SOLARWINDS WHITEPAPER

Best Practices for Effective Firewall Management

Author: Vinod Mohan

Follow SolarWinds:

Firewalls are one of the more complicated devices on a network to configure, manage, and troubleshoot because there are implications that affect the network, security, and systems processes. A firewall defines the perimeter-level security for an enterprise. Network administrators should be able to manage firewalls effectively to ensure the IT infrastructure is guarded against unauthorized and potential harmful traffic from outside the network. The following are important firewall management best practices that will benefit all networks and network administration teams.

#1 Clearly Define A Firewall Change Management Plan

Firewall changes are inevitable. They are an on-going process that ensures that firewall rules continue to get stronger and more capable of warding off security threats. At the same time, a not-so-well-planned change can leave a gaping hole in your network security.

A well-defined firewall change management plan should include:

- A detailed plan on changes and their objectives
- An estimation of risks due to the policy changes, their expected impacts, and a mitigation plan
- A centralized change-management workflow and change-control policy between different network teams and proper change approvals
- Proper audit trails of the change including who made the change, when they made it, why they made it, and the outcome of the change.

Do not fear change in firewall policies! Just be proactive and prudent in planning well in advance.

#2 Test the Impact of Firewall Policy Change

Once you plan a policy change (i.e. adding a new rule or modifying an existing one), test the change before you implement it. This is highly recommended as you can study the impact of the change in a test environment to avoid unexpected detriment to the network in terms of firewall performance, network traffic flow, and the change's impact on other devices and systems.

To test your policy change, you can use a virtual sandbox. Or you can use a firewall security management tool to conduct predictive change modeling to simulate and virtually send packets across the network path with the new or modified firewall rule. For this process, you need to:

1. Trace the path of packet traversal through the network layer and confirm that all devices along the path allow the packet to reach its intended destination.

2. Confirm that the firewall is allowing and blocking data according to the established policies and rule sets.
3. Perform an analysis to identify which device policies are blocking the packet from reaching its destination.

This is done by finding all routable paths to the packet destination, taking into account NATing along the path, and evaluating the ACL on each device along the path to check if the device allows or drops the packet.

#3 Clean Up and Optimize Firewall Rule Base

This is a critical activity that will have a positive impact in enhancing firewall security, improving firewall performance, and boosting the efficiency of your operational firewall management. There might be many firewall rules, objects redundancies, duplicate rules, and bloated rules that can cause security and management headaches.

- Redundant or duplicate rules slow firewall performance because they require the firewall to process more rules in its sequence.
- Orphaned or unused rules make rule management more complex, which creates a security risk by opening up a port or VPN tunnel.
- Shadowed rules can leave any other critical rule unimplemented.
- Conflicting rules may create backdoor entry points.
- Unnecessarily boated firewall rules can complicate firewall security audits.
- Erroneous or incorrect rules with typographical or specification inaccuracies can cause rules to malfunction.

Optimize your firewall rule base and clean up your unwanted firewall rules properly and regularly.

#4 Schedule Regular Firewall Security Audits

Firewall policy audits are necessary to ensure that firewall rules are compliant with organizational security regulations as well as any external compliance regulations that apply. Erroneous or unauthorized firewall policy changes can often cause non-compliance. IT security teams should always conduct periodic firewall security audits to identify policy violations.

Because constant firewall rule changes can result in a misconfiguration or exposure to a new network, you need to be able to determine the critical hosts exposed to dangerous services based on ACLs, routing, NAT rules, and anti-spoof settings and isolate the rules that are responsible for flagged risks. Firewall security audits can help identify how changes to the network will affect your security profile. You should also perform firewall security audits under the following conditions:

- When there is a new firewall installed
- When there is firewall migration activity happening on the network
- When there is bulk configuration changes made on firewalls

#5 Monitor User Access to Firewalls and Control Who Can Modify Firewall Configuration

A firewall is your first line of defense. You don't want unauthorized people gaining access and altering your firewall configuration. It's important to institute stringent network-access security and user-permission control to ensure that only authorized administrators have access to change firewall rules. Also, that these activities are logged in audit trails and are available for audits and compliance.

