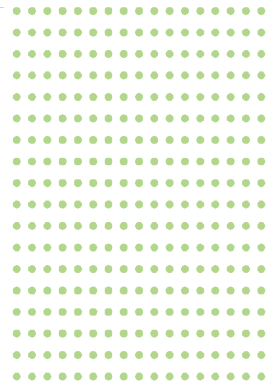


Tufin SecureTrack™

Firewall Operations Management

January 2010

tufin



www.tufin.com

Table of Contents

Introduction	3
Comprehensive View of Firewall Policy.....	3
Configuration Change Management	4
Security Policy Optimization and Cleanup	5
Risk Management.....	5
Corporate Auditing and Compliance.....	6
Automatic Security Policy Generation.....	7
Compliance with Best Practices.....	7
Scalable, Distributed Architecture	8
Firewall Operations Management: The Automated Solution.....	8

Introduction

Managing network security for a large organization has become a highly complex operation involving dozens or even hundreds of firewalls. Multiple sites and teams, different hardware and software vendors – all of these factors make it extremely difficult to ensure security in a consistent, efficient way. At the same time, corporate security policies have become more rigorous, and companies need to comply with a growing body of industry and government regulations.

To make sure that security standards are being met, most organizations rely on periodic audits – a process involving days of manual, painstaking effort. In addition to the tremendous investment of time and resources, relying on audits is a reactive approach to network security that can leave threats undetected for months at a time.

Today's security operations teams urgently need a management solution that can proactively improve network security while automating labor-intensive day-to-day tasks. In practical terms, firewall operations teams need:

- Central management starting with a top-down view of all firewalls in the organization.
- Change management to ensure that every change to security policy is accountable and in accordance with corporate standards.
- Policy optimization and cleanup to improve firewall performance and reduce hardware costs.
- Risk analysis and business continuity management to proactively evaluate the impact of every configuration change – before it is implemented.
- Automated security audits to efficiently comply with corporate policies as well as industry and government regulations.
- Automatic security policy generation to enable rapid deployment of new firewalls without disrupting business continuity or resorting to permissive rules.
- Alignment with best practices from vendors and security industry veterans.

Tufin SecureTrack™ enables security operations teams to efficiently align operations with organizational objectives. With a powerful set of central management tools, SecureTrack tackles the practical challenges that operations teams face every day. This paper takes a closer look at each of the key requirements in firewall operations management and explains how SecureTrack can help your company to reduce risk, lower costs, and achieve its strategic security objectives.

Comprehensive View of Firewall Policy

Large enterprises currently manage dozens, if not hundreds, of individual firewalls. Each firewall has its own policy - a complex set of rules defining the access privileges and restrictions for specific users and services. Today, administrators lack a unified top-down view of all of their firewall policies from various vendors, and need to individually monitor each piece of the puzzle.

Tufin SecureTrack provides a convenient, top-down view of all firewall rule bases in the organization, even if they are from multiple vendors. You can view the current configuration as well as historical views and snapshots. Each rule base is displayed

using the vendor's native layout and conventions. SecureTrack makes it simple to visually compare and review firewalls. For example, you can analyze a side-by-side view of the same firewall at two different points in time, and you can compare the settings of different firewalls in a variety of views and reports.

With an accessible web interface, SecureTrack enables you to centrally manage alerts and notifications and generate reports for all of your firewalls, whether you are on or off-site. Since it is easy to learn and use, within minutes you can integrate SecureTrack into your network environment and start real-time monitoring of your infrastructure.

In addition to the list of vendors currently supported by SecureTrack, the Tufin Open Platform (TOP) enables enterprises and integrators to easily extend the platform and support additional vendors and infrastructure components through a simple plugin.

Configuration Change Management

Organizations are constantly in motion. So implementing a corporate security policy is not a one-shot deal. Every day, configuration changes are made in response to user requests for network access, security threats and changes to the network structure. Monitoring, tracking and analyzing these configuration changes is probably the biggest challenge facing firewall administrators today. And the problem is not limited to rule bases. Changes to the configuration and performance of the firewall operating system or firmware also directly impact security and business continuity, yet they are difficult to track with conventional methods.

Tufin SecureTrack continuously monitors and keeps track of every firewall configuration change including changes to rules and network objects such as hosts and services. Comprehensive change reports include all firewalls and vendors, using the vendor's native conventions – for example, field names and colors. SecureTrack offers a variety of customizable change reports as well as comparisons of different firewalls, or different historical snapshots. Reports can be sliced by firewall, by rule, by object, or by the type of change.

Full accountability is assured since each change is stored along with the administrator's name, the time, and the server where the change originated. SecureTrack makes it possible to determine who made a change with a simple query, rather than searching through numerous log files for the needle in the haystack.

