SOLARWINDS WHITEPAPER

Firewall Management with SolarWinds Network Configuration Manager & Athena FirePAC

Follow SolarWinds:

solarwinds

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 such as making a new business accessible to trading partners
- Providing new users and new networks with access to internal/external IT assets.
- Adding services
- Allowing a new service to a critical host
- Infrastructure changes
- Maintaining service availability
- Blocking services
- Blocking access

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

Firewall Management Challenges

Network complexity has evolved rapidly over the last 10 years. Today's networks consist of many different network devices (firewalls, routers, switches, etc…) from many different vendors, with many access mechanisms into the network (wireless, mobile devices, email, portals for partners and customers, FTP servers, and peer-to-peer applications and communications) all introducing security risk to the enterprise.

Firewalls continue to be one of the cornerstones of network security and, as such, have become more sophisticated and complicated to operate and manage resulting in a number of challenges for the IT professional.

- Organizing the rule base to support the business while maintaining security policy

- Understanding the impact of changes
- Managing a multi-vendor environment

Dynamically changing networks, evolving needs of the business, and emerging external threats all drive the need to add or change rules. Ideally, these rules would be added to the firewall in an organized manner and enhanced to suit specific business purposes. Unfortunately, that is not reality. 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 effect of rule additions, changes, or disablement is not only painfully tedious, it is error prone. As the rule base increases, the number of possible combinations explodes. 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 then it becomes virtually impossible to figure out the impact of each rule manually.

In most networked environments, firewalls from multiple vendors exist to provide security defense-in-depth. Even though firewalls from different vendors serve a similar purpose, their design and architecture are different. Cisco firewalls, for example, have rule sets that can be enforced on an entering or exiting interface of the traffic as well as a "NAT control" feature that serves as an additional access control function while Juniper NetScreen firewalls enable users to apply rule sets based on the origination zone and the destination zone. 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 and without a unified view of what exists in these firewalls, one cannot easily compare rules. Additionally, there is no unified interface for accessing and managing these firewalls across vendors; they are often managed from separate consoles and getting access to the configuration or pushing changes might often involve logging into the device using SSH or telnet.

Firewall Analytics

As mentioned above, firewall configurations can easily grow complex. Managing firewall configurations for 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 Profile - scans your inventory for high-risk firewalls and cleanup and report on before and after health and performance

Search - 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 that increase the size of the rule base. With this analytic function, administrators can adeptly change existing rules instead.

Rule/Object Cleanup & Optimization – by analyzing firewall configs and logs, the user can isolate redundant, covered, and unused rules to increase performance and rulebase efficiency through rule analysis, usage analysis, and rule re-ordering. Through rule analysis, the user can maximize the opportunity for cleanup by catching every possible case of redundancy. Redundancies represent errors in the configuration that play no role in the firewall's behavior and can be immediately removed. Usage analysis looks at the rule and object usage based on hit counts and traffic data for a given period of time.

This is useful to remove temporary rules and rules that are no longer needed. Additional improvements can be achieved through rule re-ordering that takes into account all rule dependencies so that the firewall's behavior is not adversely impacted.

Security Audit - Automated evaluation of security and compliance policies as changes are happening to the firewalls to detect violations in real-time.

Change Impact - 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.

Historical Rule Tracking – maintain a history of the business justification for each firewall rule as well as tracking the rules that have changed over time.

The Role of Configuration Management

Firewall analytics are only one of the tools required to ensure optimal performance and health. Automating the process of configuration changes, change detection, device management, and policy reporting through a Network Change and Configuration Management (NCCM) tool will greatly simplify the firewall configuration process and reduce the risk of human error.

Change Management – simultaneously modify configurations across multi-vendor devices without the need for complex scripting and CLI commands.

Real-time Alerts – when configuration changes occur to protect against unauthorized unscheduled, or erroneous changes.

Policy Violation Detection & Reporting – ensures that firewall configurations meet federal regulations and corporate policies.

Automatic Config Backups – automatically backup firewall device configurations on a regular basis

