Firewall Management Essentials

Version 1.4
Released: October 7, 2013

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051
info@securosis.com www.securosis.com

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

Licensed by Firemon

FIREMON
PROACTIVE SECURITY MANAGEMENT

FireMon provides enterprises, government, and service providers with security management software that gives them deeper visibility and tighter control over their network security infrastructure. The FireMon solution set – Security Manager, Policy Planner and Risk Analyzer – enables customers to identify network risk, proactively eliminate those vulnerabilities and strengthen security throughout the organization, and reduce the cost of security operations and compliance. Together, they create a highly-effective and consistent solution for efficiently managing security operations. For more information, visit http://www.firemon.com. Follow us on Facebook, Twitter, or LinkedIn, or on our blog.

Copyright

Firewall Management Essentials
Table of Contents

Introduction

It starts right there in PCI-DSS Requirement 1. *Install and maintain a firewall configuration to protect cardholder data.* It's the first requirement so firewalls must be important, right? Not that PCI is the be-all and end-all of security goodness, but it does represent the low bar of controls you need to have in place to defend against attackers. As the first line of defense on a network, the firewall's job is to enforce a set of access policies that dictate what traffic is allowed to pass. A firewall is basically a traffic cop on your network, as well as a segmentation point between networks.

Like a closet in your house, if you don't spend time sorting through old stuff it can become a disorganized mess, with a bunch of things you haven't used in years and no longer need.

Between compliance mandates and over 20 years of history, firewalls are a mature technology and have been installed at pretty much every company. The device might be called an access router or UTM, but it provides firewall-style access control. Each firewall runs on a set of rules that basically define what ports, protocols, networks, users — and increasingly applications — are allowed to run on your network. And just like a closet in your house, if you don't spend time sorting through old stuff it can become a disorganized mess, with a bunch of things you haven't used in years and no longer need. That metaphor fits your firewall rule base — security administrators frequently admit (often in a whisper) to having thousands of firewall rules, many of which haven't blocked anything in years.

The problem is that, like your closet, your firewall rule base will not organize itself. It just gets worse if you put it off. And it's not like rule bases are static. New requests come in to open this port or allow that group of users to do something new or different, pretty much every day. The situation can spiral out of control quickly, especially as you increase the number of devices in use. That creates significant operational, performance and security problems, including:

1. **Attack surface impact:** When a change request comes in, how many administrators actually do some work to figure out whether the change would create any additional attack surface or contradict existing rules? Probably not enough, so firewall management — first and foremost — must not reduce the protection provided by the firewall.

2. **Performance impact:** Each additional rule may require the firewall to perform another check on every packet that comes through, so adding rules adversely impacts device performance. Rule order also matters — the sooner you can block a packet the less rules you need to process — so rules should be structured to block unauthorized connections as early as possible.

3. **Change verification:** If a change was made, was it made correctly? Even if the change is legitimate and your operational team is good, there will still be human errors. Another problem in firewall management at scale is verifying each change.

4. **Weak workflow and nonexistent authorization:** What happens when you receive a rule change? Do you have a way to ensure each change request is legitimate? Or do you do everything via 10-year old forms, spreadsheets, or email? Do you have an audit trail of who asked for each change and why? Can you generate documentation to show why each change was made? If you can't that will probably be an issue, because your auditor will need substantiation for changes.

5. **Scale:** The complexity of managing any operational device increases exponentially with each additional device you have to manage. Firewalls are no exception. If you have two dozen or more devices, odds are you have an unwieldy situation, with inconsistent rules creating security exposure. If you have hundreds or thousands of firewalls in place, there is no way to manually keep all of the policies in alignment and coordinated to reduce attack surface.

6. **Heterogeneity:** Many enterprises use multiple firewall vendors, which makes it even more difficult to enforce a consistent security posture across a variety of devices.

As with almost everything else in technology, innovation adds a ton of new capabilities while increasing operational challenges. The shiny new object in the network security space is the Next-Generation Firewall (NGFW). NGFWs enable definition and enforcement of policies at the application layer. That finally enables you to build a rule more granular than `ALLOW port 80` — instead specifying individual web-based applications to permit and block. Depending on the application, you may also be able to restrict specific application features or behaviors. For example, you might allow access to Facebook walls but block Facebook chat. You can enforce polices for users and groups, as well as certain content rules (we call this DLP Lite). The NGFW is definitely not your grand-pappy's firewall, and the additional capabilities dramatically complicate firewall policy management.

As with almost everything else in technology, innovation adds a ton of new capabilities while increasing operational challenges.

> Adding more functions to a device inevitably increases policy complexity — making solid operational discipline all the more important.