SecureTrack also integrates with leading ticketing systems so that changes can be tracked from the original request through approvals to implementation. Each change in a SecureTrack report includes a link to the relevant ticket so that you can automatically launch the relevant ticket for more information.

Using real-time alerts, SecureTrack sends e-mail to designated administrators in response to every change that may conflict with corporate security policy. Rather than wait for the next audit, SecureTrack empowers you to proactively prevent security risks before they actually arise. Alerts are also useful for ongoing management – even when you are off site, SecureTrack alerts can inform you of any or all changes via e-mail.

Security Policy Optimization and Cleanup

As thousands of tickets are processed by the firewall operations team, and organizational security objectives evolve over time, the underlying rule bases containing the firewall policies become very large, intricate and complex. In fact, many of the rules and objects in a typical firewall rule base are obsolete. These unused rules represent a potential security hole and should be eliminated. Yet firewall administrators do not have an easy way of identifying these rules with standard administration tools.

In addition to security risks, a poorly maintained rule base can have a major impact on performance. The entire rule base is parsed from top to bottom with every network connection, and as the rule base grows, hardware requirements also increase.

SecureTrack analyzes the actual usage of firewall rules and labels each rule as heavily used, moderately used, or unused. SecureTrack also analyzes object usage within each rule, indicating specific network objects and services that are no longer in use. It is advisable to review every unused rule and object, and remove those that are not necessary and may represent a security risk.

To improve firewall performance, SecureTrack makes recommendations regarding the position of specific rules – placing the heavily used rules at the top of the rule base and moving the least-used rules to the bottom. SecureTrack also indicates rule shadowing – places where rules overlap, or effectively “hide” other rules – so that you can re-position rules intelligently.

Risk Management

The implications of a firewall configuration error can be severe – from a security breach to network downtime, or even a network service interruption. Therefore, it is important to analyze the impact of every change before it is implemented in the production environment. The same is true for the firewall gateway operating system, where routine system maintenance can expose vulnerabilities or even disrupt business.

In addition, security managers must be able to assess risk and vulnerability at any given time – for all relevant network security devices. The challenge is greatest in distributed organizations with multiple teams. Inevitably, different teams develop their own standards and working methodologies. To ensure that everybody is successfully implementing security guidelines, organizations need to implement automated solutions that can evaluate risk and compliance at all times.

To manage risk and ensure business continuity, SecureTrack uses a multi-step approach. All of these capabilities are firewall-vendor agnostic and implemented transparently in heterogeneous firewall environments:

- Security administrators define the organization’s security compliance policy for mission-critical and risky services within SecureTrack. SecureTrack automatically compares every change that is made to the firewall configuration and sends out a real-time alert if the organizational compliance policy is violated.
- Before implementing a change, administrators can use SecureTrack’s Policy

Analysis to simulate the change on the rule base and identify possible conflicts or violations. This proactive risk analysis tool can save hours of painstaking, manual rule base review.

- For administrators and managers alike, the automated Risk Management Report instantly evaluates the current level of risk and displays your Security Score along with scoring on a prioritized list of risk factors. The report can be run at the organizational level or per gateway, and indicates risk trends in addition to the current state. To determine the Security Score, the report uses your compliance policies as well as a group of predefined risk factors culled from leading industry standards. You can set your own priorities and customize the report to exclude specific policies, risk factors or even rules that cause false-positive violations.

Corporate Auditing and Compliance

Companies now understand the business impact of network security and are demanding a high level of transparency and accountability from network operations teams. In addition, more and more companies need to conform to government and industry standards such as PCI-DSS and SOX.

To meet these increasingly rigorous standards, companies need the ability to efficiently perform periodic audits. Owing to the size and dynamic nature of firewall rule bases, it is extremely time-consuming to do this manually, even for an expert. Companies need an automated audit process that can be configured to meet the specific requirements of both corporate and regulatory standards.

To hold individuals accountable for their actions, companies need to maintain an accurate audit trail of all security policy and operating system changes. It is preferable that the audit trail come from an objective third party or automatic logging tool. Furthermore, companies need to enforce and demonstrate a separation of duties designed to ensure that all changes are approved and monitored properly.

SecureTrack provides automatic audit reports that test current firewall configuration against your corporate security policy as well as a configurable checklist of standards. Along with a list of violations, Tufin's audit reports provide information on how to resolve or mitigate the infraction. Specialized reports, such as the PCI-DSS Audit, are already designed according to the requirements of the industry standard. Audit reports can be scheduled for automatic, periodic execution and mailed to all relevant security officers.

SecureTrack supports periodic audits with continuous change tracking and a comprehensive audit trail that provides full accountability and demonstrates implementation of a separation of duties. Change reports can be generated at any time to show the configuration changes that were made both to the rule base and to the firewall operating system.