- Adopt network configuration management techniques to monitor firewall configuration changes in real time and provide alerts if there are unwarranted configuration changes.
- Ensure that you have a configuration restore option in place when unexpected or incorrect configuration changes have been made on the firewall and you need to revert back to an earlier state.
- Monitor firewall logs to identify any unauthorized break-in attempt on the firewall from both outside and inside the network.
- Create user profiles and assign varying levels of access to IT staff who are in charge of managing firewalls.

#6 Update Firewall Software Regularly

Firewall vendors release software upgrades to their firewalls for many security reasons. It's imperative that you keep your firewall software version updated to ensure you don't leave any loopholes that would compromise security. You can also perform vulnerability tests on your firewall to assess your software for flaws and weaknesses.

#7 Centralize Firewall Management for Multi-Vendor Firewalls

Companies generally have firewalls from multiple manufacturers as this helps provide in-depth security to the network. Although all firewalls serve the same purpose of providing security, firewalls from different vendors are architecturally different. This necessitates a different level of administration and support, and different personnel skill sets for managing a heterogeneous firewall environment. For example, Cisco® firewalls have rule sets that can be enforced on an entering or exiting interface of the traffic. They also have a "NAT control" feature that serves as an additional access control function. Juniper® NetScreen™ firewalls enable users to apply rule sets based on the origination zone and the destination zone.

If you are managing multiple firewall policies and settings, it is possible that you can end up having inconsistencies in your configurations. There is also the additional administrative challenge of using different management consoles, which complicates the rules and policies comparison.

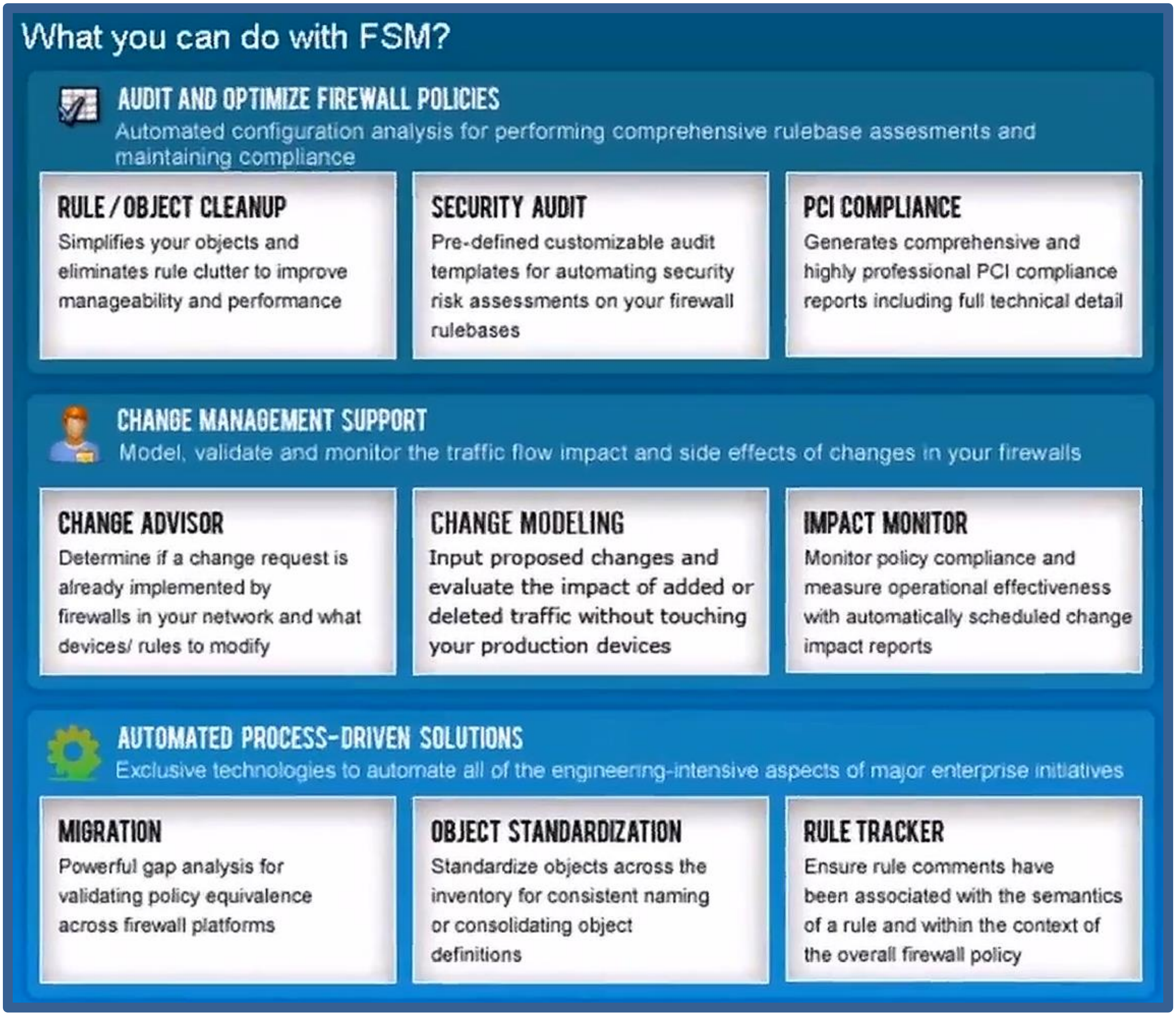
A centralized multi-vendor firewall management tool provides a unified view of firewall policies and rules allowing you to easily compare and manage firewall rules, perform security auditing and reporting, troubleshoot configuration issues, and provide support with gap analysis for firewall migration.