At the same time network security is undergoing a period of consolidation. Traditionally separate functions such as IPS and web filtering are making their ways onto a consolidated platform we call the Perimeter Security Gateway (PSG). Adding more functions to a device also inevitably increases policy complexity — making solid operational discipline all the more important. In any sizable organization the PSG rule base will be even more difficult or even impossible to manage manually. Automation is critical to improving speed, accuracy, and effectiveness.

This paper returns us to our network security roots providing an opportunity to document our research on the essentials of managing firewalls and potentially leveraging new automation tools to facilitate and improve your management capabilities. This is relevant both to classical firewalls and PSGs — it covers the major aspects of managing your installed base of firewalls, and positions you for operational success as you embrace the additional capabilities of the PSG.

Don't the Firewall Vendors Do This?

We need to address the elephant in the room before we continue. You are probably wondering why firewall vendors don't handle this. That is a good question, which we've pondered for years. There wouldn't be a market for firewall management tools if firewall vendors did their jobs better. But they don't, so a market developed over the past 5 years and that market is accelerating as the operational complexities of network security increase. For some reason firewall vendors don't have good tools to optimize their rule bases. The cynic (who could that be?) would say that's because poorly configured rule bases kill device performance, and might force premature upgrades to bigger devices. Yeah, that's pretty cynical.

> There wouldn't be a market for firewall management tools if firewall vendors did their jobs better. But they don't, so a market developed.

Firewall vendors also don't include very good workflow or compliance reporting in their management capabilities, because they tend to focus on adding features rather than improving the management of features they already have. Finally, there isn't any real incentive for vendors to support heterogeneous firewalls, so if you have multiple vendors installed… you are out of luck. And it does not appear likely that any incumbents are going to get religion to address these issues any time soon, so you need to consider third-party tools to improve management of your firewalls.

Change Management

As we tackle this first aspect of firewall management, let's start by setting up an operational process for success. By building a consistent workflow to manage the change process you can address many of the issues mentioned above, and:

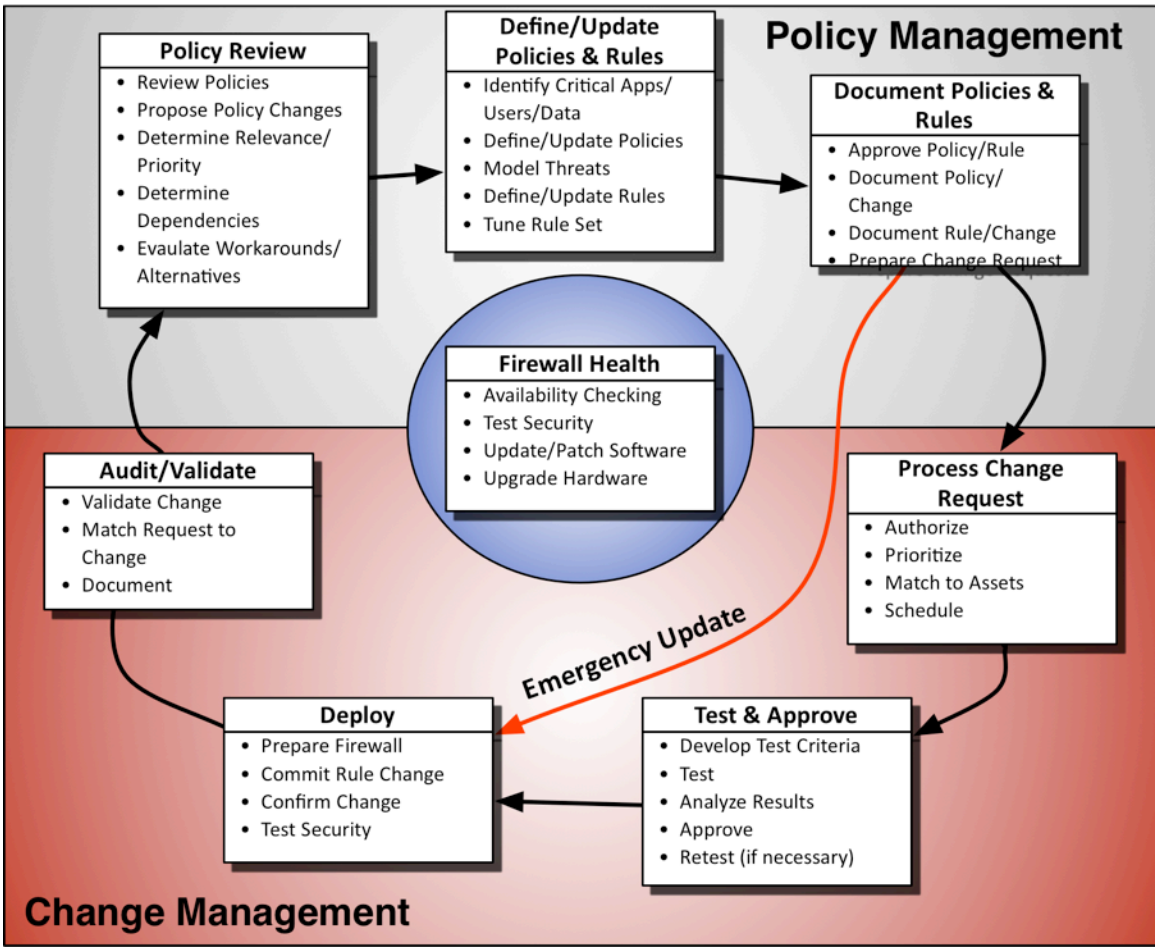
1. **Improve accuracy:** If you make an incorrect change or rules conflict with other rules, you can add significant attack surface to your environment.
2. **Require authorization:** It is difficult for many security admins to say 'no', especially to persuasive business and technology leaders who 'need' their stuff RIGHT NOW. A consistent and fair authorization process reduces or eliminates bullying and other shenanigans folks use to get what they want.
3. **Verify changes:** Was the change made correctly? Are you sure? Verification that each change was correct and successful is important, particularly from an auditing context where you'll have to substantiate the changes that are made.
4. **Maintain an audit trail:** Speaking of auditing, making sure every change is documented, with details on the requestor and approver, is helpful both when preparing for an audit and for ensuring a positive outcome.

