



# **FIREWALL ECONOMICS**

**A Spire Research Report**

## Executive Summary

There are three main processes that drive the firewall administrator's responsibilities - the periodic changes made when adding, modifying, or removing rules from the rulebase, the ruleset audits and reviews in concert with security and compliance efforts, and log monitoring and review associated with forensics work.

Each of these processes has pitfalls that contribute to complex rules that weaken the perimeter defenses. In particular, administrators fall victim to temporary rules remaining permanent, changes to the network, unused rules, and opportunity costs.

These problems revolve around the manual nature of firewall administration. Firewall economics provides for opportunities in efficiency and effectiveness of these administrative activities. Efficiency involves reduced costs for administration and effectiveness corresponds with reduced risk.

The best way to become more efficient and effective in firewall management is to incorporate automated techniques to assist in performing the three main processes of the administrator.

### About Spire Security

Spire Security, LLC conducts market research and analysis of information security issues. Spire provides clarity and practical security advice based on its "Four Disciplines of Security Management," a security reference model that incorporates and relates the functions of identity management, trust management, threat management, and vulnerability management. Spire's objective is to help refine enterprise security strategies by determining the best way to deploy policies, people, process, and platforms in support of an enterprise security management solution.

This white paper was commissioned by Secure Passage, LLC. All content and assertions are the independent work and opinions of Spire Security, reflecting its history of research in security audit, design, and consulting activities.

# FIREWALL ECONOMICS

## Table of Contents

<b>INTRODUCTION</b>	<b>I</b>
<b>THE ROUTINES OF THE FIREWALL ADMIN</b>	<b>I</b>
Ad hoc Requests	I
Rule base Audit and Review	2
Log Review and Monitoring	3
Obstacles in Firewall Administration	3
<b>FIREWALL ECONOMICS</b>	<b>4</b>
Firewall Management – ROI from Reduced Costs	5
Effectiveness -- Risk and the Firewall	8
<b>BEST PRACTICES IN FIREWALL MANAGEMENT</b>	<b>9</b>
Remove unused rules	9
Look for ways to automate the work	9
Build rulebase review into change control	9
Aggregate and evaluate logs	10
Tie log information to ruleset evaluation	10
<b>SPIRE VIEWPOINT</b>	<b>10</b>

## Introduction

Every firewall administrator can empathize with comedian Steven Wright who said, “You know that feeling you get when you are leaning back in the chair, and you almost fall, but catch yourself? I feel like that all the time.” Firewall administrators are constantly receiving change requests without knowing which one will cause an error. And errors on the perimeter can be disastrous whether they result in an initial penetration inbound to the network or the final leak of information on the outbound side.

It doesn't seem like firewall administration could be so unsettling, but this is the reality – there is still significant reliance on firewalls for primary access control at the perimeter. Any security professional with a few years' experience in the enterprise has stories about ports left open or firewalls misconfigured. Add to this the added oversight of compliance needs and the decreasing budgets, and the unease can be palpable.

These challenges don't always get noticed by those who simply want their application or system to work. Firewall rules management is a lot more tenuous than is commonly perceived.

This white paper highlights the challenges of firewall administration and discusses the economic consequences to efficiency and effectiveness associated with porous firewalls, complex rulesets, and an increased time to perform operations.

## The Routines of the Firewall Admin

The firewall administrator's life is consumed by a handful of different processes. First and foremost, they must address the ad hoc requests for opening ports in the firewall. This seems counterintuitive given that most security professionals are interested in reducing the number of holes in the firewall, but it is common nonetheless. Second, the firewall administrator must conduct audits of the rulebase, often in conjunction with new requests but also as part of broader audits and compliance reviews performed by external groups. Finally, the firewall administrator reviews logs. Sometimes, this review is in support of forensic activities after things go wrong, and other times it augments the audits that occur as administrators struggle to evaluate the activity that is occurring at an access control point.

