

Effective Solutions for Firewall Management

Using SolarWinds Orion Network Configuration Manager with Athena FirePAC

by Chandra Reddy, Security Engineer

White Paper

Effective Solutions for Firewall Management

Using SolarWinds Orion Network Configuration Manager with Athena FirePAC

Abstract

Long hours, non-stop pressure, problem solving 99% of the time—these are the typical words used to describe the day-to-day life of network engineers and firewall administrators. Making routine changes to the infrastructure should not be an additional source of stress, but with the additional roles of monitoring and troubleshooting often times it is. The reasons for this added stress are described in this paper along with an effective solution for addressing these problems using SolarWinds Orion Network Configuration Manager (NCM) and Athena FirePAC for firewall analysis.

Introduction

To effectively manage and protect the enterprise network assets being controlled by firewall devices, it is essential that administrators have access to the latest configurations and understand what they contain. Some of the activities firewall administrators do on a regular basis are:

Allowing access

- Making a new business accessible to trading partners.
- Providing new users and new networks with access to internal/external IT assets.

Adding services

- Adding a new trading partner is being added and providing access to some specific services
- Allowing a new service to a critical host

Infrastructure changes

- Augmenting a business service additional servers
- Creating a new data center

Maintaining service availability

- Making sure that planned changes do not effect service availability or open new security holes

Blocking services

- Disallowing some services to reach a critical host
- Blocking dangerous services

Blocking access

- Blocking attacks from external hosts

These day-to-day activities are often interrupted by other tedious, manual and time consuming initiatives such as:

- Tuning the firewalls to get optimum performance
- Making sure that specific corporate policies defined by the Security officer are not violated

- Cleaning up the rules, as the rule size becomes immense and very difficult to manage
- Preparing for a firewall audit and responding to queries from a firewall auditor.
- Getting ready for a PCI audit!
- Migrating a firewall configuration to a different type of firewall

Why is this so difficult?

Enterprise networks with an already complex web of inter-connections will inevitably grow more complex because of the need to add rules in order to provide network access and protect against attacks. Ideally, rules would be added to the firewall in an organized manner. Furthermore, rules would be organized and enhanced to suit specific business purposes. Unfortunately, that is not reality. As firewall administrators transition, rules are added in an ad hoc manner and the collection of configurations across the network eventually becomes a disordered, chaotic mess.

Manually understanding the complete effect of a rule that refers to object groups having multiple levels of membership hierarchy is not only painfully tedious, it is error prone. As the rule base increases, the number of possible combinations explode.

For example, we have observed rule bases consisting of a total of 875 rules with 125 Deny rules using almost 4000 address objects/groups and 800 service objects/groups has hundreds of thousands of combinations.

If there are many overlaps between the rules and if the rule base is sprinkled with many rules blocking dangerous services (which tends to be the case in open network environments where the desire for open policy has to be reconciled with a policy to protect certain critical assets), then it becomes virtually impossible to figure out the impact of each rule manually.

Also, in most networked environments, firewalls from multiple vendors exist to provide security defense-in-depth. However, there is no unified interface for accessing and managing these firewalls across vendors; they are often managed from separate consoles. Getting access to the configuration or pushing changes might often involve logging into the device using SSH or telnet. Without a unified view of what exists in these firewalls, one cannot easily compare rules. Even though firewalls from different vendors serve a similar purpose, their design and architecture are different.

Cisco firewalls have rulesets that can be enforced on an entering or exiting interface of the traffic. Cisco firewalls also have a "NAT control" feature that serves as an additional access control function. Juniper NetScreen firewalls enable users to apply rulesets based on the origination zone and the destination zone, where each zone contains networks that are partitioned using interfaces and routing tables. It is rare to have firewall administrators who have an understanding of all firewall types and this will introduce inconsistencies in policies deployed to the firewalls.

Configuration Management

In order to manage changes, a configuration repository system is needed. Moreover, this system needs to automatically detect, collect and store changes that happen in the device configuration. This will provide quick access to the latest or any previous configuration. What is also needed is a unified interface for the entire inventory of device configurations. The ability to review and push changes back to the device from a single place reduces the chance of undesirable changes.

