FIREMON

WHITE PAPER

IMPROVING FIREWALL CHANGES

OVERCOME PROCESS AND COMPLEXITY CHALLENGES BY FOCUSING ON THE FIREWALL.

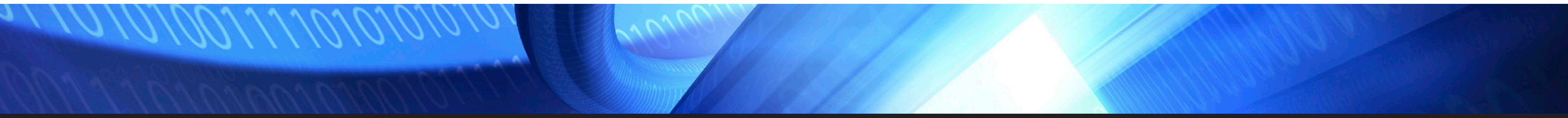
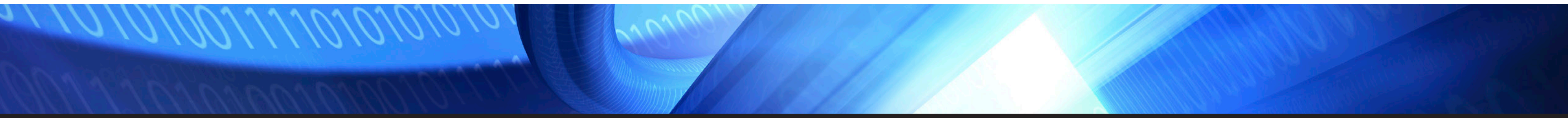


Table of Contents



Executive Summary

Firewall changes are a constant. As business grows, changes must be made to the firewall to accommodate the new requirements. These changes present a number of challenges to firewall administrators and can present serious risk to the business. Changes in general, whether to a firewall, router, application or any other part of the IT infrastructure, are the single greatest cause of outages. If change is not effectively managed, it presents a serious risk to business continuity.

One of the greatest causes of ineffective change is an incorrect change, not simply an accident, but a concerted effort to make the right change that in reality is simply incorrect. In particular, with a firewall, the complexity of the existing infrastructure along with the complexity of the change makes incorrect changes a likely result. Process is part of the answer—ensuring all changes have been reviewed and approved prior to implementation and that changes are verified after they are implemented.

However, process alone is not enough. A number of processes have been in place for years. Process technology solutions, such as Remedy, have existed as long as the firewall. And yet, mistakes are still made, ineffective changes are still implemented and none of these processes have made the job of the firewall engineer any easier. Technology that is firewall-aware, and that can automatically track changes, recommend correct changes and aid in the enforcement of the change process is necessary to address the unique challenges facing enterprises today.

Challenges of Firewall Changes

Firewalls are a mature technology and yet the administration of firewalls has evolved very little since they were first introduced nearly two decades ago. A list of rules defining access to and from certain locations or users with defined services or applications is still the basis of all firewalls. Adding, deleting or modifying these rules is the most common change to a firewall. These changes happen at a staggering rate, with enterprises often editing more than 100 rules a week.

In addition to the sheer number of rules presenting a management challenge, the implications of making a mistake are dire. The moment that a change is made is the moment most likely to cause issues. By definition, if things are working well, then something has to change to cause a problem. Of course, many things can change, including environmental issues like hardware failure, changes to the threat landscape such as a disgruntled employee being fired, and expected administrative modifications of the configuration. While administrative modification is not the only kind of change, it is the most frequent and is the one that is controllable. To emphasize this point further, research shows that 62 percent of network outages are caused by human error[1]. Not nearly as well known is the percentage of security risks introduced by changes. Of course, when you consider that 99% of all firewall breaches are caused by incorrect configurations, it is clear that ineffective change is the cause of security risk posed to the enterprise.

None of this is new information nor is it surprising. Much effort has been expended to reduce the negative impacts of change. Comprehensive processes with process technology are often implemented to address these problems. However, in many cases, they are designed only to add checks into the process. That's not a bad thing, but each step adds cost to a change. Unfortunately, these added costs don't solve some of the most basic problems with firewall changes: how to make the change and how to determine if it is a good change. In effect, the process has become little more than a speed bump, implemented in the hope that, by slowing the process down, the risk will be reduced. While there is some truth to this notion, it is a costly effort that does not provide equitable return.