Network Security Operations

A few years ago we built a huge and granular process map for network security operations as part of our Network Security Operations Quant research. One of the functions we explicitly described was managing firewalls, mapped out in detail below.

A granular process map can be overwhelming, and isn't normally implemented in its entirety. But it illustrates what is involved in managing these devices. To ensure you understand how we define some of these terms, we include a brief description of each step from that research.

Detailed Firewall Management Process Map



Policy, Rule, and Signature Management

In this phase we manage the content underlying the network security devices. This includes attack signatures as well as the policies and rules that control response.

1. **Policy review:** Given the number of monitoring and blocking policies available on network devices, it is important to keep rules (policies) current. Deploying too many policies imposes a severe performance hit and can waste a great deal of time on false positives. It is a best practice to review network security device policies to prune rules that are obsolete, duplicative, overly open, prone to false positives, or otherwise unneeded. Policy review triggers include signature updates, service requests (new application support, etc.), external advisories (to block a certain attack vector or work around a missing patch, etc.), and policy updates resulting from operational management of the device (per change management process described below).

2. **Define and update policies and rules:** This entails defining the depth and breadth of network security device policies, including the actions (block, alert, log, etc.) taken when an attack is detected — whether via rule violation, signature trigger, or another method. Note that as the capabilities of network security devices continue to expand, a variety of additional detection mechanisms come into play, including increasing visibility into application traffic and identity stores. Logging, alerting, and reporting policies are defined here. It is important to take the hierarchy of policies into account. At the top organizational policies apply to all devices; they may be supplemented or overridden by business unit or geographic policies. Those higher-level policies feed into the policies and/or rules implemented at a location, which then filter down to rules and signatures implemented on a device. The hierarchy of policy inheritance can dramatically increase or decrease the complexity of rules and behaviors. Initial policy deployment should include a Q/A process to ensure no rules impair the ability of critical applications to communicate either internally or externally.

3. **Document policies and rules:** The planning stage is an ongoing process, and documentation is important for operational and compliance reasons. This step lists and details the policies and rules in use on devices according to operational standards, guidelines, and requirements.

Change Management

In this phase rule and signature additions, changes, updates, and deletions are handled.

1. **Process change request and authorize:** Based on either a signature or policy change within the Content Management process, a change to network security device(s) is requested. Authorization requires both ensuring the requestor is allowed to request the change, and determining the change's relative priority, in order to select an appropriate change window. The change's priority is based on the nature of the signature or policy update, as well as the risk of attack. Then build out a deployment schedule based on priority, scheduled maintenance windows, and other factors. This usually involves the participation of multiple stakeholders — ranging from application, network, and system owners, to business unit representatives if downtime or changes to application use models are anticipated.