As mentioned above, firewall configurations can easily grow complex. Managing firewall configurations for firewalls from multiple vendors makes this an extreme burden. What is needed is a technical assistant, if you will, that understands the science of firewalls. This assistant is the firewall analytics tool. It completely understands all components of the firewall configuration for *meaning* and *intent* and can provide the following help to the firewall administrator:

Firewall Analytics

- An ability to search for address and service objects and object groups using object name or object content showing the complete hierarchy of the object groups involved. This aids the user in figuring out which objects can be used or modified for handling the change requests to the firewall rules. Without this ability, objects will get duplicated and will eventually need to be cleaned up as the size of the object base becomes large.
- Address and service based advanced rule search (by names or content) will aid the user in figuring out the rules that are already in place and whether these can be modified or new rules need to be added for handling the change requests to the firewall rules. Without this ability, the quick solution is to add rules—this either duplicates rules or adds new rules which increase the size of the rule base. With this analytic function, administrators can adeptly change existing rules instead.
- A report on the impact of traffic entering the firewall at a given interface, not only as ACL rules, but also as to how the NAT, VPN and routing rules are applied. With this report the firewall administrator can more easily handle changes to non-ACL rules.
- An analysis of the impact of a change before a change is pushed to the device will help in better understanding the impact on service availability as well as the exposure of any security holes. This also will result in few configuration changes and less rule “bug” fixing.

Rule Cleanup and Optimization

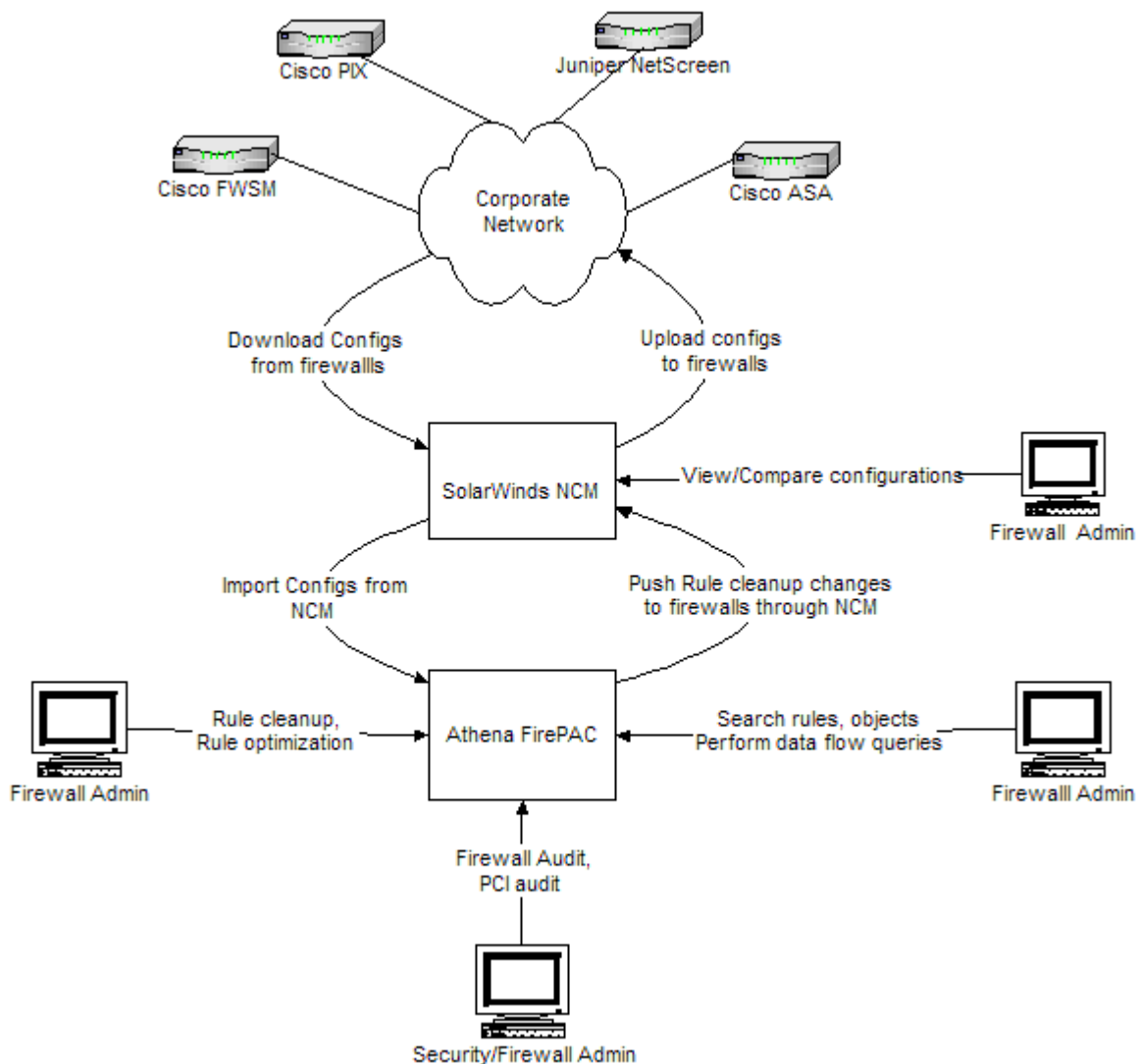
- Identification of objects that have not been used in any rules after going through the membership hierarchy is useful for cleaning up unused objects and reducing the size of the object base.
- Identification of which rules are unnecessary and hence can be cleaned up by analyzing the order of the rules and the contribution of each rule to traffic entering the firewall. This can also be used to determine which rules can be combined, reducing the size of the rule base. Rule order dependencies taking into account the rule order, rule overlap and the rule actions are also useful for reordering the rules for better firewall performance.
- Determination of unused or “stale” rules which can be removed to simplify the configuration, reduce the rule base size or keep the firewall configuration focused on current business purposes. This determination should be based on the use of the firewall log data or firewall rule usage data to identify the most used rules and unused rules. The most used rule data along with the rule order dependencies can be used for reordering rules to improve firewall performance without changing firewall behavior.