Changes must be effectively managed or they are likely to result in network outages, excessive effort or security risks, or, most likely, all of the above.

Process Limitations

Change Management is most often associated with the "process" of changes. In fact, Google the phrase "change management" and the first few entries are Wikipedia articles describing the process of change management. In particular, the Wikipedia article http://en.wikipedia.org/wiki/Change_management_(engineering) describing Change Management for Engineering, defines it as:

> *The change management process in systems engineering is the process of requesting, determining attainability, planning, implementing, and evaluating of changes to a system. It has two main goals: supporting the processing of changes – which is mainly discussed here – and enabling traceability of changes, which should be possible through proper execution of the process described here.*

There is no doubt that implementing and following a change management process is beneficial in improving the outcome of changes as well as improving the traceability of changes as demanded by most compliance standards. However, simply having a process, or even having a process-enabling technology, is still very deficient in many cases.

Anecdotally, consider the fact that IT change management systems have been around longer than the firewall. In most cases, firewall changes have been part of the IT change management process since they were first implemented. And yet, 20 years later, mistakes are still made and firewall policies are more complex than ever. Clearly the existing IT process is not completely effective.

[1] The Yankee Group 2002 Network Downtime Survey

Tracking each change request to ensure that the right people are involved and that the change is completed successfully is a key part of the process. However, it solves only a small part of a larger problem. The bigger issue with security in general and firewalls specifically is making the correct (secure) change. This complex technology problem is not adequately addressed by generic IT change processes. Generalized change processes are not firewall-specific, they do not help design the solution, they do not aid in either the review or the verification steps and they do not capture changes outside the process. These are not trivial issues.

Generic change management systems that capture general information such as date of request, name and description are effective at tracking progress, but they do very little to help define the access requested and are certainly not the solution. In most cases, customers work around these deficiencies by attaching a Word document or a spreadsheet that describes the request. These work-around "solutions" are a clear indication that something is wrong with the system.

Making the right change is perhaps the biggest issue related to firewall change management. A number of studies[2] [3] have identified that as the complexity of the firewall configuration increases, the number of mistakes increases. Security is under additional scrutiny not associated with other disciplines in that the success of a change is measured not only by if it "works," but also if it maintains an acceptable level of security. This additional burden is a significant difference in the time and effort that must be exerted to ensure the correct change is made. The existing change process tools do nothing to address this problem.

The review and verification of changes are hindered by the same issues in engineering the correct solution. Excessive complexity, limited visibility and a lack of useful tools in the change process make reviewing and verifying changes nearly impossible. In the best scenario, excessive time and effort is spent to ensure that the security of the network is maintained. In the worst case, security is left to the engineer solely and only functionality is verified, defeating one of the primary goals of the change process: to ensure the correct change is made.

In addition to the difficulty of managing changes that go through a standard change process, there is a significant challenge in managing the changes outside of the change process. Whether those changes are made by a malicious attacker or a misguided engineer who means well, the impact can be disastrous.

Unmanaged change is a leading cause of network outages. Not only is unmanaged change a problem in its own right, without knowledge of where the change occurred, recovering from these outages may take hours or even days. An even more severe result of unmanaged change is the potential to miss a blatant security gap. With hundreds of rules per firewall, a single undetected change to a firewall policy could significantly compromise the network.

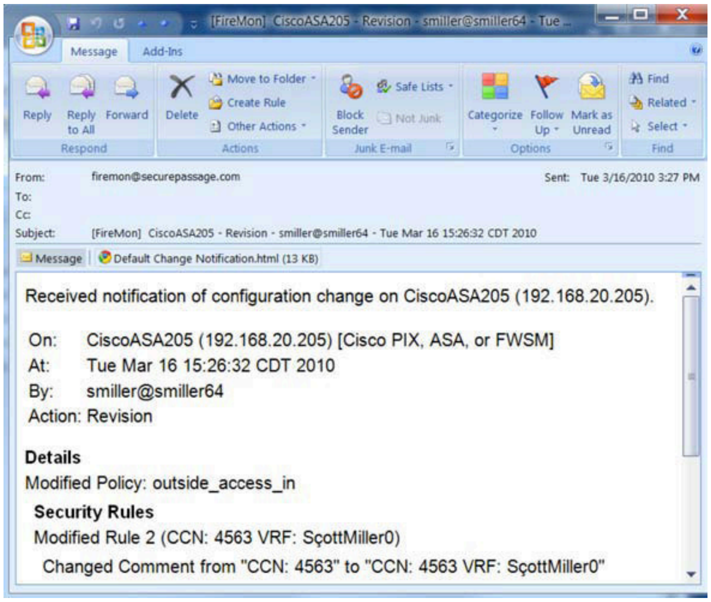
How FireMon Solves the Firewall Change Management Challenge