### Ad hoc Requests

Change requests for the firewall almost always constitute opening up more ports to allow connections through it. Firewall administrators only begrudgingly accept this responsibility as it is contrary to their nature to want to increase risk in the enterprise. The administrator must satisfy the request while providing the proper balance between the increase in accepted risk from the change itself and the potential for errors which can also increase risk inadvertently.



The decision-making process is fairly straightforward:

- ▶ Identify the location of the existing point at which a connection request gets denied. This is necessary to ensure that the order of the rules is correct so the new connection request will be allowed.
- ▶ Review existing rules to see if a change can be made to an existing rule that would also satisfy the request. For example, increasing the range of ports or IP addresses in an existing rule may be more effective than creating a new rule that is more specific.
- ▶ Determine whether a new rule should be specific or more general. While a smaller attack surface (and correspondingly a more specific rule) results in lower risk, there is a tradeoff between writing specific individual rules for security and the corresponding management and performance issues that may arise from the increased complexity.
- ▶ Make any necessary adjustments.

These steps form the actionable part of the request process. Usually, the requests will be part of a broader change management process that involves provisioning the request, collecting appropriate approvals, notifying the requestor of completion, and finalizing the action.

## Rule base Audit and Review

As changes add up, the firewall rule base gets more complex. Periodically, a full-fledged review of the ruleset is required simply because there are too many rules to manage and errors are becoming more frequent. In addition, compliance requirements often involve reviews by auditors that can catch an administrator by surprise and significantly interrupt operational activities.

The high level objective of the auditor is to understand how traffic flows through a firewall – which connections are allowed and which ones are denied. The basic approach is to start with a checklist of the small number of ports that are allowed and ports that are denied and then assess all of the one-offs in various other ways, using auditor experience to determine what configuration aspects constitute a problem.

This approach would be fine if there were only a few dozen rules to deal with, but often there are hundreds or even thousands of rules that must be assessed. Even more importantly, multiplying the number of likely source IPs, destination IPs, and ports shows that there are tens- or hundreds-of-thousands of connection possibilities to evaluate.

As regulations and laws tighten up firewall configurations, more attention to detail is required to protect against non-compliance. Manual audits are expensive and can often be incomplete, resulting in a higher likelihood of leaks and inappropriate connections.

## Log Review and Monitoring

During the final part of the firewall administrator's 30-hour day, log monitoring becomes important. It is the least predictable aspect of the job and yet becomes top priority when it is needed. Log review comes into play when troubleshooting a connection problem – e.g., a help desk call came in asking, “Why isn't my application working?” – or even more importantly when there is some hint of a security breach. Sometimes, these breaches are inbound as when a server is attacked after making NetBIOS available to external traffic. Other times, the breach is outbound like when a post shows up on Yahoo! Finance that appears to provide confidential information about an enterprise (we use the notion of “breach” here at its broadest level of applicability).

Reviewing logs provides the firewall administrator the clearest view into what is happening day-in and day-out with firewall activity. This assumes that logging is turned on and ALL connection attempts (allowed and denied) are logged. The challenge to the administrator is aggregating hundreds of millions of log entries across multiple firewalls and making sense of it all.

All of these processes contribute to an unstable rulebase that is highly complex, full of errors, and almost contradictory in its nature – contributing weaknesses as often as it provides security. The next section discusses the nature of these security weaknesses in detail.

## Obstacles in Firewall Administration

It is clear that there are a number of obstacles that can trip up a firewall administrator in day-to-day activities. The notion of complexity is a simple one to understand as many administrators already lament the number of rules in their rulebases. Every security professional begins training with a “deny all” mentality that drives the need to minimize attack surface. Practically speaking, this can be a challenge in many enterprises that see the firewall as another obstacle to bypass.

An assessment of these failures and identification of causes leads to questions of temporary fixes becoming persistent, increased complexity of the network, and opportunity costs with scarce resources.

