr/local/bin/gzip  $BASEFIRST*
/usr/local/bin/gzip  /checkpoint-oldlogs/$MONTH/ascii/$LOGTODO

if [ "X$HOUR" = "X23" ]; then
  cd /var/opt/CPfw1-41/log
  mv $MYDATE*.log.gz /checkpoint-oldlogs/$MONTH/
  cd /checkpoint-oldlogs/$MONTH/ascii
  gzip -dc $MYDATE* | /usr/local/sbin/fwlogsum -l - -S -P 30 -T -o
fwlogsum-$MYDATE.html
  cp /checkpoint-oldlogs/$MONTH/ascii/fwlogsum-$MYDATE.html /opt/fw-
web/fwstats/
  chmod 444 /opt/fw-web/fwstats/fwlogsum-$MYDATE.html
  rm /opt/fw-web/fwstats/Today.html
  ln /opt/fw-web/fwstats/fwlogsum-$MYDATE.html /opt/fw-
web/fwstats/Today.html
fi
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

Rhoades, David. Auditing Routers and Firewalls. Sans 2001, Baltimore, Maryland May 2001.

Edlridge, Brett. "Biggest Firewall Maintenance Mistakes". http://www.allasso.pt/base/docs/11031796360.pdf

Lumeta Corporation. "Firewall Project". 2003. http://www.lumeta.com/figrewall.html

ESTec Security. "Firewall Rule Set Audit". 2002. http://www.security.estec.com/products_services/services/firewallruleset_audit.htm

McGraw-Hill. "Firewalls Complete – Firewall Maintenance". Oct 16, 2002. http://www.windowsecurity.com/whitepapers/Firewalls_Complete__Firewall_Maintenance.html

Nakatsuma, Johta. "Johta Nakatsuma Repository". May 13, 2002. http://www.geocities.co.jp/SiliconValley-Cupertino/8240/en/index.html

Holcomb, Jason. "Using the Cisco Pix Device Manager". http://www.giac.org/practical/GSEC/Jason_Holcomb_GSEC.pdf

Jan 5, 2003. http://www.phoneboy.com/fom-serve/cache/111.html.

Sundstrom, Peter. Ginini Technologies Software. Mar 1, 2003. http://www.ginini.com/software/fwlogsum/

Brenton, Chris. Mastering Network Security. Published by Sybex Network Press. 1999

Karl Wiegers, Karl. "Requirements Engineering". Taken from Software Requirements, 2nd Edition was published in 2003 by Microsoft Press. Change Control Process. http://www.processimpact.com/process_assets/change_control_process.doc

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.