- **Focus on the Firewall**
  It is clear that process plays an important role in addressing firewall change management issues, but it is also clear that process alone is not sufficient. To be effective, the process must be augmented by a solution that aligns the process with the device. This solution should focus on the firewall and include at least five key elements:
  - Real-Time Change Monitoring
  - Firewall-Specific Process
  - Firewall Engineering Tools to Plan Changes
  - Review and Verification Tools
  - Traceable Historical Changes

[2] "Fast, Cheap and in Control: A Step Towards Pain Free Security!" Bhatt, Sandeep, Okita, Cat, Rao, Parsad, HP Laboratories, September 21, 2008

[3] "Survey on Firewall Policy Management," FireMon, Spring 2009

FireMon’s Security Manager and Policy Planner solutions offer all of these features and more. With powerful tools to aid in analysis, along with detailed documentation to provide visibility and traceability of changes over time, FireMon keeps the focus on the firewall.



From: firemon@securepassage.com Sent: Tue 3/16/2010 3:27 PM
To:
Cc:
Subject: [FireMon] CiscoASA205 - Revision - smiller@smiller64 - Tue Mar 16 15:26:32 CDT 2010

Received notification of configuration change on CiscoASA205 (192.168.20.205).

On: CiscoASA205 (192.168.20.205) [Cisco PIX, ASA, or FWSM]
At: Tue Mar 16 15:26:32 CDT 2010
By: smiller@smiller64
Action: Revision

Details
Modified Policy: outside_access_in
Security Rules
Modified Rule 2 (CCN: 4563 VRF: SçottMiller0)
Changed Comment from "CCN: 4563" to "CCN: 4563 VRF: SçottMiller0"

Image 1: Change Notification Delivered in Email

- **Real-Time Change Monitoring**
  Change monitoring is a technical activity that detects when changes are made to a system. FireMon Security Manager detects all firewall changes, both planned and unintended, retrieves them and archives the previous firewall configurations. And Security Manager keeps firewall administrators informed of changes with email notifications that describe the differences between the current configuration and the previous one.
- **Firewall-Specific Process**
  Any change management system can gather approvals and enforce a generic workflow. FireMon focuses on firewalls. What are best practices for managing firewall changes? What data is necessary for the administrator to make a good change? Is the change made today appropriate and will it be understandable in the future? FireMon was built with answers in mind.

  FireMon Policy Planner collects change requests with firewall-specific access data like business justification and the action and service requested. Once submitted, firewall administrators have all the information they need to start planning the access. That means less time spent on follow-up questions and more time spent engineering solutions.
- **Firewall Engineering Tools to Plan Changes**
  Firewall change management is an engineering and operations challenge. Not only must configuration changes be made quickly through the proper workflow, but ideally, each configuration change should be correct from the start. Policy Planner’s rule recommendation tools analyze current configurations to find the best way to implement the requested access. Policy Planner indicates if the access already exists, where a configuration could be modified to meet the request, or if a new rule should be created.

  Assessing and communicating the risk of a proposed change is a challenge. By knowing what modifications are about to be made to the firewall and using its patented risk assessment engine, Policy Planner provides all the details necessary to prevent introducing risky access. And to ensure that new rules maintain compliance Policy Planner identifies and highlights proposed rules which would violate existing compliance policies.