### Administrator interference

The first obstacle is a simple one – any time there are multiple people involved in administration, there are bound to be points of confusion, overlap, or downright malice. Whether the administrator is within the firewall group or operating in support of a related group, differences in process and the complexity associated with multiple parties operating independently can easily contribute to errors in the rulebase.

### Persistent “temporary” changes

The administrator must deal with situations where “temporary” solutions to a problem – making firewall changes in support of a new extranet application or service, for example – become permanent. In the frenzy of a high-pressure

development effort, sometimes the change control process is bypassed (perhaps for good reason). But afterwards, the rule that was applied is never removed. Because these rules are intended as quick fixes, they are often not evaluated appropriately within the context of the full ruleset and thus have an increased likelihood of leading to problems.

### **Dealing with corporate network changes**

The firewall administrator is usually the last to know. The network is reconfigured such that groups and resources get reorganized within the network and the firewall operations group is not notified. This is a crucial problem that must be resolved immediately, because connections could be made to inappropriate systems through the firewall.

Not only does the firewall administrator need to examine rulesets, but s/he needs to pay attention to changes going on across the network that may affect security.

### **Remnant rules of yore**

If a business unit leader contacted the firewall administrator and said, "I don't need that rule any more, you can remove it," any firewall administrator would immediately start looking for hidden cameras. It rarely happens. Yet as networks and business requirements change, these unused rules crop up. Sometimes, new changes reactivate the rules in unanticipated ways.

### **The simple problem of complexity**

As firewall rules get added to the rulebase and the rulebase gets more complex, at some point mistakes will be made. The paper "Taxonomy of Conflicts in Network Security Policies" by Hamed and Al-Shaer classifies the common types of firewall rule errors – shadowing, correlation, redundancy, and exceptions.

## **Firewall Economics**

With firewall activities and obstacles defined, the implications on efficiency and effectiveness are profound. The concept of firewall economics captures these needs for efficiency and effectiveness of administration, management, and operation of the firewall resources. An enterprise must ensure that its processes and its use of assets are efficient – that is, the benefits (outputs) are maximized within the scope of the allocated costs (inputs).

From a firewall management perspective, efficiency comes from minimizing costs for the available tasks and operations. In financial terms, enterprises seek the lowest total cost of ownership (TCO), highest return on investment (ROI), or other net financial benefits.

In addition, solutions need to be effective – where actual outcomes are measured in relation to expected outcomes. Firewall effectiveness is really a function of ensuring that the connections meet the requirements of the organization. It is an attempt to minimize the error rate and thus maintain the strongest security posture possible.

With firewalls and other security solutions, effectiveness is a function of optimizing risk – that is, minimizing risk with respect to a specific set of allocated resources.

## Firewall Management – ROI from Reduced Costs

Return on Investment is often considered the “Holy Grail” for information security solutions. And the Holy Grail hunt turns into a holy war as security professionals debate the definition of ROI and whether the benefit is possible in scenarios involving cost centers. Can you get a return on investment in security? That’s simply a semantic argument that masks the facts. Regardless of what the financial benefit may be called, the goal is to generate savings by spending less than the amount currently being spent on some business function.

With business cost centers like security, there is no direct revenue opportunity to help generate a return; there are only costs that can be reduced. In accounting, these costs are grouped into capital expenses (CapEx) and operational expenses (OpEx).

Capital expenses are incurred and therefore accounted for throughout the lifetime of an asset that is expected to last multiple years. Capital expenses in IT consist of hardware and software. The obvious (and only) capital expense with firewalls is the firewall itself. Sometimes, it is a combined cost for appliances, or the capital investment is split between hardware and software. These are real costs governed by accounting principles of amortization and depreciation to allocate these costs over multiple years.

Operating expenses are those expenses that are incurred and realized immediately. Operating expenses include personnel expenses, services, and maintenance fees. While straightforward to account for, the burdensome part about OpEx is determining the time spent by participants for any business function.

### Calculating ROI for firewall management

The basic approach to calculating ROI is to collect the operating and capital expenses for labor, software, hardware, and maintenance and compare them to the projected costs associated with an alternative scenario. If the costs in the alternative scenario are lower than the current situation, then the scenario is worth considering.

