Interested in learning more about security?

SANS Institute
InfoSec Reading Room

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

Improving Firewall Security post Acquisition

This paper aims to discuss the challenges in putting together a secure Check Point Firewall-1 solution to protect our existing information and assets and that of our new acquisition. It is assumed that the reader will have a generic knowledge of firewalls, related terms and their use. In the paper the word 'policy' refers to the security document and the word 'rulebase' refers to the Check Point rules.

Copyright SANS Institute
Author Retains Full Rights

AD

Improving Firewall Security post Acquisition

Maree Connolly

Submitted for SANS GIAC GSCEC Practical

Assignment version: 1.4b, option 2

28 July 2004

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

Abstract

This paper aims to discuss the challenges in putting together a secure Check Point Firewall-1 solution to protect our existing information and assets and that of our new acquisition.

It is assumed that the reader will have a generic knowledge of firewalls, related terms and their use. In the paper the word 'policy' refers to the security document and the word 'rulebase' refers to the Check Point rules.

History

Our organisation is a large financial institution that focuses on retail consumers and small to medium sized businesses. Formed historically from a number of mergers and acquisitions the organisation recently purchased another similar company including its products and IT services. These IT services, merged with our own, offer support to business units such as 24/7 Call Centres, retail branch and agency networks and an Internet presence. The challenge for the IT department was to continue to provide 24/7 availability of its IT systems whilst merging and integrating the recently acquired systems. The integration of these systems was an enormous task and a small component of this involved securing the network.

Before snapshot

Previous audits of the firewall environment had highlighted risks that needed to be mitigated. This work was implemented alongside the integration of the firewall rulebases. To assist in the understanding of the differences between the two organisations I have referred to our systems as "existing" and the acquired systems as "inherited". The following points outline the problems and opportunities identified:

Check Point Firewall-1

Check Point Firewall-1 was in use at both organisations. A decision was made to continue to use Check Point as our firewall software.

Security staff were not retained

None of the security staff from the acquired organisation had been retained. Communication between the two organisations was at times difficult and added to the challenge of trying to understand the inherited firewall rulebases.

Limited documentation of inherited firewall rules

Documentation of the inherited rules was extremely limited and was recorded in the inherited organisation's service request software. We did not have access to the service request software so could gain little from the references in the firewall comment field.

© SANS Institute 2005, Author retains full rights.

The methods of naming and grouping Objects, Networks and Groups in the inherited rulebases were unfamiliar and poorly commented, if at all. Due to this we had very little idea as to the identity of what each object represented. The inherited firewall rulebases used Object names based on IP rather than descriptive names. The comment field in the Object definition was not used.

Unavailable Firewall Security Policy

A Firewall Security Policy from the inherited organisation was not made available to assist in the understanding of how the rules were formed.

No knowledge of inherited applications

The applications being secured by the firewall rulebases were not fully understood. In many instances we were not aware of what groups of rules might be applied to what applications.

Last review of inherited firewall rules unknown

The "currency" of the rules was unknown. We could not be sure which rules were still active and which rules may have been obsolete.

Software revision levels outdated

The software revision levels in the existing environment were outdated and did not have vendor support.

Complexity of existing firewall rulebases

The existing firewall rules were difficult to manage, complex and disorderly.

In summary, the rules may have permitted more traffic than necessary, and as a result there may have been an increased opportunity for unauthorised access to services and applications.

Lack of information on acquiring foreign firewall rulebases

Information on how to approach the securing of a network by firewalls after an acquisition is extremely limited. Technical information regarding how to merge firewall rulebases is available from various Internet URLs such as www.checkpoint.com[1], however published methodologies and experiences of other organisations are rare.

During Snapshot

We set up a project team of specialists to consider the options for merging the organisations' firewalls. These specialists represented the following teams:

© SANS Institute 2005, Author retains full rights.

Firewall Team – The Firewall Team is responsible for performing the operational firewall tasks to secure the applications and services of the organisation.
IT Security Team – The Information Technology Security Team's role is to assist the organisation in achieving and maintaining industry accepted practice in the areas of IT security and disaster recovery.
IT Audit – The IT Audit team monitors and evaluates the effectiveness of the IT policies within the organisation.
IT Project Office – The Project Office provides project management rigour and governance to deliver IT operational initiatives.
External Vendor – The Vendor provides expertise in both the Firewall Software and Hardware Systems.

The project team obtained executive approval for the approach chosen and was to communicate on a regular basis with a steering committee. The project would be planned using the methodologies provided by the Project Office including Release and Test Strategies. To gain approval for the project we considered the following alternatives:

Start from scratch

Starting from scratch would involve creating new rules for each firewall. We called it the "big bang" approach. This would involve applications owners and all those requiring access to submit a service request outlining Source, Destination, Service and reason for requesting access. This information would be analysed by the team and a decision made whether to allow or deny. A rulebase could be readily formed based on these requirements and would not allow excess access. Although this would allow for well-understood and current firewall rules, it was discounted as an option due to the required outage and disruption to production services. Additionally, there was the risk that many application owners did not know how their respective applications used the firewall.