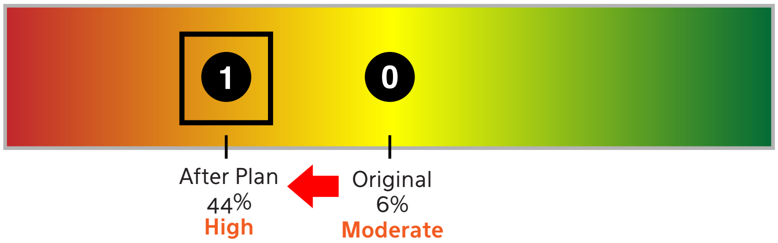


Image 2: Model effect of requested changes - BEFORE implementation

- **Review and Verification Tools**
  Most change management systems present tickets for approval without the complete context of the request or the designed solution. Policy Planner presents the business requirement for the access next to the proposal for the technical implementation so that stakeholders understand precisely what they are approving. Once the new configuration is deployed, Security Manager collects the configuration and provides details of the change for comparison with the plan. At every stage in the firewall change management process, administrators can rest assured that their changes are correct, approved, and implemented as planned.
- **Traceable Historical Changes**
  From the management of access request tickets, to the collection and analysis of the resulting configuration changes, Security Manager provides a complete history of each firewall. Details of every change, including errant changes made outside the standard process, are available in graphical reports. These reports include the documentation of access, including access justification, business owner, and rule expiration date, all displayed within the context of the rule. The result is an audit trail available in graduated detail so that everyone who manages that firewall can understand its past and present, and can better plan for future changes.
- **Integrate into the Enterprise**
  Most enterprises have an established change management system. FireMon can integrate into existing business process tools like Remedy, bringing firewall intelligence to standard enterprise systems. For example, FireMon's rule recommendation tool and verification tool can plug into a third-party system at the Design and Verification steps. Then, managers and auditors can use FireMon to validate that access requested through their system was correctly engineered, approved and implemented. Whether it's supporting existing internal processes and technology with device-specific knowledge, or acting as a standalone change management system, there is a Policy Planner configuration to suit any organization.
- **Document the History**
  It can be done now, easily, or it can be done a year from now, painfully. Either way, configuration changes to firewalls must be documented, usually to comply with corporate standards or with regulatory requirements. For anyone who is too busy making changes to document them, FireMon makes it easier.

  Relevant change management information such as requestor and expiration date can be automatically drawn from third-party ticketing systems into Security Manager, where it is permanently associated with the modified policy and rule. Data such as justification and business owner can be entered directly in the comments column of a rule; Security Manager retrieves this meta-data along with the configuration. Additionally, administrators can choose to add meta-data directly to the configuration archived in Security Manager. When collected, data points from the ticket and the configuration become documentation of the security policy, available as a reportable history for every managed firewall. And the administrator who is asked, "Why was this change made?" can easily answer.

Summary

Changes to enterprise firewalls are the inevitable result of administrative initiative, and sometimes, malicious intent or mistakes. Each change is an opportunity to improve the integrity of the security policy, but as firewall configurations grow more complex and less understandable, even planned changes are made without sufficient knowledge. That's when a good change becomes a risky one.

An established change management process helps, but neither the process nor its underlying technology have the device specificity essential to managing firewalls. Generic processes and systems do not help design and track the correct firewall change from the beginning, much less enforce a firewall-specific change process. As such, the risk of incorrect changes increases, and with it, the risk posed to the enterprise.

Firewall changes should be managed with a firewall-aware technology. The ideal technology solution supports change management by: collecting all configuration changes in real time; offering a change management process specifically for firewalls; providing rule planning, review and verification tools to design and confirm configuration changes; and archiving all configuration changes with supporting documentation. The best solution also integrates into existing enterprise systems intelligently, and enables immediate, incremental documentation of policy changes.

Better firewall changes are made through better firewall management. Firewall-aware technology such as FireMon Security Manager and Policy Planner is where better management starts.

Additional Recommended Reading

To read the following articles of interest, please visit our Resource page at www.firemon.com/company/resources.aspx.

Performance Impacts of Complexity

This article discusses the impact of policy size and rule order on firewall performance.

Firewall Cleanup White Paper

This white paper highlights considerations for improved firewall efficiency, better security and reduced policy complexity.

Firewall Economics – Spire Security Research Report

This paper highlights the challenges of firewall administration and discusses the economic opportunities associated with automation.

Survey Report on Firewall Complexity

This report provides survey results for more than 250 network and IT personnel regarding their management of complex firewall policies.