Preparing for Firewall/PCI Audit

- Automated evaluation of PCI checks as changes are happening to the firewalls would detect violations to corporate policies as changes are happening not at some later time when an audit is performed. Also simplifying PCI requirements is an ability to define customized zones for the firewalls and then define and evaluate policy checks on traffic entering and exiting the firewall through these zones.

How do SolarWinds Orion NCM and Athena FirePAC help?

SolarWinds Orion NCM is the configuration management solution and Athena FirePAC is the firewall analytic solution that firewall administrators need if they are to be safe, efficient and strategic. By using SolarWinds Orion NCM and Athena FirePAC, you can more effectively manage firewall configurations and the changes that are made to these firewall configurations.



Using SolarWinds Orion NCM, you can do the following:

- Manage the configurations of network devices such as firewalls, routers, switches, VPN concentrators and wireless access points.
- Download and upload device configurations via TELNET, SSH, or SNMP.
- Compare, version, and review downloaded configurations.
- Create detailed network inventories and reports.
- Schedule jobs to update configurations each night, execute command scripts, remotely reboot devices, and run reports.

SolarWinds Orion NCM provides a set of predefined policies that can be used to ensure device configurations conform to both internal business practices and federal regulations, such as Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability (HIPAA), and Computer Inventory of Survey Plans (CISP). Policy reports are generated by scanning configuration files and identify any discovered rule violations. For example, a Cisco policy rule triggers a violation if the configurations include a community string public by looking for “snmp-server community public”. You can add your own rules using a variety of built-in regular expression constructs that are executed on the configuration.

Using Athena FirePAC, you can completely understand what is inside your firewall, its current behavior or the impact of a change you plan to make. With Athena FirePAC, you get all the forensics needed to accomplish the following for Cisco PIX/ASA/FWSM, Check Point and Juniper NetScreen firewalls:

- Cleanup the 10 - 30% of unnecessary rules that exist in firewall rule bases.
- Find an optimized rule order that increases the firewall performance based on reordering of the most used rules taking into account rule order dependencies; so that the firewall behavior is preserved.
- Search rules across firewalls with advanced rule search, by using Address and Service object names or object content.
- Search address and service objects across firewalls, by using object names and object content.
- Find which ACL, NAT, VPN and Routing rules are applied and in what order on the traffic entering your firewall.
- Understand the change in traffic flow because of changes to the firewall configuration.
- Use predefined traffic data flow checks that helps you prepare for firewall and PCI audits.
- Define custom zones and custom data flow checks for defining and enforcing your corporate security policies.
- Schedule batch reports on a group of firewalls

Who is Athena Security?

Over 300 companies use Athena products to reduce the risks to critical hosts by eliminating the vulnerabilities, non-compliances and errors in firewall infrastructure. Athena FirePAC is an affordable, easy to use firewall analysis tool for large or small enterprises. It confirms that each firewall is configured to behave correctly. FirePAC performs safe, offline analysis on the rule base to predict how data flows through the firewall to reach critical hosts. Install it on your desktop in seconds, and generate reports that reveal exactly how your firewall is working. See more at <http://www.athensecurity.net>

Who is SolarWinds?

SolarWinds provides powerful, simple and affordable network management software and network monitoring software to more than 85,000 customers worldwide -- from Fortune 500 enterprises to small businesses. Focused on the real-world needs of network professionals, SolarWinds products are downloadable, easy to use and maintain, and provide the power, scale, and flexibility needed to manage today's complex network environments. SolarWinds' growing online community, _thwack, is a gathering-place for problem-solving, technology-sharing, and participating in product development for all of SolarWinds' products. Learn more today at <http://www.solarwinds.com>

References

Athena Security completes integration with SolarWinds Orion Network Configuration Manager
<http://www.athensecurity.net/athenasolarwinds.html>

Athena Security website <http://www.athensecurity.net>

SolarWinds website <http://www.solarwinds.com>