Since SecureTrack issues real-time alerts any time a configuration change violates corporate policy, all security threats can be addressed immediately. This transforms the periodic audit into the reporting process it is meant to be, with transparency and accountability being its primary aims.

Automatic Security Policy Generation

Network security teams are frequently asked to secure unrestricted network segments – for example, between branch offices or merged companies – or to tighten up permissive firewall policies. This is very difficult to achieve without accidentally disrupting critical business services. Through labor-intensive manual log inspection, administrators try to identify legitimate business traffic and create a rule set that will meet both security and business objectives. But given the complexity of network traffic today, this process is not only tedious and error-prone – it is also not very effective. As a result, companies often deploy firewalls with permissive ANY rules that do little to fulfill their security objectives. Network security teams need an automatic solution for defining new firewall policies and tightening up permissive ones that can reduce deployment times and ensure business continuity.

With SecureTrack’s Automatic Policy Generator™ (APG), managers can automatically generate a new, robust firewall policy based on a thorough analysis of current network traffic. APG creates a rule base that is not too permissive, is optimized for high performance and organized for easy management and maintenance. Fast and efficient, APG processes thousands of logs to create a new rule base within minutes. By repeating the process several times and adjusting a variety of parameters, managers can define a highly optimized firewall policy in hours, rather than in weeks or months.

APG also provides security professionals with a powerful new tool for tightening existing firewalls, re-building complex, heavy rule sets, and analyzing the rule bases of firewalls inherited from other organizations.

APG is powered by patent-pending Permissive Rule Analysis technology, which proactively tightens the security posture of a firewall by rewriting rules that grant too much access. For example:

Source	Destination	Service
WebServers	AppServers	ANY
When the Service field contains ANY between two groups of servers		

Usually, these types of permissive rules are put into place in order to avoid interruptions to critical business services. APG takes exactly the opposite approach. By analyzing traffic logs, APG builds a rule base from the bottom up, allowing precisely the object/service sets that are in actual business use.

Compliance with Best Practices

Over the years, security best practices have evolved that enable organizations to manage their security infrastructure more effectively. Given the variety of devices – different vendors, versions and administration tools – it is difficult to enforce industry best practices throughout the organization. Managers need tools that define best practices and are able to identify non-conformance for the full range of security

devices.

In SecureTrack, Tufin has gathered a long list of best practices derived from firewall vendors, industry experts and years of practical experience. The configurable Best Practices Audit report instantly checks compliance with practices such as log tracking (rules that are untracked or unlogged), permissive rules (that allow traffic from too many IP addresses), network object name patterns, firewall OS settings, and more.

Scalable, Distributed Architecture

At large organizations, firewalls and related network devices are frequently distributed among multiple sites, even in different countries, making centralized management a challenge.

Tufin SecureTrack features a robust distributed architecture that is suitable for wide area networks. For large, distributed organizations, collectors are deployed at each site and forward data to a central database for administration. SecureTrack is designed to overcome connection downtime between components and ensure a continuous, centralized management environment.

Firewall Operations Management: The Automated Solution

As firewall infrastructure grows more distributed and diverse, operations teams need central management solutions to ensure a reliable level of accuracy and consistency. Tufin's SecureTrack enables operations teams to monitor, track and report changes for all firewalls in the organization. SecureTrack features all of the tools that operations teams need to slash routine, manual tasks and ensure network security every day:

- **Change tracking and analysis:** SecureTrack monitors firewall policy changes, reports them in real-time and maintains a comprehensive, accurate audit trail for full accountability.
- **Security infrastructure optimization:** Analysis and clean-up of complex rule bases and objects to eliminate potential security breaches and improve performance.
- **Risk management:** Assessment of Security Score and risk trends based on conformance to compliance policies and industry-standard risk factors.
- **Auditing and regulatory compliance:** Automated audit reports to demonstrate compliance with corporate policy and regulatory standards including PCI-DSS, SOX, HIPAA, ISO 17799 and Basel II.
- **Multi-vendor visual monitoring:** Intuitive, graphical views of policies, rule bases and configuration changes for the largest variety of vendors and network devices.
- **Comprehensive security policy analysis:** In-depth analysis of organizational security policy implementation on a wide range of security devices.

- **Automatic firewall policy generation:** Creating a new firewall policy based on an analysis of actual network traffic and elimination of permissive rules.
- **Firewall OS Monitoring:** Monitoring of critical firewall operating system components and server performance indicators to prevent service interruptions and enable effective auditing.
- **Multi-vendor best practice audit:** Ability to compare current configuration with best practice recommendations derived from extensive industry experience.
- **Scalability and customization:** Distributed architecture supports unlimited firewalls, rules and network objects in multiple regions. Reports can be customized to meet your needs.

Tufin, SecureChange, SecureTrack, Automatic Policy Generator, and the Tufin logo are trademarks of Tufin Software Technologies Ltd. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.