Enforce our security standards

All users from the acquired organisation could be forced to access applications and services via the same methods and procedures as those in place for the existing organisation. This would result in a reduced rulebase and a more easily understood operating environment. Although considered beneficial for the firewall administrators, it was not considered a viable business alternative as there was not the time or budget to train users in new procedures, have new software installed, provide additional IT support etc in the timeframe allowed. Also, some of the applications in use by the acquired organisation were unique, and an alternative was not available in the existing organisation.

Enforce our Firewall Security Policy

Our Firewall Security Policy would be used to remove or tighten any rules in the inherited rulebase that did not comply. The project would undertake a review of the firewall rulebases based on this objective with the undertaking

© SANS Institute 2005, Author retains full rights.

that we would try to minimise the impact to the production environment. This was the approach that was chosen

Continue to operate separate firewall rulebases

Keeping the firewalls of both organisations separate would help maintain the continued security of the existing organisation. The project team reviewed the rationalisation savings and deadlines and agreed that this solution could not be maintained much past the short term.

A decision was made to merge the firewall rulebases and to tighten the resultant firewalls and object database. This decision was made after considering the costs, resources, business continuity and overall security as outlined above. The project was split into two major implementation streams:

- Firewall upgrades;
- Rulebase cleanup.

Firewall Upgrade

Our firewall architecture consists of Nokia firewalls installed with High Availability using VRRP. Check Point FW-1 is installed on these firewalls and is managed centrally from an Enterprise Management Server. The firewalls are operating in an “active / backup” arrangement with the active firewall referred to as the “Primary” and backup as “Secondary”.

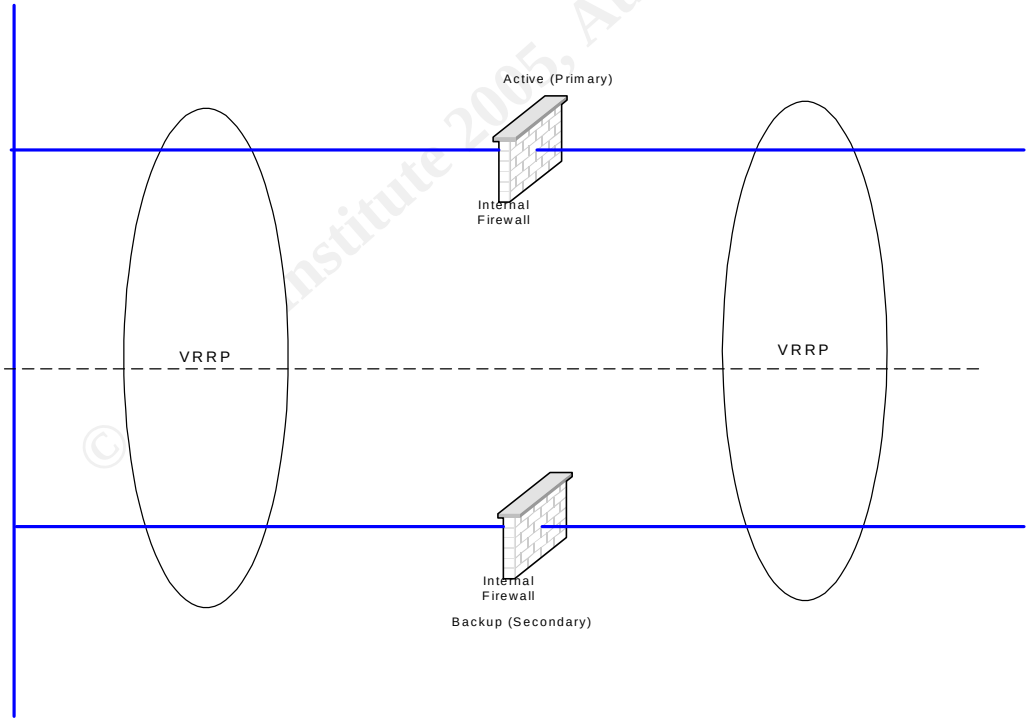


Figure 1 Architecture Diagram demonstrating VRRP

© SANS Institute 2005, Author retains full rights.