### Opportunity Cost

Amidst all of this activity, firewall administrators must juggle many responsibilities. Often, there isn’t enough time to perform the necessary tasks. The direct impact of these challenges is understood, but there is an indirect problem as well – opportunity cost. In economics, opportunity cost points to the loss of ability to perform one activity in lieu of needing to perform another. In firewall administration, this might mean that there is direct cost of an administrator making a change and an indirect opportunity cost because that administrator might not be able to review firewall logs. There are many proactive things firewall admins could do; however, there is not enough time to do everything manually. Automation will free up time to be more proactive.

The significant manual overhead described in this paper hints that an opportunity exists to get ROI in firewall management. As with any tedious task, automation can provide significant productivity gains to free up personnel either to perform their tasks more frequently or to perform other tasks, thereby increasing security for the organization.

This example, then, will calculate the potential ROI when moving from a mostly manual approach to firewall management to one employing a firewall policy analyzer solution to automate routine tasks. Ultimately, every enterprise puts its own unique spin on firewall management and will have its own unique numbers. However, the estimates used in these scenarios were based on observations and experience with firewall management activities.

For calculating OpEx, three different categories of work were identified earlier in the paper - firewall changes, rulebase audits, and log management. These major categories can be assessed and a dollar amount associated with productivity can be calculated.

The first step to calculate labor costs is to estimate an hourly rate for the firewall administrator. The firewall administrator in the example makes \$65,000 over 2,080 hours (52 weeks), for an hourly rate of \$31.25.

ASSUMPTIONS	
Annual Salary	\$65,000
Annual Hours	2,080
Hourly Rate (salary / hours)	\$31.25

Table 1. Firewall administration assumptions.

Next, we estimate the total number of hours per year for each of our three major functional activities. This calculation involves identifying the time to complete a single event and multiplying it by the total number of events in a year. For the current situation, this information should come from timesheets or well-informed estimates based on existing activities. As indicated previously, these numbers may vary significantly for enterprises and should be used as a representative model only.

CURRENT SCENARIO: MANUAL COSTS			
Activity	Frequency	Duration	Total Hrs
Firewall Changes	104 (2 per wk)	4 hrs	416 hrs
Rulebase Audits	4	16 hrs	64 hrs
Log Management	26	4 hrs	104 hrs
<b>TOTAL HOURS</b>			<b>584 hrs</b>
<b>LABOR COST</b>	<b>584 x \$31.25</b>		<b>\$18,250.00</b>

Table 2. Total labor costs per firewall - current scenario.

In this example, the current scenario shows 584 hours worth of firewall administration in a year. Multiplying this times the \$31.25 results in administrative

costs of about \$18,000 for each firewall instance. So a company with 10 firewalls is going to have annual costs of \$180,000. With many of the largest companies having over 500 firewalls (\$9 million), it is easy to see how these manual costs add up.

A firewall policy analyzer provides key capabilities to automate firewall management, including:

- ▶ Determining what rules are impacted by a change and identifying the appropriate placement/ordering of rules.
- ▶ Identifying duplicate, overlapping, or overbroad rules in the rulebase.
- ▶ Tracking changes and associating them with change control tickets.
- ▶ Automating full security assessments of firewall policies.

Automating this manual process can result in significant time savings. Table 3 shows the corresponding numbers for a scenario that leverages a firewall policy analyzer to reduce the amount of time it takes to conduct these activities.

<b>AUTOMATED SCENARIO</b>			
<u>Activity</u>	<u>Frequency</u>	<u>Duration</u>	<u>Total Hrs</u>
Firewall Changes	104 (2 per wk)	.5 hrs	52 hrs
Rulebase Audits	4	2 hrs	8 hrs
Log Management	26	1 hr	26 hrs
<b>TOTAL HOURS</b>			<b>86 hrs</b>
<b>LABOR COST</b>	<b>86 x \$31.25</b>		<b>\$2,687.50</b>

Table 3. Total labor costs per firewall – automated scenario.