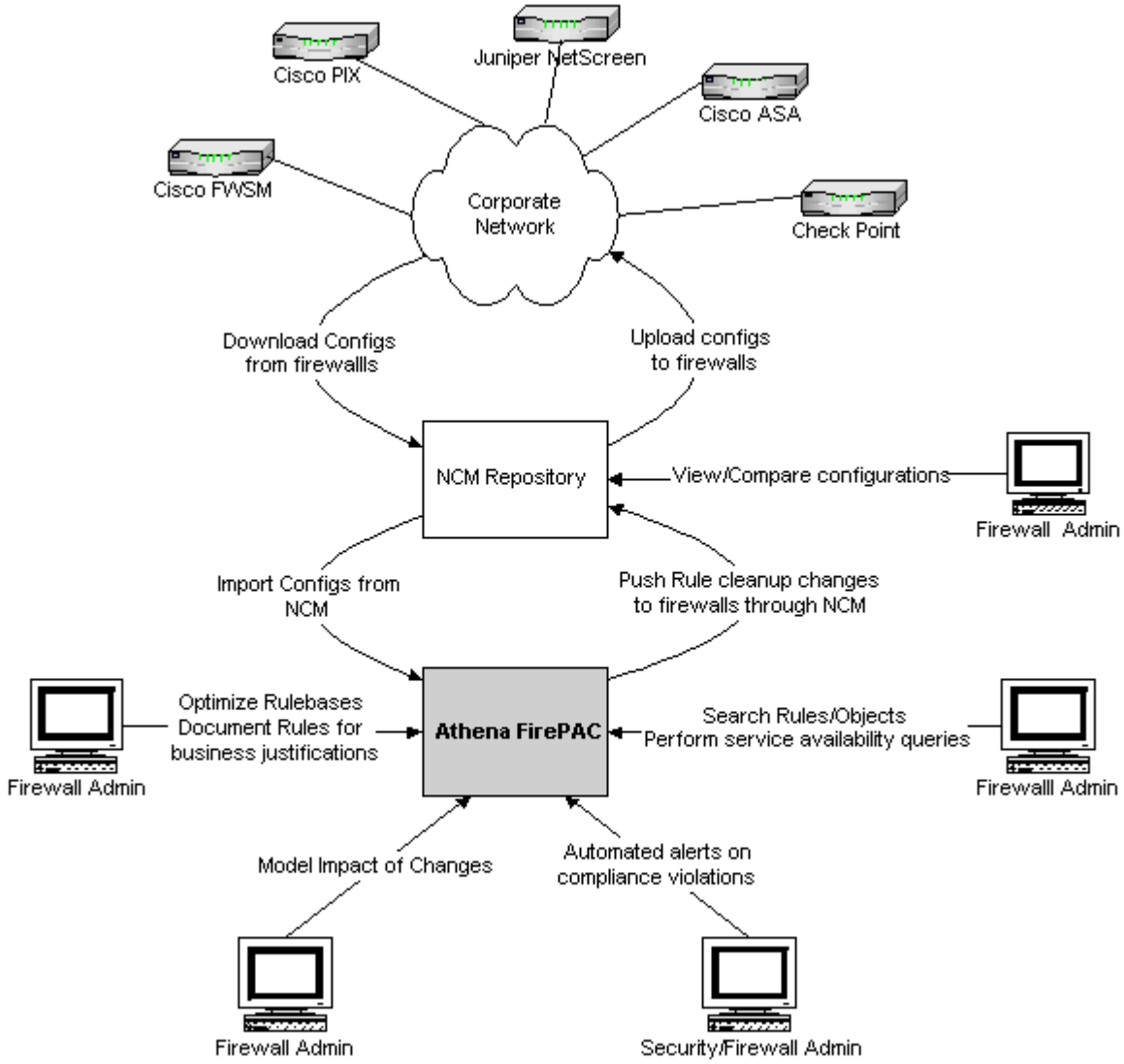
Config Comparisons & Rollback – identify and repair unauthorized and failed configuration changes with a side-by-side comparison

User Roles, Permissions, and Activity Tracking – protects against unauthorized firewall config changes

Unified Interface – across all firewalls in the network eliminates the need for device specific utilities

How do SolarWinds Network Configuration Manager and Athena FirePAC help?

SolarWinds Network Configuration Manager (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 NCM and Athena FirePAC, you can more effectively manage firewall configurations and the changes that are made to these firewall configurations.



SolarWinds Network Configuration Manager delivers affordable, easy-to-use network change and configuration through a full-featured, web based console that offers point-and-click simplicity and easy access to firewall configuration data. NCM simplifies managing network configurations by continuously monitoring device configurations and providing immediate notification of configuration changes to help resolve problems before they impact users.

- Simultaneously modify configurations across many multi-vendor firewalls through automated bulk-change management
- Receive real-time network change notifications when firewall configurations change
- Detect firewall config policy violations to ensure compliance with federal and corporate requirements
- Compare configurations and restore to a previously known state
- Automatically backup firewall configurations on a scheduled basis

- Inventory network devices and create detailed reports.
- Schedule jobs to update configurations each night, execute command scripts, remotely reboot devices, and run reports.

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.

FirePAC offers a virtual environment, disconnected from the actual network, to accurately simulate the behavior of data packets on the network.

The system can determine whether a change is required, and if so, it identifies the specific devices on the network and the precise rules that require to be changed.

Athena FirePAC is available as an integrated firewall management solution with SolarWinds NCM.

Before a change is deployed to production, you can model the impact on traffic flow without injecting any data into the network. Once a change looks satisfactory, automated scripts can be pushed through Orion NCM.

For maintaining compliance, you can update the business justification for modified and added rules, and track a rule throughout its lifecyle.

FirePAC offers powerful filtering capabilities for isolating policies by rule and object content.

Automated scripts can be used to cleanup the 10 - 30% of unnecessary rules that exist in most firewall rulebases.

Apply a recommended optimized rule order that increases firewall performance while keeping firewall behavior preserved.

Who is Athena Security?

Athena provides software solutions to improve compliance and reduce the cost of managing enterprise firewalls. With a global customer base of several hundred customers and thousands of users across a suite of products, Athena specializes in network-aware policy assessment and operational support tools for firewall and security engineers. See more at http://www.athenasecurity.net

Who is SolarWinds?

SolarWinds provides powerful, simple and affordable network management software and network monitoring software to more than 95,000 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. Download a free, fully-functional 30-day trial of SolarWinds Network Configuration Manager.

References

Athena Security completes integration with SolarWinds Network Configuration Manager (http://www.athenasecurity.net/athenasolarwinds.html)

Athena Security website http://www.athenasecurity.net

SolarWinds website http://www.solarwinds.com