The firewalls had inconsistent versions of the operating system and patch levels. The Check Point software was also revisions behind although consistent across all firewalls. We planned to upgrade both the software and operating systems to bring them into line with current revision levels and to ensure vendor support. Along with the upgrades, a set of management procedures would be written to allow anyone in the Firewall team to build a Check Point firewall and manage it within our environment. The procedures were also to be used as the standard for any other firewall or management equipment introduced. The steps taken to upgrade were as follows:

- Switch the active firewall from being the primary firewall to the secondary firewall. To ensure the secondary firewall was functioning correctly we operated it as the primary firewall for a week before upgrading the usual primary firewall.

- At the end of the week, upgrade the usual primary firewall (which is now the secondary) and carry out connectivity and operability testing. The testing should focus on components that could potentially be impacted by the firewall change. For example, it would not make sense to perform bounds testing, application logic testing, or a data flow analysis. A sensible approach is to ensure various application components can still inter-communicate after the firewall change.

- A script was to be written to partially automate some of the testing tasks. It is not a substitute for any manual testing, rather a tool that can be used to quickly assess any problems with network connectivity across the network resulting from the firewall upgrade. The advantage of using a script to perform such tests is the consistency. If the script is run before and after the upgrade, the results can be compared as a simple method to determine if there was any connection issues. The main goal of the script is to attempt TCP connections to various IP addresses. The results are logged to a file. Whilst the automated testing method will be a valuable tool in quickly assessing the general availability of services, manual testing procedures will still be required, and are a vital task in ensuring the success of the change control process. The manual testing will also be required in instances where a particular function cannot be easily automated.

- On the successful conclusion of these tests, switch the upgraded firewall back to being the active primary firewall.

- Perform appropriate testing again.

- If problems arise as a result of the upgrade that cannot be quickly resolved within the scheduled cutover time, commence the back out strategy detailed below.

- Run on the upgraded firewall for a minimum of one week, monitoring performance and network connectivity.

© SANS Institute 2005, Author retains full rights.

- If no issues arise as a result of the upgrade to the primary, proceed to upgrade the secondary firewall.

- Upgrade the secondary and carry out local testing.

- Switch the active firewall from being the primary firewall to the secondary firewall.

- Perform appropriate testing.

- If problems arise as a result of the upgrade that cannot be quickly resolved within the scheduled cutover time, commence the back out strategy.

Back-out strategy: Switch the active firewall from being the primary firewall to the secondary firewall. This can be accomplished in a number of ways, with turning off the primary unit as a simple method of performing the switchover. The failed unit can then be disconnected from the production network, and a post-cutover diagnosis performed to try and identify the problem.

This method resulted in the least outage for the organisation.

Rulebase Cleanup

Document rulebase clean up objectives

A level of skill and experience of the firewall administrators selected for the project was assumed. To enable me to contribute to the project with the latest security information I was granted permission to attend the SANS GSEC Mentor Program. This program enhanced my understanding of the information available on The Twenty Most Critical Internet Security Vulnerabilities[2] list. This list contains "the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited vulnerable services in UNIX and Linux." In many instances I was able to gain practical hands-on experience in using tools[3] to exploit the vulnerabilities contained in the list. The knowledge gained by using the tools would also be used extensively through the project.

At the end of Top Twenty Vulnerabilities List is an Appendix A titled Common Vulnerable Ports[4]. This document states that "Blocking these ports is a minimum requirement for perimeter security, not a comprehensive firewall specification list. A far better approach is to block all unused ports". This approach is adopted by my organisation and in addition I regularly monitor the Top Twenty Most Critical list.

To achieve consistency in delivery a set of objectives were formed by consensus of a team made up of representatives from IT Security, IT Audit, and the Firewall administrators. These objectives formed part of the standard to be followed in analysing the rules.

© SANS Institute 2005, Author retains full rights.

- The rulebases must adhere to the firewall policy document produced by the IT Security team.

- All rules identified in the rulebase with “ANY” in the Source, Destination, or Service field must be analysed and made more restrictive.

- Unused rules are to be removed. An unused rule was defined as a rule that does not appear in the Check Point Logs for a minimum of 5 weeks.

- Every rule must be richly commented. The comment field must contain at a minimum the business purpose and preferably the service request number and date, and the firewall administrator’s initials.

- Rules relating to business applications were to be grouped together into the rulebase.

- The rulebase should be ordered in a manner that enhanced readability, and on going maintenance and auditing of the firewalls.

- All network objects used within the rulebases were to have descriptive comments added. This did not apply to default objects that are included in the base installation of the Check Point Firewall.

- All unused objects were to be removed.

- All network object names were to conform to the standard of the existing organisation.

- All Automatic NAT rules were to be removed and manual NAT rules implemented.

- Any opportunities to consolidate the rulebase, without impacting security or manageability, were identified. Rules that provide similar functions were to be identified and merged where possible.

With these objectives in mind we were ready to begin the cleanup. The first task we had to undertake was to merge the different firewall rulebases and their object databases.