2. **Test and approve:** This step includes development of test criteria, any required testing, result analysis, and approval of the signature/rule change for release once it satisfies requirements. Testing should cover signature installation, operation, and performance impact. Changes may be implemented in 'log-only' mode to observe their impact before committing to blocking mode in production. With an understanding of the impact of the change(s), the request is either approved or denied. Obviously approvals from a number of stakeholders may be required. The approval workflow must be understood and agreed on in advance to avoid significant operational issues.

3. **Deploy and confirm:** Prepare the target devices for deployment, deliver the change, and return the devices to normal operation. Verify that changes were properly deployed, including successful installation and operation. This might include use of vulnerability assessment tools or application test scripts to ensure there is no disruption of production systems or attack surface added as a result of the change.

4. **Audit/validate:** The full process of making a change encompasses more than merely having the operations team confirm it during the Deploy step — another entity (internal or external, but not part of the ops team) should audit it as well to provide separation of duties. This entails validating the change to ensure policies were properly updated and matching it against a specific request. This closes the loop to make sure there is documentation (and an audit trail) for every change.

Emergency Update

In some cases, including data breach lockdowns and imminent or active zero-day attacks, a change to the network security device's signature/rule set must be made immediately. An 'express' process should be established and documented in advance as an alternative to the normal full change process, ensuring proper authorized approval for emergency changes, as well as a rollback capability in case of unintended consequences.

Key Firewall Management/Change Automation Features

As we get into what capabilities we need a firewall management tool to provide in terms of change management, there are several key features, including:

1. **Configurable workflow:** Some organizations don't have any process at all, so they are happy to have a firewall management tool dictate tasks and approvals. But most already have a well-established process, and it rarely makes sense to blow the entire process up. The FM tool should offer a reasonable out-of-the-box process, and be configurable to support existing processes and integration with existing work/task management systems.

2. **Notification of change request:** Once a change request comes in, the first task is to actually notify someone. Any FM tool should support a variety of notification options, allowing multiple parties to be notified as needed.

3. **Flexible approval/authorization:** Once the request is received the authorization/approval process needs to begin. This includes the aforementioned notification, as well as support for complicated workflows and multi-stage approvals, depending on the nature of the request.

4. **Rule Recommendation:** In large and/or complicated networks, a request to provide access for application X may involve a variety of changes on multiple devices. A key capability of FM solutions is to recommend effective changes that will properly implement the access request without creating unnecessary rules and complexity in firewall policies while greatly reducing the time and effort to accomplish this task.

5. **Security posture assessment and policy checking:** Once the change has been approved, it would be great to understand how it impacts the overall security posture, as well as check to ensure it doesn't violate existing configuration policies. We will discuss optimizing rules later in this paper.

6. **Change tracking and verification:** One of the key values of automating firewall change management is to get a better handle on workload, backlog, and responsiveness. The FM tool should track all change requests with a closed loop, verifying that each change has been made correctly and successfully.

7. **Task management:** Hand in hand with closed-loop tracking of firewall change requests goes the ability for security administrators and operations folks to track work queues. This ensures they are working on the most important changes, and getting them done in a timely fashion.

8. **Integration with help desk systems:** Some operations groups already have well-established task management systems integrated with their help desk systems. Bidirectional integration with these tools is important to avoid duplication of work, and to ensure that both systems prevent current views of what needs to get done.

9. **Audit trail and compliance reporting:** A key value of automation is the ability to maintain an audit trail. You need to make sure your FM tool tracks everything, cannot be tampered with, and generates reports for both internal use and compliance. Additionally, ensure reports can be customized as necessary.

Of course this list isn't exhaustive. But it hits the high points of what to automate for firewall change management.

Automatic provisioning

One of the current religious battles on firewall operations involves whether the FM tool should actually commit changes to the firewall. You know, kind of like having Skynet managing missile defense systems. What could go wrong? All kidding aside, many security administrators are uncomfortable with a tool making changes directly, and have legitimate concerns.

One of the current religious battles on firewall operations involves whether the FM tool should actually commit changes to the firewall. You know, kind of like having Skynet managing missile defense systems.

We don't like wading into religious battles, so fortunately there is middle ground to be found. Some changes — simple network changes, reordering existing rules, etc. — pose acceptable risk to the security posture, and as such are good candidates for automated changes. Others,

including supporting new applications and changing entitlements for key organizations, demand additional scrutiny and human oversight.

Either way it is reasonable to expect your tool to generate scripts, command-line code, and/or detailed instructions for committing a change. Even if your folks have hands on keyboards to make changes themselves, they should get as much guidance as possible from the FM tool.

Provisioning Access for Business Applications

Another new function being introduced by firewall management vendors is the ability to have business users request access for specific applications or to shut down unsupported applications. The FM tool can translate that request into a set of instructions to be implemented on the firewall to allow or block access as necessary. Given the challenges of translating business-speak into access rules, and the importance of getting applications operational quickly without adding attack surface, this capability makes sense as part of the FM tool suite.

