CLEANING UP YOUR FIREWALL CLUTTER

HOW TO OPTIMIZE FIREWALL POLICIES AND IMPROVE PRODUCTIVITY WITH ALGOSEC

An AlgoSec Whitepaper

The Need to Reduce Complexity of Firewall Policies

Firewalls continue to be the first line of defense, handling vast amounts of traffic across the enterprise. On the perimeter alone, firewalls filter millions of packets daily. In today's dynamic business environment, firewall policies are constantly being changed and modified. Firewall administration teams in large organizations often process dozens of rule additions and changes daily. Add in Next-Generation Firewalls, which deliver newfound policy granularity at the application and user level, and firewall configurations continue to dramatically grow in complexity over time.

Complex firewall configurations negatively impact IT in several ways:

- **Lengthy, costly and complex audits** - The ability to complete a manual audit of the firewall today has become nearly impossible.
- **Increased Risk** – Complex and bloated rulesets make it more difficult to understand the impact of the security policy, and identify risky firewall rules.
- **Performance Degradation** – Firewalls sequentially sift through endless rulesets to identify the rule that matches every packet, slowing down the network and requiring organizations to invest in costly hardware upgrades.

> *"For one firewall, we were able to remove 30,000 rules. Now we can use those assets more optimally. A firewall with 500,000 rules isn't going to cope as well as one with 100,000 rules. By optimizing our devices, AlgoSec saves us money in the long term."* - Marc Silver, Security Manager, Discovery SA

AlgoSec automatically analyzes firewall rulesets, logs and routing information to provide organizations with actionable recommendations for cleaning and optimizing network security policies.

Uncluttering Firewall Policies

AlgoSec helps organizations cleanup their firewall policies, easing the network administrator's job while boosting performance and eliminating security holes. AlgoSec optimizes firewall policies by identifying:

- **Unused rules**: Ideal candidates for removal, these rules have not matched any packet during a specified time (configurable by AlgoSec). Often the application has been decommissioned or the server has been relocated to a different address. AlgoSec looks at the firewall logs and compares the actual traffic to the rules in the policy.
- **Covered or duplicated rules:** Rules that can never match traffic, and thus can never be used, because a prior rule or a combination of earlier rules prevents traffic from ever hitting them. Covered and duplicated rules decrease firewall performance.
- **Redundant special case rules**: Rules that are covered by a subsequent rule, and can be removed without altering the security policy. The earlier rule is a "special case" of a succeeding rule.
- **Disabled rules**: Rules that are marked "disabled" and are not in operation are ideal for removal, unless the administrator keeps them for occasional use or for historical record.

- **Time-inactive rules**: Rules that were active for a specified time in the past and that time expired. Retaining such rules may create security holes.
- **Rules with a time clause**: In addition to time-inactive rules, AlgoSec also lists all of the rules with a time clause, whether active or not. Showing these rules will raise the administrators awareness of time-dependent rules that are about to become inactive.
- **Rules without logging:** Rules that are defined not to generate logs (i.e. highly used rules that control low risk traffic) because they consume a large amount of disk space. Listing the rules without logs will help the administrator verify that the lack of auditing for these rules is not contradictory to corporate policy or regulatory compliance.
- **Least used rules and most used rules**: Rules that matched the smallest number of packets or the largest number over a predefined and configurable period of time. Most used rules may be repositioned higher up in the configuration and least used rules in lower down to improve firewall performance. AlgoSec also shows the last date when each rule was used, which may also help with reordering and cleanup decisions.
- **Rules with empty comments or comments that do not comply with corporate security policy**: The firewall comments allow the administrator to add free text that is usually used to describe the rule usage, the reason for creating the rule, the ticket number in the help desk trouble-ticketing application and any other information associated with the rule – to ensure compliance with corporate policy or regulatory compliance. AlgoSec reports on tickets without comments and tickets with non-compliant comments.