Merge Firewall Rulebases

The firewall rulebases and the objects databases were merged using the procedures located on Check Point’s Internet Knowledgebase. Although password protected on the Check Point web page, the procedures for merging Check Point firewall rulebases are freely available at a number of other web pages.[5]

© SANS Institute 2005, Author retains full rights.

To merge the rulebases takes two steps:

1. Merge the Objects.C databases
2. Merge the Rulebases

After carefully backing up all copies of firewall rulebases and Object databases, the merge procedures were followed. We did not encounter any problems during any of the documented steps and the end result was a combined single Objects database and combined rulebases.

Methodology of Cleanup

The Rulebase Cleanup consisted of a series of Change Release cycles that contained packs of approximately 50 rules. The Change process involved a series of communications, signoffs and scheduling exercises to gain approval for the change to the implemented. The following methodology was used to ensure the rule packs met all the requirements of the change process.

Audit merged rulebases

The firewall rulebases from both organisations were inadequately commented such that the applications and services making use of the rules were unknown or unclear. One of the first steps in the review of the rules was to understand the applications and the services being used. As part of the project team I was tasked with the analysis of these rules both for some of the existing firewalls and the acquired firewalls which had been merged. To enable an inspection of the logs, all rules were to have logging enabled.

Log all rules

As part of the clean up I had to identify whether a rule was still in use. To assist me in doing so, logging was set to “LOG” on all rules and the firewall rulebase installed some weeks prior to the start of the series of change releases. This enabled me to identify lesser-used but still important data, such as end of month processing.

With logging enabled on all rules I was ready to commence the analysis of the rulebases. A diagram representing this process follows:

© SANS Institute 2005, Author retains full rights.

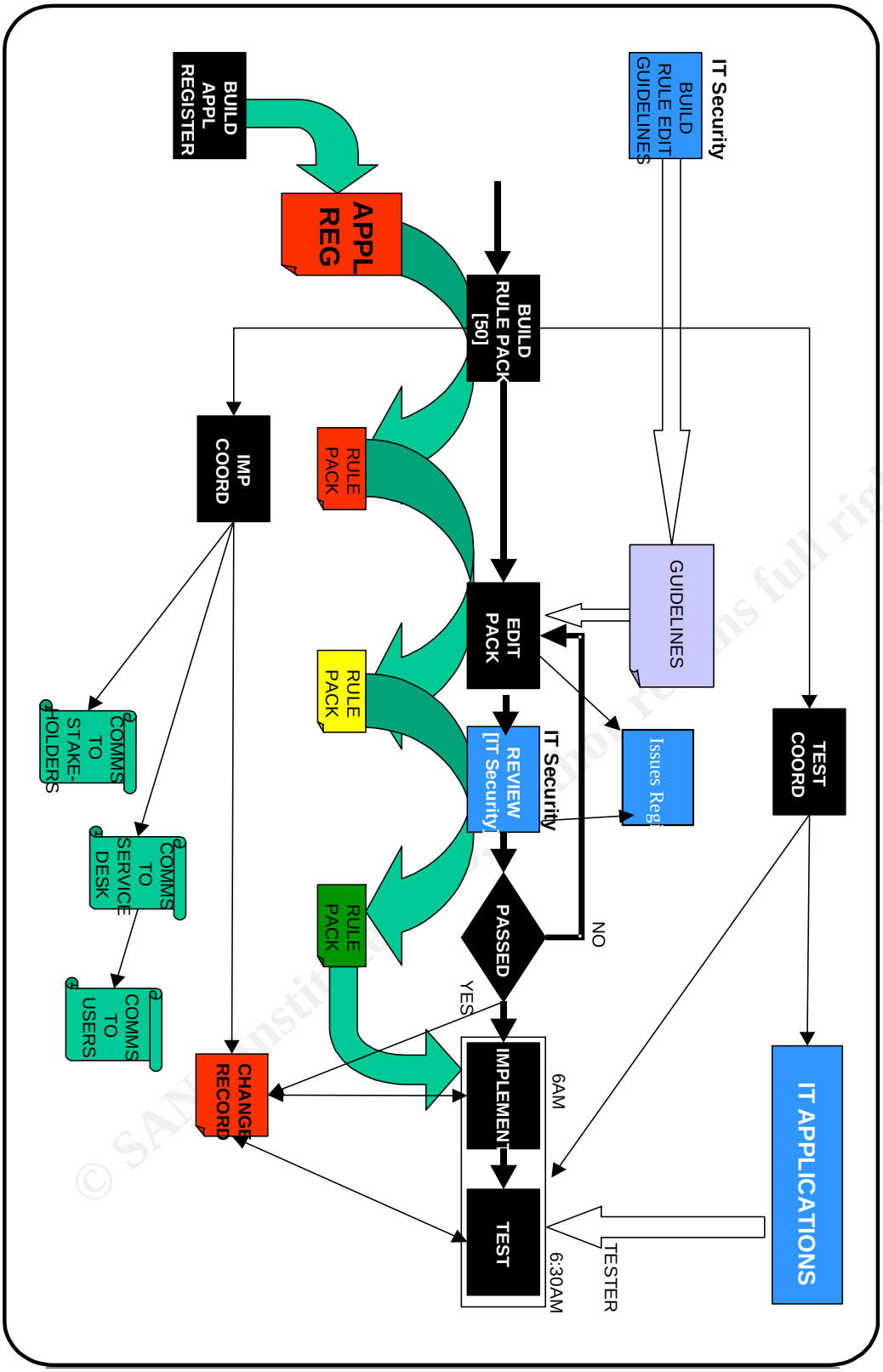
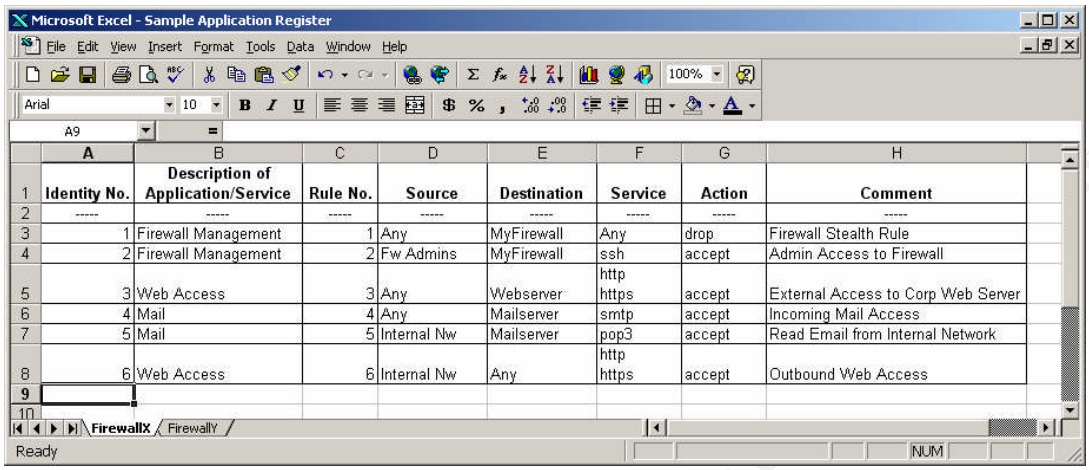