Our research indicates that this cutting-edge requirement appeals primarily in very mature operational environments with well-established network security operational processes and toolsets.

Our research indicates that this cutting-edge requirement appeals primarily in very mature operational environments with well-established network security operational processes and toolsets. Using a toddler analogy, many organizations are barely able walk in terms of managing their firewalls, using highly involved processes with few tools to manage network security devices. This capability is more like running, and only applicable to organizations with their acts together on both workflow and rule optimization.

Not that this capability won't be important in the future as network security evolves to next-generation, application aware platforms. We think it will, but it's still a early requirement for the bulk of enterprises. Although keep in mind the reality that in many organizations application development teams (or another group within IT) has the responsibility to understand the connectivity requirements for each application. So for a FM tool to offer this capability, the organizational model must be able to support it. But in either case, the FM tool can and should provide insight into assessing the risk of the rules already in place and providing the documentation to substantiate implemented controls, in alignment with the charter of the security function.

Optimizing Rules

So you need to occasionally clean up and reorganize — getting rid of stuff you don't need, making sure the stuff that's still in there belongs, and arranging things so you can easily access the stuff you use the most.

Now that you have a solid, repeatable, and automated firewall change management process, it is time to delve into another major aspect of managing your firewalls: optimizing rules. We talked about how firewall rule sets tend to resemble junk closets earlier. You have a ton of crap (firewall rules) in there, most of which you don't use, and whatever you do use is typically hard to reach. So you need to occasionally clean up and reorganize — getting rid of stuff you don't need, making sure the stuff that's still in there belongs, and arranging things so you can easily access the stuff you use the most. Now let's drop the analogy to talk firewall specifics.

You need to optimize rules for a variety of reasons:

1. **Eliminate duplicate rules:** When you have a lot of hands in the rule base, inevitably rules get duplicated. Especially when the management process doesn't require a search to make sure an overlapping rule doesn't already exist.

2. **Address conflicting rules:** At times you may add a rule (such as `ALLOW port 22`) to address a short-term issue, even though you might have other rules to lock down the port or application. Depending on the ordering of the rules, other rules might conflict, either adding attack surface or breaking functionality.

3. **Get rid of old and unused rules:** If you don't go back into the rule set every so often to ensure your rules are relevant, you are bound to build up rules that are no longer necessary, such as access to that old legacy mainframe application that was decommissioned 4 years ago. It is also useful to go back and confirm with each rule's business owner that their application still needs access, and they are willing to accept responsibility for those rules.

4. **Simplify the rule base:** The more rules, the more complicated the rule base, and the more likely something will go wrong. By analyzing and optimizing rules on a periodic basis, you can find and remove unneeded complexity.

5. **Improve performance:** If you have frequently used rules at the bottom of the rule base, the firewall needs to go through every preceding rule to reach them. That can bog down performance, so you want the most frequently hit rules as early as possible in the firewall rule set — without conflicting with other rules, of course.

6. **Controlling network risk:** Networks are very dynamic, so you need to ensure that network and firewall configuration changes don't add attack surface. In that case, you may need to either roll back the change or make a corresponding firewall rule change to compensate for the additional attack surface.

For all these reasons going through the rule base on a regular basis is key to keeping firewalls running optimally. Every rule should be required to support the business, accurately configured, and ordered to maximize device performance.

Key Firewall Management Rule Optimization Features

Specific features you should get in your firewall management product or service directly address the requirements above.

1. **Centralized management:** A huge benefit of actively managing firewalls is the ability to enforce a set of consistent policies representing security posture across all firewalls, regardless of vendor. You need a scalable tool that supports all your devices, and should have a single authoritative source for firewall policies.

2. **Recommend rule changes:** If a firewall rule set gets complicated enough, it is hard for any human — even your best security admin — to keep everything straight. So a FM tool should be able to mine an existing rule set of thousands of rules to find and get rid of duplicate, hidden, unused, and expired rules. Tools should assess the risk of each rule and flag rules which allow too much access (you know: `ALLOW ANY ANY`).

3. **Optimize rule order:** A key aspect of improving firewall performance is making sure the most frequently hit rules are close to the top of the rule base. The tool should track which rules are hit most often through firewall log analysis and suggest an ordering to optimize performance without harming security posture.

4. **Simulate rule changes:** Clever ideas can turn out badly if a change conflicts with other rules or opens up (or closes) the wrong ports/protocols/applications/users/groups, etc. The tool should simulate rule changes and predict whether each change is likely to present problems.