10 Useful Tips for Firewall Rule Creation & Management

1. Ensure all rules and objects follow standard naming conventions. Otherwise, identifying the unwanted rules later on will be very difficult.
2. Prioritize the rules in proper logical order to ensure that the firewall processes them according to the security requirements of your firewall policy. Here is a set of general rule recommendations:
    a) Global deny rules
    b) Global allow rules
    c) Rules for specific computers
    d) Rules for specific users, URLs, and Multipurpose Internet Mail Extensions (MIME) types
    e) Other rules based on your organizational network policy
3. Always group rules that belong together for easy management.
4. Don't complicate firewall management by unnecessarily nesting rule objects.
5. Try to use the same rule set for similar firewall policies with the same group object.
6. Add expiry dates (as comments) for temporary rules and regularly review these dates for rule clean-up.
7. Avoid using the "***Any***" option in the firewall's "***Allow***" rules. This may result in allowing every protocol through the firewall.
8. Never have the "***Allow All***" rule as your first rule.
9. It's better to have a "***Deny All***" rule as your first firewall rule, and then add other exceptions to allow traffic as needed.
10. Run regular risk queries to identify vulnerable firewall rules.

About SolarWinds® Firewall Security Manager

SolarWinds Firewall Security Manager (FSM) is a multi-vendor firewall security and change management solution that simplifies firewall troubleshooting and security management for your multi-vendor, Layer 3 network devices. It also helps you find and fill gaps in your security rules. Use Firewall Security Manager to view and query device configurations in a normalized format, compare configuration versions, and model configuration changes before implementing them.



What you can do with FSM?