When tables 2 and 3 are matched up head-to-head, the savings become clear.

<b>COMPARISON</b>			
<u>Activity</u>	<u>Current Hrs</u>	<u>Auto Hrs</u>	<u>Savings</u>
Firewall Changes	416 hrs	52 hrs	364 hrs
Rulebase Audits	64 hrs	8 hrs	56 hrs
Log Management	104 hrs	26 hrs	78 hrs
<b>TOTAL HOURS</b>	<b>584 hrs</b>	<b>86 hrs</b>	<b>498 hrs</b>
<b>LABOR COST</b>	<b>\$18,250</b>	<b>\$2,688</b>	<b>\$15,562</b>
<b>10 Firewalls</b>	<b>\$182,500</b>	<b>\$26,875</b>	<b>\$155,625</b>
<b>500 Firewalls</b>	<b>\$9,125,000</b>	<b>\$1,343,750</b>	<b>\$7,781,250</b>

Table 4. Comparison of total labor costs per firewall (annual).

To calculate ROI, the last piece of information required is the cost of the automated solution – in this case, the firewall policy analyzer. The example shows that any solution with costs that are less than approximately \$150,000 creates a positive return within the first year (note: it is common to evaluate a solution over a longer period – often 3-5 years).

A firewall policy analyzer like FireMon® from Secure Passage will generally cost about \$15,000 for 10 firewalls and \$500,000 for 500 firewalls. So, at the lower level, a simplified ROI scenario shows a net benefit of approximately \$140,000 (\$155,000 - \$15,000 costs) for that \$15,000 investment, for a return nearing 1,000 percent in the first year alone. Similarly, the 500 firewall scenario shows a benefit of almost \$7.8 million compared to its \$500 thousand cost, for a 1500+ percent return.

Numbers this good beg skepticism, and so it is useful for any enterprise to perform its own analysis to ensure that appropriate benefits are properly identified.

## Effectiveness - Risk Reduction and the Firewall

ROI is an efficiency metric – with cost centers it arises anytime you can reduce your existing costs by investing in a directly-related solution. But what about effectiveness? We also want to measure whether an investment can effectively reduce risk. Enter Return on Security Investment (ROSI) the oft-misunderstood cousin of ROI.

While ROI is a function of reduced costs, ROSI is a function of reduced risk. It is an economic measure of value that compares the cost of some new control to the change in annual loss expectancy (or some equivalent measure). Before addressing ROSI, it is useful to understand risk more clearly.

### Thinking about Firewall Risk

With respect to firewalls, it is useful to think about risk as the likelihood that a network connection is malicious within the context of total potential network connections. A unique network connection can be identified by the source IP address, destination IP address, and destination port number.

Using total possible unique connections as the population set, one can assess the effectiveness of a firewall by determining how many connections are allowed and how many are denied. Any change in effectiveness can then be measured by the relative impact on connections – closing down ports will reduce risk and opening ports will increase risk.

### Getting to Return on Security Investment

Return on Security Investment (ROSI) involves comparing the amount of money spent on a control to the amount of risk that is reduced. If the control spending is less than the risk reduction value, then the control is getting a positive ROSI. If the control spending is greater than the reduction amount, then there is a negative ROSI and the control should be re-evaluated.

Contrary to ROI and TCO calculations, ROSI is an economic estimate. It doesn't affect financial statements or accounting practices at all. That said, it is real nonetheless. In fact, even when the aspects of risk are not quantified, the decision making process employs them inherently. This is worth repeating – any security professional who asks the question “is it worth it?” when deciding on control measures, is performing an implicit ROSI calculation.

## Firewall ROSI

To apply ROSI to firewalls, the security professional must have an understanding of the value of the assets being protected. As an example, let's use \$100 million. Further, assume that there is a 1% chance that an attack will occur sometime in the next year. Therefore, the annual loss expectancy is \$1 million.

