

Business drives complexity in device configurations. FireMon's policy optimization helps you avoid unnecessary complexity, easing administration and benefiting security.

Security device configurations change constantly. Changing business requirements demand accurate and prompt adjustment to the devices that protect an enterprise. Making configuration changes to these devices can be difficult when balancing the need for rapid and correct security protection with the long-term manageability of the device. Sometimes, new firewall rules are added to a policy when an existing rule could be modified to meet the requirement. Other rules become obsolete but remain in the security policy. As a result, the policy grows larger and needlessly complex.

Security administrators strive for effective, manageable security policies, but frequent changes may lead to a less-than-ideal rule base. Often times, creating a new rule meets a business-driven change more simply than sifting through a rule base for one rule to modify. And security administrators don't have the countless hours necessary to comb through logs to find rules that are no longer in service and delete them. Additional business pressure to recover swiftly from emergencies like outages and device failures makes rule base optimization even less feasible.

Also, companies are responding to regulatory requirements that require rule bases to be audited regularly. For example, many retailers and financial institutions must adhere to the guidelines described in the Payment Card Industry (PCI) Security Data Standard, specifically, requirement 1.1.8 that calls for the periodic review of firewall and router rule sets. Consequently, security administrators struggle to find an appropriate, auditable configuration while they manage time-sensitive issues and changes.

FireMon can help security administrators understand their security device configurations and ensure that the configurations are kept as concise as possible. By utilizing FireMon's rule usage analysis tool and in-context policy behavior tests, administrators can acquire the information they need, and confidently make the changes that keep their enterprises secure.

Understand Your Policy

Analyze Current Usage

Identify and report on which of your firewall rules are most-used, least-used and unused.

Reduce Complexity

Understand when new rules are necessary and when old rules can be removed.

Evaluate in Pre-Deployment Phase

Evaluate different scenarios for how to handle new functionality requests.

Troubleshoot Connectivity Issues

Determine exactly how the security device is reacting to traffic without searching through logs.

Enhance Firewall Performance

Understand how reordering your rules can improve the performance of your devices.

Secure Passage

www.securepassage.com

Main: 816.421.1901

Fax: 816.421.1938

info@securepassage.com

1627 Main St. Suite 200
Kansas City, MO 64108
United States of America

How Can FireMon Help?

Analyze Traffic Behavior

Quickly and easily determine how a firewall policy will behave with FireMon's policy test feature. Define a virtual IP packet with source, destination and protocol information. FireMon will evaluate the selected policy and return the exact rule that is acting on that traffic, including what action is being taken.

Policy Test can:

- ▶ Evaluate in-context how a policy behaves under user-defined conditions. It can also evaluate multiple policies simultaneously.
- ▶ Run tests on policies before deployment, while active or once archived.
- ▶ Test different scenarios without impacting production systems.
- ▶ Show results that include all rules that would respond to the defined traffic.
- ▶ Evaluate firewall policies in order to:
 - ▲ Identify vulnerabilities and troubleshoot connection problems.
 - ▲ Identify duplicate or redundant rules.
 - ▲ Determine if and where a new rule is needed.
 - ▲ Avoid including unnecessary rules.

Rule that will take effect for this traffic is:

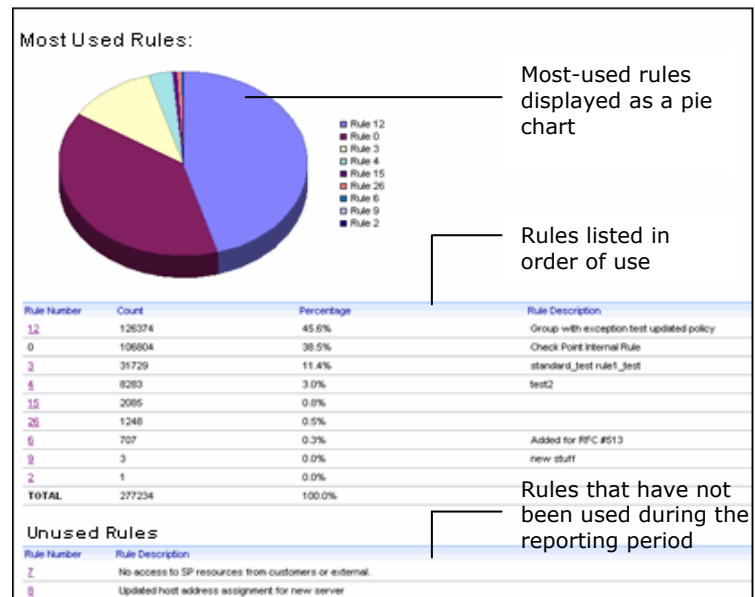
NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME
5	Nortel_Net	SQLServer	*	Any	sqlnet2	accept	Log	Any

Analyze Policy Usage

FireMon's rule usage analysis report highlights the most-used, least-used, and unused policy rules. Discover which rules are acting on a lot of traffic and should be reordered to improve performance. Also, identify rules that are unessential and remove them from the rule base.

Rule Usage Analysis can:

- ▶ Show which rules are used most-often and least-often.
- ▶ Show rule use frequency.
- ▶ List unused rules.
- ▶ List rules that are not being logged.



For more information on FireMon or to download a free 30-day trial, please visit www.securepassage.com.