AUDIT AND OPTIMIZE FIREWALL POLICIES

Automated configuration analysis for performing comprehensive rulebase assesments and maintaining compliance

RULE / OBJECT CLEANUP

Simplifies your objects and eliminates rule clutter to improve manageability and performance

SECURITY AUDIT

Pre-defined customizable audit templates for automating security risk assessments on your firewall rulebases

PCI COMPLIANCE

Generates comprehensive and highly professional PCI compliance reports including full technical detail

CHANGE MANAGEMENT SUPPORT

Model, validate and monitor the traffic flow impact and side effects of changes in your firewalls

CHANGE ADVISOR

Determine if a change request is already implemented by firewalls in your network and what devices/ rules to modify

CHANGE MODELING

Input proposed changes and evaluate the impact of added or deleted traffic without touching your production devices

IMPACT MONITOR

Monitor policy compliance and measure operational effectiveness with automatically scheduled change impact reports

AUTOMATED PROCESS-DRIVEN SOLUTIONS

Exclusive technologies to automate all of the engineering-intensive aspects of major enterprise initiatives

MIGRATION

Powerful gap analysis for validating policy equivalence across firewall platforms

OBJECT STANDARDIZATION

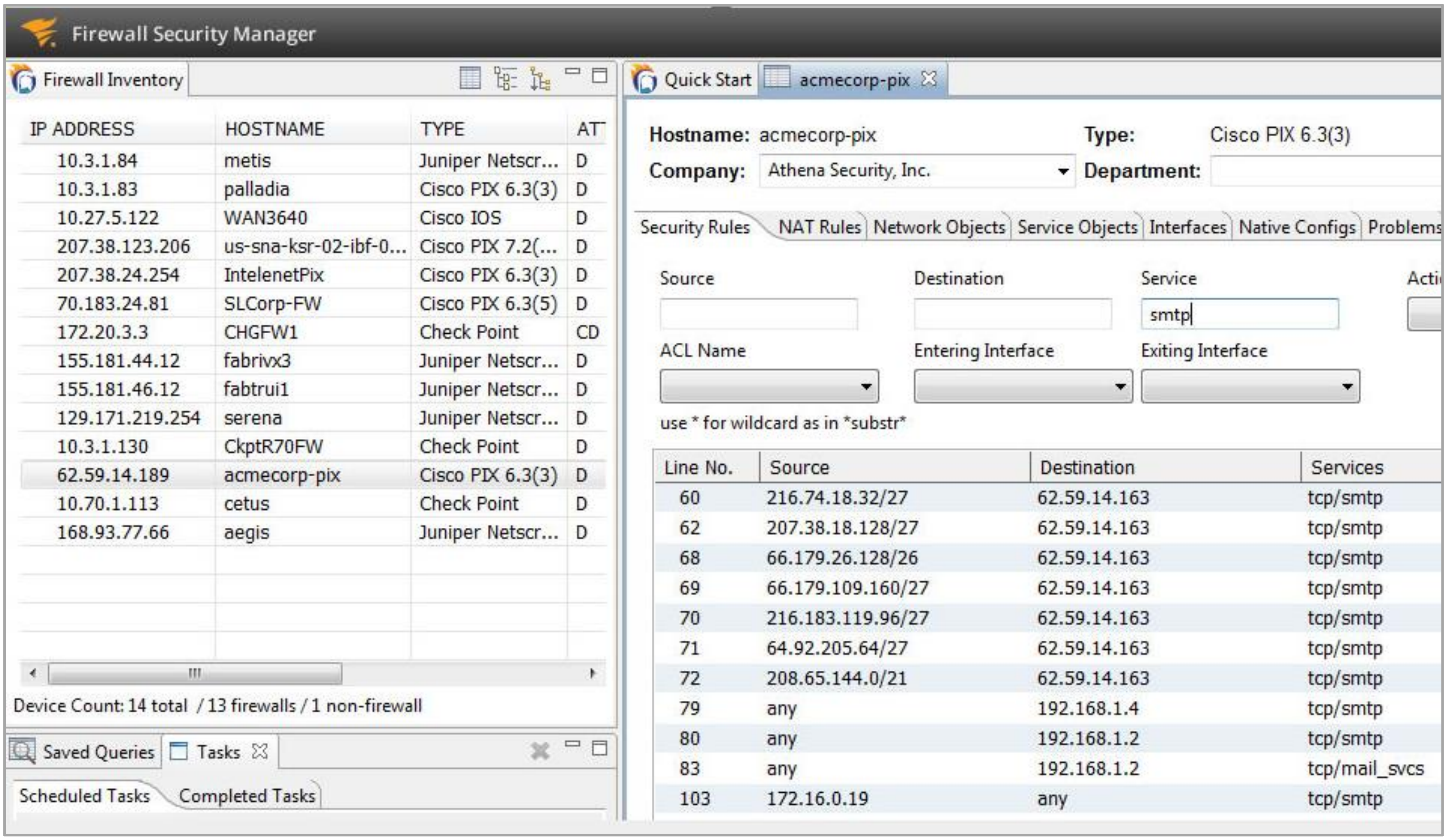
Standardize objects across the inventory for consistent naming or consolidating object definitions