5. **Monitoring network topology and device configuration:** Every network and firewall configuration change can expose additional attack surface, so the tool needs to analyze every proposed change in context of the existing rule set to control network risk. This involves polling managed devices for their configurations on a periodic basis, as well as monitoring routing tables.

6. **Check compliance:** Changes can also cause compliance violations. So you need a firewall management tool to flag rule changes that might violate compliance mandates.

7. **Recertify rules:** The firewall management tool should offer a mechanism to go back to business owners to ensure rules are still relevant and that they accept responsibility for their rules. To facilitate this, you should set expiration dates on the rules, and then require an owner to confirm each rule is still necessary upon expiration. This provides an ongoing and consistent means to prune the rule set on an ongoing basis.

Asking for Forgiveness

Speaking of firewall rule recertification, you certainly can go through the process of chasing down all the business owners of every rule implemented on your devices, if you know who they are, and getting them to confirm each rule is still needed. That's a lot of work. You could choose a less participatory approach as well: make changes and then ask forgiveness if you break something. There are a couple options with this approach:

You could choose a less participatory approach as well: make changes and then ask forgiveness if you break something.

1. **Turn off unused rules:** Use the firewall management tool's ability to flag unused rules and just turn them off. If someone complains you know the rule is still required and you can assume they would be willing to recertify the rule. If not you can get rid of it.

2. **Blow out the rule base:** You can also wipe the rule base and wait for complaints about applications you broke. This is only sane in dire circumstances, where no one will take responsibility for rules or people are totally unresponsive to attempts to clean things up. But it is an option.

NGFW Support

With the move to Next-Generation Firewalls (NGFW), you need to start managing policies which are not simply based on port/protocol/source/destination combinations. You have to address applications, identities, and content. Even better, you can get very granular in what is allowed for specific applications, enabling you to set specific policies for key application features such as Facebook chat and Twitter direct messages.

Your firewall management tool needs to not only support and optimize these advanced rules, but also to facilitate the migration to application-aware rules.

Your firewall management tool needs to not only support and optimize these advanced rules, but also to facilitate the migration to application-aware rules. By analyzing firewall logs, the tool should be able to suggest a set of NGFW policies to reflect your organization's usage patterns for websites and other applications. Many NGFW vendors have their own tools to facilitate this migration but none are cross-platform, and they tend to ignore optimization once rules are migrated.

The addition of threat prevention (IPS) and malware detection to the NGFW to become a PSG also adds complexity. Over time you should expect your firewall management tool to be able to configure, optimize, and tune attack policies — and to suggest specific actions based on malware determinations. This is not your grandpappy's firewall — the PSG requires a much more sophisticated operational environment to keep its rules under control.

Firewall Migration

Another advantage of firewall management tools is heterogeneous firewall support. Firewall vendors treat their devices like the Hotel California. Once you import rules they never want you to leave. Vendors have little incentive to ease migration to competing devices.

But that may not fit the way you want to run your environment. You might want to move devices around. Or buy some cheap gear on eBay. Or maybe use firewalls from an acquired company currently deployed as doorstops. Regardless of use case, a firewall management tool should help you maintain a consistent security posture by normalizing the nuances of each firewall vendor's capabilities and feature sets. Even better, the tool should optimize policies as they are deployed so each device is working as efficiently as possible.

Managing Access Risk

Now let's work through managing risk using the firewall. First we need to define risk, because depending on your industry and philosophy, risk can mean many different things. For firewall management we care about the risk of unauthorized parties accessing sensitive resources. Obviously if a device with critical data is inaccessible to internal and/or external attackers, the risk it presents is lower.

For firewall management we care about the risk of unauthorized parties accessing sensitive resources. Obviously if a device with critical data is inaccessible to internal and/or external attackers, the risk it presents is lower.

This "access risk management" function starts with understanding the network's topology and security controls. Basically what the network looks like and what is connected to it. Visualized attack paths show how an attacker could access a critical device. With this information you can see which devices need patching or remediation, what firewall holes need to be closed, and other needed network workarounds — and then prioritize fixes. Another benefit of visualizing attack paths is improved understanding when changes on the network or security devices unintentionally expose additional attack surface.

So what does this have to do with your firewall? That's a logical question, but a key firewall function is access control. You configure the firewall and its rule set to ensure that only authorized ports, protocols, applications, users, etc. can use the network. Moreover, you can lock down critical devices, applications, etc. to accept traffic only from certain other devices or segments within your network. A misconfigured firewall can have significant and severe security consequences, as discussed above.