A firewall policy analyzer is being considered to reduce the number of rules and total potential connections. In general, the firewall administrator believes he can reduce his connections by 25%. This would lower the risk from 1% down to .75%, with a corresponding reduction in annual loss expectancy to \$750 thousand, resulting in \$250 thousand in reduced risk.

If a firewall policy analyzer can be purchased for \$50 thousand, then the corresponding ROSI is 400%  $((\$250k - \$50k) / \$50k)$ .

Obviously, this is a rudimentary calculation. It seems clear that not every connection bears the same amount of risk that an attack will occur. A more complex calculation would involve "natural frequencies" of connections using real log information.

## Best Practices in Firewall Management

Managing a firewall can be challenging work, but there is ample information available to identify those practices which optimize the process and operations within its scope.

### Remove unused rules

Removing unused rules in firewalls is like changing the oil in a car - it may seem routine and non-essential until it is ignored and serious malfunctions occur. Removing these rules eliminates complexity from the rulebase and prevents mistakes that could arise as other rules are manipulated. And since every rule carries with it a processing penalty, reducing the number of rules will increase performance.

### Look for ways to automate the work

Automation gives firewall administrators the opportunity to focus on analysis and not administrative routines like collecting and sorting rulesets and logs. The extra time gained from automation can be used to analyze rulesets in more in-depth ways and elevate benefits from tactical to strategic.

### Build rulebase review into change control

With automation, the administrator can perform "what-if" scenarios and understand the impact of a change prior to applying it directly to the firewall. Functionally, built-in review is likely to lead to quicker changes with fewer errors.

## Aggregate and evaluate logs

Analyzing logs can be one of the most beneficial aspects of risk management. Unfortunately, they are so verbose that aggregation and evaluation can be logistically challenging. Seek out ways to aggregate, summarize, and report on logs to get a better understanding of the security posture of firewalls.

## Tie log information to ruleset evaluation

As administrators get better at evaluating rulesets and logs, using the information in context can become a strong benefit to the overall program. Understanding the frequency of rule usage along with the contextual impact of reordering can allow for optimal ruleset configuration.

## Identify opportunities for return

ROI and ROSI are both real opportunities with respect to firewall management. We know our rulesets are larger and more complex than they should be. Some combination of both measures would provide the appropriate justification for automating management to reduce costs and risk simultaneously.

## Spire Viewpoint

Firewalls are a fact of life in the security profession. They are the figurehead for perimeter security and provide fundamental Internet protection. They exist at every trust boundary and because they have been around for so long, the rulesets have had many changes associated with them.

Firewall administration can be extremely difficult with the need to track changes, validate rulebases, and facilitate audits for a number of devices. The high level of complexity creates a high potential for errors that lead to security weaknesses.

You don't want to reinvent the wheel for every firewall review and audit. Selecting the right tool for the right purpose is an important consideration for administrators with large, complex firewall deployments.

## About Secure Passage

FireMon from Secure Passage is a firewall management automation tool that was designed by security professionals. It addresses the problems outlined in this paper. The FireMon unused rule reports can help you clean up your policy. Real-time change notifications can be set to automatically inform users of risky changes. FireMon's policy test functionality can be used to make the right rulebase changes. The side-by-side policy comparison view provides the right visibility to help administrators troubleshoot and evaluate their environments. And, the compliance and documentation framework simplifies normal processes to make the IT security team more efficient and proactive.

Enterprises and organizations should implement a firewall management automation tool if they haven't already. FireMon from Secure Passage can help enterprises and organizations achieve a return on this investment in a short timeframe.

### Contact Spire Security

To comment about this white paper or contact Spire Security, LLC about other security topics, please visit our website at [www.spiresecurity.com](http://www.spiresecurity.com).

This white paper was commissioned by Secure Passage, LLC. All content and assertions are the independent work and opinions of Spire Security, reflecting its history of research in security audit, design, and consulting activities.