In addition to analyzing rules, AlgoSec also analyzes objects. Firewall objects contain lists of IP addresses, or IP address ranges, and are a convenient way for a firewall administrator to relate to names rather than numbers. When AlgoSec performs its analysis it translates the names to the list of IP addresses and matches rules and packets to the addresses associated with them. AlgoSec analyzes the following for objects:

- **Unattached objects**: Objects that are not attached to any rule. AlgoSec also displays unattached global objects.
- **Empty objects**: Objects that do not contain any IP address or address range.
- **Duplicate objects**: Objects that already exist but are recreated contributing to the policy “bloat”.
- **Unused objects**: Objects whose address ranges do not match any packet during a specified time. AlgoSec also displays unused global objects.
- **Unused objects within rules**: Objects within rules that were not used recently, and can be removed from the particular rules. This allows more granular rule optimization and cleanup to reduce the existing rule base to the traffic actually used.

By removing the unnecessary rules and objects that were detected by AlgoSec, the complexity of the firewall policy is reduced. This improves management and performance and removes potential security holes.

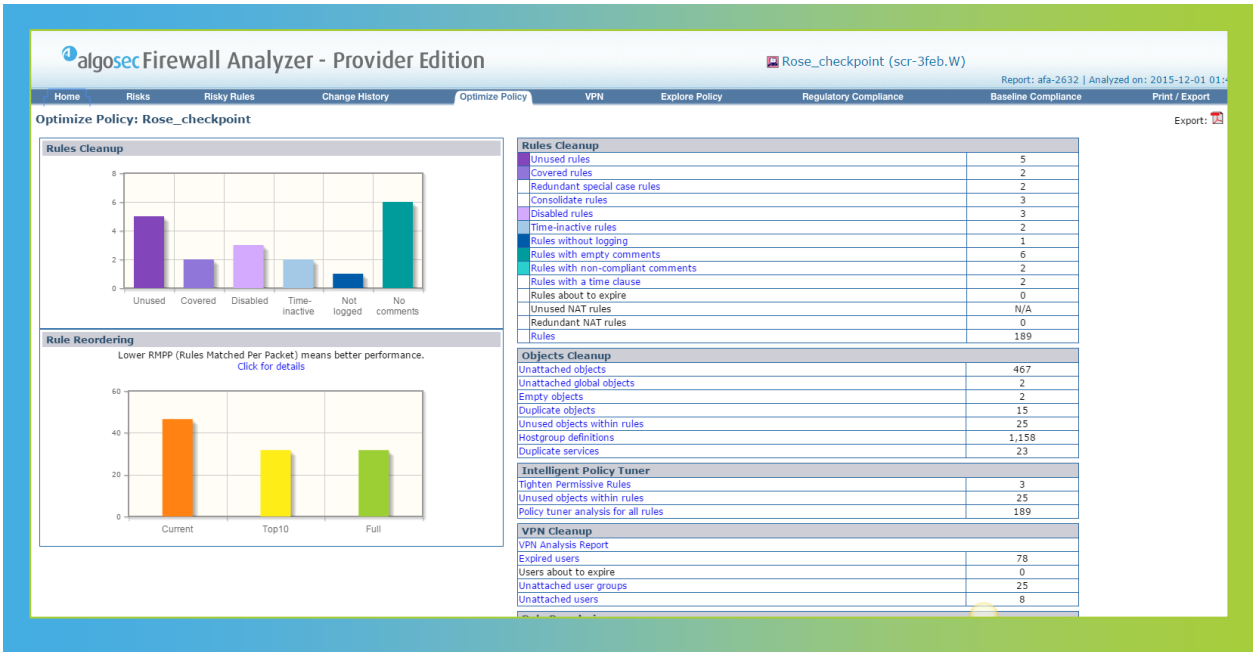

Figure 1: “Optimize Policy” summary page example

Don’t Forget About Optimizing VPN Configurations

A common misperception is that a virtual private network (VPN) is secure, but that may not be the case. VPN configurations can also become bloated with outdated policies and should be reviewed as candidates for cleanup.

For example, it is possible that the following items may be removed without affecting the firewall configuration:

- Expired users: Users that are not active and cannot login.
- Unattached users: Users which are not associated with any rules.
- Unattached user group: User groups which are not associated with any rule.

Intelligent Rule Reordering Gives Firewall Performance a Boost

AlgoSec provides recommendations for optimizing a rule's location in order to improve firewall performance while taking the firewall's actions into account and ensuring that policy decisions and the filtering logic are preserved. The recommendations offer the firewall administrator a new position for each rule. The administrator can decide whether to move the rule to its exact new recommended position or to another position in the same area, while keeping blocks of rules intact.