Figure 2 Rulebase Cleanup Methodology

© SANS Institute 2005, Author retains full rights.

Develop an Application Register

An Application Register was created using an Excel Workbook utilising the script available from WYAE[6]. This script "reads the configuration files of Check Point Firewall-1 and produces a well readable, cross-referenced HTML summary of the firewall configuration". The template below is an example populated with data that can be found in the Check Point FW-1 NG Training Guide. Each firewall would have its own worksheet based on this template.



Identity No.	Description of Application/Service	Rule No.	Source	Destination	Service	Action	Comment
---	---	---	---	---	---	---	---
1	Firewall Management	1	Any	MyFirewall	Any	drop	Firewall Stealth Rule
2	Firewall Management	2	Fw Admins	MyFirewall	ssh	accept	Admin Access to Firewall
3	Web Access	3	Any	Webserver	http https	accept	External Access to Corp Web Server
4	Mail	4	Any	Mailserver	smtp	accept	Incoming Mail Access
5	Mail	5	Internal Nw	Mailserver	pop3	accept	Read Email from Internal Network
6	Web Access	6	Internal Nw	Any	http https	accept	Outbound Web Access

Figure 3 Sample Application Register

The worksheets would be identified by each firewall's name and populated by its rules. As can be seen from the example, additional columns were added to include Identity Number and a Description field. These fields are explained as follows:

- *Identity No*. – This is a unique number given to a rule so that in the likely event the rule contents change or the rule's position in the rulebase changes, it can be easily located.
- *Description of Application/Service* – This column is to assist in identifying rules that belong to a particular application or service.

For the initial worksheet population and first pass through the Application Register I was not required to determine whether the rule was adequate or indeed used, but only to identify a category.

If the use were obvious, it would be noted in the Application Description column and these rules would be grouped separately. This would allow us later on to make rule changes in batches according to these groupings.

If the application or group using the rule were not obvious I would list the rule under something generic such as "browsing" or "file transfer". These groupings would later be implemented into the NG firewall rulebase under "Headings". The example below shows the use of Headings for External

© SANS Institute 2005, Author retains full rights.

Access and Mail. Again the demonstration software supplied by Check Point has been used.