For example, years ago when supporting email security devices, we got a call about an avalanche of spam hitting the mailboxes of key employees. The customer was not pleased, but the deployed email security gateway appeared to be working perfectly. Initially perplexed, one of our engineers checked the backup email server and discovered it was open to Internet traffic due to a faulty firewall rule. Attackers were able to use the back-up server as a mail relay, and blasted all the mailboxes in the enterprise. With some knowledge of network topology and the paths between external networks and internal devices, this issue could have been identified and remediated before any employees were bothered.

Key Access Risk Management Features

When examining the network and keeping track of attack paths, look for a few key features:

1. **Topology monitoring:** Topology can be determined actively, passively, or both. For active mapping you will want your firewall management tool to pull configurations from firewalls and other access control devices. You also need to account for routing tables, network interfaces, and address translation rules. Interoperating with passive monitoring tools (network behavioral analysis, etc.) can provide more continuous monitoring. You need the ability to determine whether and how any specific device can be accessed, and from where — both internal and external.

2. **Analysis horsepower:** Accounting for all the possible paths through a network requires an *n* * (*n*-1) analysis, and *n* gets rather large for enterprise networks. The ability to re-analyze millions of paths on every topology change is critical for providing an accurate view.

3. **Prioritization:** There are many things that you can fix, but which one (or handful) are most critical to do *right now*? By factoring in access risk to your prioritization efforts (perhaps via a risk scoring mechanism), you can make the changes that will have the most significant impact on your security posture, as opposed to just making the next change on the list.

4. **What if?** You will want to assess each possible change before it is made, to understand its impact on the network and attack surface. This enables the organization to detect additional risks posed by a change before committing it. If that customer had had a tool to help understand that a firewall rule change would expose their backup email server to attackers, they would have reconsidered.

5. **Alternative rules:** It is not always possible to remediate a specific device due to operational issues. So to control risk you would like a firewall management tool to suggest appropriate rule changes or alternate network routes to isolate the vulnerable device and protect the network.

Although we discussed these functions as distinct requirements of firewall management, you need all these functions to work together to achieve operational excellence.

It should be clear that all these firewall management functions depend on each other. Optimizing rules is part of the change management process, and access risk management comes into play for every change. And *vice versa,* so although we discussed these functions as distinct requirements of firewall management, you need all these functions to work together to achieve operational excellence.

Quick Wins

We are big fans of a *Quick Wins* approach, because far too many technologies sputter as deployment lags and the investment's full potential is never realized. The quick wins approach focuses on building momentum early in the deployment by balancing what can be done right now against long-term goals. If a project team doesn't prove value early and often, the implementation is likely doomed to failure. For firewall management the lowest hanging fruit is optimization of existing rule sets before implementing a strong change management process. But let's not put the cart before the horse — first you need to deploy the tool and integrate with other enterprise systems.

The quick wins approach focuses on building momentum early in the deployment by balancing what can be done **right now** against long-term goals.

Deployment and Integration

The good news for firewall management is that one central server can handle quite a few firewalls — especially because the optimization and change management processes happen on a periodic, rather than continuous or real-time, basis. It's not like management devices need to be inline and monitoring continuously, so deployment architecture should not make or break the implementation. Typically you deploy the firewall management server in a central location and have it discover all the firewalls in your environment as it examines the network topology. Alternatively, you might kickstart the effort by feeding a list of your existing firewalls (including configurations, credentials, and rule sets) into the system.

Do you want one central system or a distributed environment? That depends on how quickly you need to be notified of changes. The longer you go before rechecking each device's configuration, the wider the window before you detect an unauthorized rule or configuration change. You need to balance resource consumption against frequent checks to narrow the exploitation window between attack and detection.

Because the change process (workflow) can run off the central server, and the math to optimize a rule set doesn't consume resources on firewalls, firewall management doesn't require a pallet of devices — even for enterprise deployments. It's not like doing malware analysis within a network security device. We see large firewall environments (think service providers) managed by a handful of firewall management devices — multiple devices for availability and redundancy, rather than for performance.

Given the operational leverage of automating an effective firewall change management process, you will want to make sure changes are tracked in whatever tool(s) the operations team uses so you don't have two sources of information, with everything out of sync.

For integration, as described earlier in this paper, you will want to pull or push information from tools such as a vulnerability management system, a SIEM/log management tool, and/or a reporting/GRC system — the enterprise security tools already in use. It is reasonable to expect your vendor to already have integrated with the leading tools in these categories. Pulling information into the firewall management tool provides more contextual understanding of which changes pose what risk.