Rule Reordering		
	RMPP	Improvement
Top 10 Optimizations	31.70	31%
Full Optimization	31.70	31%
Current Rule Order	46.56	

Rule Usage Statistics	
Unused rules	5
Unused objects within rules	25
Least used rules	5
Most used rules	5
All rule usage (count, last date)	189
All NAT rule usage (count, last date)	N/A
Policy tuner analysis for all rules	189

Figure 2: "Optimize Policy" rule reordering optimization summary example

AlgoSec also offers a top-10 list of rules to optimize the reordering process. This list is comprised of the 10 rule-relocation recommendations which provide the greatest improvement. In many cases a handful of rule relocations are sufficient to significantly increase performance. Sometimes moving only a single rule which is not among the top used, but is located low in the firewall policy, will provide the greatest value.

Tightening Permissive Firewall Policies for Stronger Security

The complexity of defining the firewall policy may often result in many overly permissive ruleswhich grant access that is wider than required by the business. Effectively tightening these rules greatly improves security and helps prepare new firewalls for initial deployment. When powered AlgoSec's automated tuning capability an organization is able to proactively configure rules that immediately result in stronger security – without impacting business requirements. The tuning process aims to accomplish three objectives for each rule or object affected by a rule:

1. **Eliminating the presence of unused objects.** AlgoSec identifies rules with objects that are unused and removes them from the rules for stronger security.
2. **Controlling Sparse Traffic.** AlgoSec analyzes the firewall policy against actual traffic logs, identifies excessively permissive rules, such as ANY Service, that allow traffic which does not flow through the network, and offers recommendations to tighten such rules.
3. **Strengthen Security in Newly-Deployed Firewalls.** Often firewalls are deployed with default configurations of fairly "wide" (permissive) policy rules. AlgoSec tightens rules to specific requirements of the target network.

RULE	NAME	SOURCE	DESTINATION	SERVICE	ACTION	COMMENT	COUNT	LAST DATE	PERCENTAGE
49		GP_Dthomson	Shiva	* Any	accept	FireFlow #345: MicroSoft Windows Update	10,697,109,115	2015-02-14	65.896%
14		GP_NW_SLI_LAN	GP_PC_ICN_besimail	TCP imap TCP smtp TCP besimail-mgt	accept	imap required to besimail servers FireFlow #361: Besimail-mgt added DT 07/02/2007	1,036,448,772	2015-02-13	6.385%
3 (Global)		rose_checkpoint SCR_vscan_EXT SCR_vscan_INT	SCR_vscan_INT SCR_vscan_EXT rose_checkpoint	* Any	accept	FireFlow #69: eSafe/WebSense machine	17,657,215	2015-02-11	0.109%

Showing 1 to 3 of 3 entries

Figure 4: Identify overly permissive rules based on usage patterns

Conclusion

Firewall policy complexity and bloating add significant burden to firewall administrators' productivity and to the performance of the firewall, but there are effective ways to manage these challenges. By leveraging intelligent analysis of logs and rulesets, firewall administrators can automate policy optimization to reduce complexity, improve security and achieve significant and measurable performance improvements.

AlgoSec enables administrators to optimize firewall operations and improve their productivity by identifying unused and redundant rules, tightening overly permissive rules, and reordering rules for optimal performance.

About AlgoSec

AlgoSec simplifies, automates and orchestrates security policy management to enable enterprise organizations and service providers to manage security at the speed of business. Over 1,500 of the world's leading organizations, including 15 of the Fortune 50, rely on AlgoSec to optimize the network security policy throughout its lifecycle, to accelerate application delivery while ensuring security and compliance. AlgoSec is committed to the success of each and every customer, and provides the industry's only money-back guarantee.

For more information visit http://www.AlgoSec.com or visit our blog.

algosec

Global Headquarters
65 Challenger Road,
Suite 320
Ridgefield Park
NJ 07660, USA
+1-888-358-3696

EMEA Headquarters
80 Coleman Street
London EC2R 5 BJ
United Kingdom
Tel: +44 207-099-7545

APAC Headquarters
10 Anson Road, #14-06
International Plaza
Singapore 079903
+65-3158-2120

AlgoSec.com