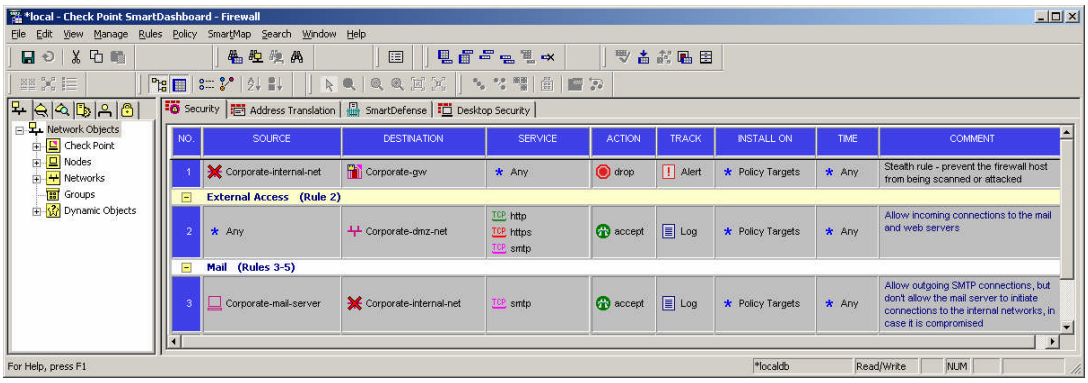


Figure 4 Sample Rulebase demonstrating Headings

Sort Application Register into Release Packs

After completion of the first pass through the rulebase, the rules were ready to be sorted under common headings. To do this involved a sort on the Description of Application/Service field. A review of the sorted register enabled me to create a pack of rules for release at approximately every 50th line in the register.

Analysis of Rules in a pack

The next task was to take a pack of rules and analyse each rule individually. I did this to ascertain the exact requirements of the rules, in terms of Source, Destination and Service. Resources available to assist were Check Point Firewall-1 NG Log Viewer, network diagrams, network tools, SANS GIAC Cookbook Tools, in particular NMAP and Ethereal. As recommended as part of the SANS training, permission from the business owner was received before using any of the Cookbook Tools.

Create New Rulebase

After determining whether each rule was required and if so, what it was used for, I was able to create a new rulebase. This new rulebase would contain both the disabled existing rule and the newly modified or created rule placed underneath. Both new and existing rules contained in the comment field Release Change number, Application Register number and business purpose. Disabling the existing rule rather than removing it, allowed for quick reference were it necessary to resurrect previous Source/Destination/Service information.

To enable quick restoration in the case of problems, the new rulebase was split into sections, the top section contained rules to be retained and their Headings and at the bottom, a heading titled Rules to be removed from

© SANS Institute 2005, Author retains full rights.

Release # contained those rules to be deleted at a later stage. These rules were not modified for use in the new rulebase, but were determined to be unnecessary, no longer used and disabled.

Quality and Peer Review new Rulebase

The complete new rulebase was to be available to IT Security to review. Their comments were to be placed into the Issues Register and a meeting held between the representatives of IT Security and myself to discuss and agree to the contents of each rule.

Create an Issues Register

Undertaking analysis of firewall rules is a subjective task based on the skills and experiences of the analyst. Judgements would be made by both myself conducting the review and also by members of IT Security who would review my findings implemented in the newly created rulebases.

The Issues Register was created to record tasks or follow up items which would need to be addressed either before the Implementation Release or before the end of the project depending on the priority assigned by IT Security.

The priorities were defined as follows:

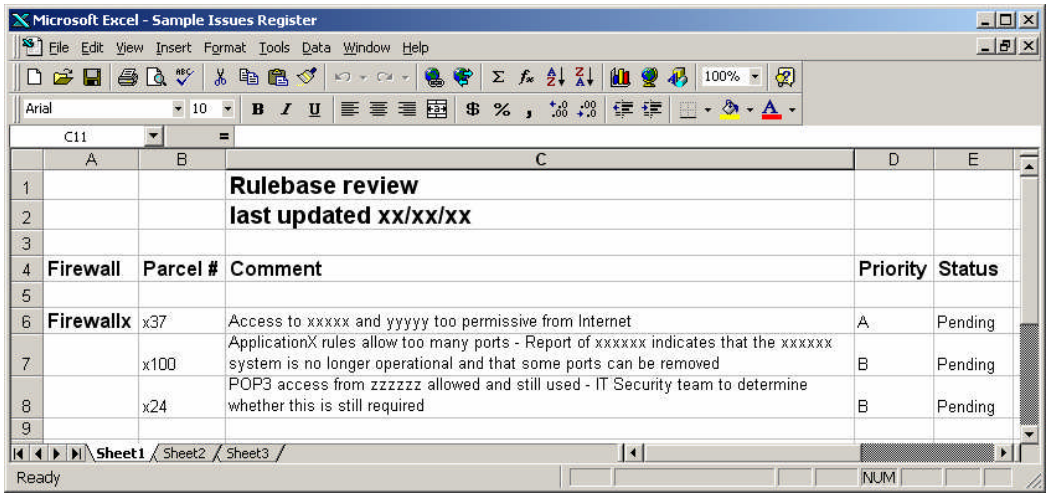
Priority	Action
A	Rules must be rectified ASAP. Releases containing priority A issues will not be approved by IT Security.
B	Must be done within current project schedule.
C	Longer term and may require further investigation or delegation. Must be addressed by mm / dd / yyyy
D	Out of project scope and may require further discussion or delegation. Should be done by mm / dd / yyyy