RULE TRACKER

Ensure rule comments have been associated with the semantics of a rule and within the context of the overall firewall policy

Feature Highlights:

- Automates security audits using over 120 customizable, out-of the-box checks based on standards from NSA, NIST, SANS and more
- Analyzes firewall configurations and logs to isolate and remove redundant, covered and unused rules and objects
- Models how a new rule, or change to an existing one, will impact your firewall policy—without touching production devices
- Helps remove unnecessary rules and objects without causing an adverse impact on existing service availability or exposing the business to unauthorized traffic
- Deploys quickly and easily. Scan your inventory for high-risk firewalls and assess your risk profile in minutes



IP ADDRESS	HOSTNAME	TYPE	AT
10.3.1.84	metis	Juniper Netscr...	D
10.3.1.83	palladia	Cisco PIX 6.3(3)	D
10.27.5.122	WAN3640	Cisco IOS	D
207.38.123.206	us-sna-ksr-02-ibf-0...	Cisco PIX 7.2(...	D
207.38.24.254	IntelenetPix	Cisco PIX 6.3(3)	D
70.183.24.81	SLCorp-FW	Cisco PIX 6.3(5)	D
172.20.3.3	CHGFW1	Check Point	CD
155.181.44.12	fabrivx3	Juniper Netscr...	D
155.181.46.12	fabtrui1	Juniper Netscr...	D
129.171.219.254	serena	Juniper Netscr...	D
10.3.1.130	CkptR70FW	Check Point	D
62.59.14.189	acmecorp-pix	Cisco PIX 6.3(3)	D
10.70.1.113	cetus	Check Point	D
168.93.77.66	aegis	Juniper Netscr...	D

Device Count: 14 total / 13 firewalls / 1 non-firewall

Hostname: acmecorp-pix **Type:** Cisco PIX 6.3(3)

Company: Athena Security, Inc. **Department:**

Source: Destination: Service: smtp Acti

ACL Name: Entering Interface: Exiting Interface:

use * for wildcard as in *substr*

Line No.	Source	Destination	Services
60	216.74.18.32/27	62.59.14.163	tcp/smtp
62	207.38.18.128/27	62.59.14.163	tcp/smtp
68	66.179.26.128/26	62.59.14.163	tcp/smtp
69	66.179.109.160/27	62.59.14.163	tcp/smtp
70	216.183.119.96/27	62.59.14.163	tcp/smtp
71	64.92.205.64/27	62.59.14.163	tcp/smtp
72	208.65.144.0/21	62.59.14.163	tcp/smtp
79	any	192.168.1.4	tcp/smtp
80	any	192.168.1.2	tcp/smtp
83	any	192.168.1.2	tcp/mail_svcs
103	172.16.0.19	any	tcp/smtp

LEARN MORE »

DOWNLOAD FREE TRIAL

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide. Focused exclusively on IT Pros, we strive to eliminate the complexity in IT management software that many have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use, and maintain, while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, thwack, to solve problems, share technology and best practices, and directly participate in our product development process. Learn more at http://www.solarwinds.com.

Resources for Additional Learning

1. **Video**: Firewall Management Made Easy with SolarWinds Firewall Security Manager
2. **Video**: Firewall Rule Analysis and Cleanup with Firewall Security Manager
3. **Video**: How to Audit Firewall Security with SolarWinds Firewall Security Manager