The area which most stands to benefit from enterprise integration is the help desk/task management system. Given the operational leverage of automating an effective firewall change management process, you will want to make sure changes are tracked in whatever tool(s) the operations team uses so you don't have two sources of information, with everything out of sync. The good news is that these help desk tools are mature, with well-developed integration SDKs. Again, it is reasonable to expect your firewall management vendor to have already integrated with your work management system.

Getting the Quick Win and Showing Value

We covered the change management process first in this paper, because it is where we typically see the most sustainable value accrued over time. But in a quick wins scenario we need to get something done *now*. So going through existing firewalls and pinpointing areas for improvement, in terms of both security and performance can provide our quick win. This is the optimization process.

The priority is to get value, but that is no good unless you can communicate it. So look to generate reports that highlight the results of early optimization efforts. You will want to show how many unused rules were eliminated (reducing attack surface), whether any of your old rules conflicted, how the cleanup improved security, etc. This quick effort (it should take a day or two) builds momentum for change management.

Once the change management process is accepted in the environment and implemented in the firewall management tool, you can start tracking service levels and response times of changes. You can also track the number of changes that *would* have increased attack surface, but were flagged and prevented by the FM tool, to show how the tool reduces risk and prevents human error.

This highlights the value of a firewall management tool for reducing the risk of a faulty rule change increasing attack surface. A what-if analysis of potential changes can ensure that nothing will break (or crush performance) before actually making a change.

You can also demonstrate value by migrating rules from one firewall to another. If you need to support a heterogeneous environment, or are currently moving to a NGFW-based perimeter architecture, these tools can provide value by suggesting rule sets based on existing policies and optimizing them for the new platform. If you are a glutton for punishment you can migrate one device without using the tool (bust out your old spreadsheets), and then use the firewall management tool for the next migration, to provide a real comparison. Or you can use an anecdote (we saved *XX* days by using the tool) to communicate its value. Either way, substantiate the value of the tool to your operational process.

Finally, at some point after deploying the tool, you will have an assessment or audit. You can again leverage and quantify the value of the firewall management tool, in terms of saving time and increased accuracy of audit documentation. Depending on the regulation, the tool is likely to include a pre-built report which requires minimal customization the first time you go through the audit, to generate documentation and substantiate your firewall controls.

Finally, at some point after deploying the tool, you will have an assessment or audit. You can again leverage and quantify the value of the firewall management tool, in terms of saving time and increased accuracy of audit documentation.

You have now learned a bit about how to manage your firewalls in a rapidly changing environment — using automation to streamline solid change management processes and efforts, and to optimize your rule base to improve performance and reduce risk. Focusing on quick wins from the deployment will build momentum for the long-term strategic value of a firewall management tool.

If you have any questions on this topic, or want to discuss your situation specifically, feel free to send us a note at info@securosis.com or ask via the Securosis Nexus (http://nexus.securosis.com/).

About the Analyst

Mike Rothman, Analyst/President

Mike's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security — such as protecting networks and endpoints, security management, and compliance. Mike is one of the most sought-after speakers and commentators in the security business, and brings a deep background in information security. After 20 years in and around security, he's one of the guys who "knows where the bodies are buried" in the space.

Starting his career as a programmer and networking consultant, Mike joined META Group in 1993 and spearheaded META's initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held executive roles at CipherTrust and TruSecure. After getting fed up with vendor life, Mike started Security Incite in 2006 to provide a voice of reason in an over-hyped yet underwhelming security industry. After taking a short detour as Senior VP, Strategy at eIQnetworks to chase shiny objects in security and compliance management, Mike joined Securosis with a rejuvenated cynicism about the state of security and what it takes to survive as a security professional.

Mike published The Pragmatic CSO <http://www.pragmaticcso.com/> in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional. He also possesses a very expensive engineering degree in Operations Research and Industrial Engineering from Cornell University. His folks are overjoyed that he uses literally zero percent of his education on a daily basis. He can be reached at mrothman (at) securosis (dot) com.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **The Securosis Nexus**: The Securosis Nexus is an online environment to help you get your job done better and faster. It provides pragmatic research on security topics that tells you exactly what you need to know, backed with industry-leading expert advice to answer your questions. The Nexus was designed to be fast and easy to use, and to get you the information you need as quickly as possible. Access it at <https://nexus.securosis.com/>.

- **Primary research publishing**: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.

- **Research products and strategic advisory services for end users**: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessment.

- **Retainer services for vendors**: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.

- **External speaking and editorial**: Securosis analysts frequently speak at industry events, give online presentations, and write and/or speak for a variety of publications and media.

- **Other expert services**: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis. For more information about Securosis, visit our website: <http://securosis.com/>.