It was agreed that Priority A and B must be resolved before the Implementation Release, however Priority C and D could be held over for further review at a later date.

Unlike the Application Register that was broken up into worksheets based on each firewall, the Issues Register was one spreadsheet formed to cater for each Release.

The firewall was identified in the Firewall column and the Pack # column was used to link the Identity Number from the Applications Register to the Release ID. A sample Issues Register follows.

© SANS Institute 2005, Author retains full rights.



	A	B	C	D	E
1			**Rulebase review**		
2			**last updated xx/xx/xx**		
3					
4	**Firewall**	**Parcel #**	**Comment**	**Priority**	**Status**
5					
6	**Firewallx**	x37	Access to xxxxx and yyyyy too permissive from Internet	A	Pending
7		x100	ApplicationX rules allow too many ports - Report of xxxxxx indicates that the xxxxxx system is no longer operational and that some ports can be removed	B	Pending
8		x24	POP3 access from zzzzzz allowed and still used - IT Security team to determine whether this is still required	B	Pending
9					

Figure 5 Sample Issues Register

Signoff and Change Control

Once agreement was been reached, IT Security was to sign off the Release's Change Request. Changes would then occur approximately three times a week. This decision was made balancing the risk of changing too many rules at once, and prolonging the duration of the project. The changes were to be made out of hours and at times acceptable to the business and testers and in a time least likely to impact production batch processing.

Test Strategy

After each change had been applied, testing would be carried out to ensure application integrity had been maintained. The level of application testing performed had to be proportional to the level of change being made. If as a result of a change, there was a significant impact on the business, the change was to be backed out immediately. If however, the change caused an impact to a very limited numbers of users, a correction would be put in place. The process outlined above mitigates this risk to a large extent, as old rules would not be immediately removed, could be uncommented and the rulebase reinstalled.

As part of the analysis of the rules, I had to identify what access or application was represented and to assign it an area of the business as "owner". This owner was then responsible for nominating a resource who would carry out the post implementation verification and testing. The development of appropriate testing to ensure the accessibility of applications post implementation rested with each application team.

On completion of each rule pack a notice similar to the example below was sent to each business unit listed. The notice included dates, times and the requirement to notify the success of testing or otherwise to the firewall administrator performing the change. This post notification was important to ensure the change was completed in the nominated change window.

© SANS Institute 2005, Author retains full rights.

Test Contact Info for Firewall Rulebase Cleanup – Release X1-X5 (Change No: xxxxx)

The Firewall Risk Mitigation Project is being undertaken to address important upgrade and maintenance tasks on the firewall infrastructure. As a part of this project the Firewall Rule Base will be reviewed and revised to comply with X security standards and improve manageability.

Time schedule for this release:

Release Date	Implement Time	Operability Test Starts	Operability Test Finished
xx/xx/xxxx	06:00 am	06:10 am	06:30 am

Critical applications involved in this release are identified as follows. Application specialists have identified areas within their applications that may be affected by the change. Application areas have been requested to confirm that pre implementation checks have been performed prior to the above date. On completion of the application areas test cases they are required to email the Firewall team advising the outcome of the test.

Xl No.	Application to be tested	Application Specialist
1.	Network Time Protocol	Person A
2.	Internet Browsing	Person B
3.	Backups	Person C
4.	DNS	Person A
5.	Datastream	Person D

Figure 6 Sample Testing Requirement Communication

Meet to discuss each Release

On completion of each release the Project Team would meet to discuss any issues or problems. It was also an opportunity to ensure the project remained on track and met its objectives.

Notification Process

The notification process was to inform the stakeholders and the business of the impending changes. While every effort was made to ensure there were no unplanned outages, it was important to notify the relevant support people who

© SANS Institute 2005, Author retains full rights.

may be called in the event of an application failure or problem. The timeframe for sending the notices related to each Release were as follows:

Upgrades	Notification
Notify stakeholders	14 days prior
Remind stakeholders	7 days prior
Notify service desk (they will propagate the notice)	3 days prior
Remind service desk	1 day prior
Rulebase changes	Notification
Notify stakeholders	7 days prior
Notify service desk (they will propagate the notice)	3 days prior
Remind service desk	1 day prior

After Snapshot

On completion of the project the firewalls were at supported revision levels and were consistent in both Operating System and version of Check Point Firewall-1. Documentation was completed that would allow us to rebuild the firewall in case of an outage or request for a new firewall. I have since used the procedures[7] to build a new firewall and have updated the documentation.

The new firewall rulebases were well commented and easy to understand and the firewall administrators have a much better understanding of the applications and services that are passing through the network.

At the end of the project we had reduced the number of rules as follows:

rules reviewed	2231
rules remaining	1023

While the resultant rulebases were deemed to be at a higher level of the security, the project highlighted areas for future security evaluation and risk reduction. These areas were documented into the Issues Register and were to be raised as future projects in order of priority. The analysis also highlighted different methods of accessing data or applications and these methods were also recorded so that a consistent and secure approach can be implemented in future.

Overall the project was a success. Not only did we enhance the security of our existing rulebases; we were able to learn a lot about our new business and its IT environment.

Maintaining currency

One of the questions asked a lot during the project was “how are we going to maintain the heightened state of security?” It is difficult in a large organisation

© SANS Institute 2005, Author retains full rights.

to know, for example, when an application or server is decommissioned, a person changes desks or a network is moved etc and so we needed to develop standards that would not require us to rely on others to tell us what has changed in the business.

To compliment existing defence in depth strategies the following guidelines were developed to help maintain currency of the firewall rules.

- When a firewall rule is modified, the service request number in the comment field of the rule is to be replaced, but within the service request itself, a comment that links back to the original service request is to be added. By following this process, all changes to the firewall, will be auditable back to their origin.

- Object names will become more descriptive and will follow the naming convention listed in the Firewall Policy[8].

- After a period of time using the new rulebases and analysing log data the firewall rules can be modified to further enhance performance and security. A paper from CERT titled "Configure Firewall Logging and Alert Mechanisms[9]" states that "You want your firewall systems to log activities pertinent to firewall operation and the rules the firewall will enforce. For significant firewall events, you want your firewall system to alert you in real time that these events have occurred." The paper outlines the steps to follow and I am using these as guidelines to further enhance the security of our firewalls.

- The use of reporting products such as fwlogsum[10] allows me to run reports to show what is active on the firewalls. The reports can, according to its developers, "summarise FW1 logs making it easier to see what services are being blocked or allowed through your firewall". I am also using utilities such as "urules" that produces a report to "summarise rule usage and unused rules." The unused rules can then analysed and possibly removed.

- Regular audits will be carried out to determine the currency of the rules.

- A project has been initiated to implement Check Point SmartView Reporter that will replace some of the tools mentioned above.

Conclusion

On completion of the project the perceived risk of harm to our network was greatly reduced. Whilst the project was deemed significant in its achievements it is important to remember that security is a constantly changing discipline and it is vital that we remain current. It will be a continuing challenge for both the administrator and management to budget the time, money and resources needed to maintain this newly heightened state of security.

© SANS Institute 2005, Author retains full rights.

References

[1] URL: http://www.checkpoint.com.au (home page) July 26, 2004.

[2] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0 October 8, 2003.
URL: http://www.sans.org/top20/#ports

[3] Cole, Eric. SANS Security Essentials with CISSP 10 Domains Cookbook. Version 2.2. SANS Institiue. USA. 2004.

[4] "Appendix A Common Vulnerable Ports." The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0 October 8, 2003.
URL: http://www.sans.org/top20/#ports

[5] Paige, Randall. "Re: How to merge multiple firewall rules in to one ?" Online posting. March 01, 2002. July 19 2004 <news: cp.products.firewall-1>
URL:
http://groups.google.com.au/groups?q=merging+firewall+policy&hl=en&lr=&ie=UTF-8&selm=%230GRYyRwBHA.405%40dogwood.us.checkpoint.com&rnum=2

[6] "WYAE – FW1Rules – Firewall Documentation".
URL: http://wyae.de/software/fw1rules/ (July 28, 2004).

[7] Firewall Installation Checklist. Australia. Giac Enterprises. 2003.

[8] Firewall Communications and Management Standard. Australia: Giac Enterprises. 2003.

[9] "Configure firewall logging and alert mechanisms". May 1, 2001.
URL: http://www.cert.org/security-improvement/practices/p059.html

[10] Humphries, Cameron. "Firewall Log Summariser". Fwlogsum. Version 5.0.2. April 30, 2004.
URL: http://www.ginini.com/software/fwlogsum/

Check Point NG with Application Intelligence Management I. Texas: Check Point Press. 2003.

Firewall Risk Mitigation Implementation. Australia: Giac Enterprises. 2003.

© SANS Institute 2005, Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced