



Advanced Security Policy Version Control

A White Paper by Tufin Technologies
November 2004

Introduction

Today's organizations rely heavily on computer networks and Internet services. As the size and complexity of networks grow, the security requirements increase at a steady pace.

Examples of challenges facing security departments include:

- New services requiring special security inspection (VoIP, GPRS, etc)
- Application security threats
- Worms that can cripple internal networks

In addition to these threats, modern organizations are continually transforming their business and network infrastructure, in order to maintain their competitive edge:

- Migrating business operations to CRM and ERP solutions
- Extending connectivity with business partners
- Enabling a wide range of mobile VPN clients for remote email and intranet use

New security threats and networking changes require increasing efforts by IT departments. As a result, large organizations typically maintain a staff of several security administrators working in shifts around the clock to manage the different networks, servers, applications and users.

Security policies that include hundreds of firewall rules are common, and there are frequently hundreds and even thousands of hosts and networks defined in security policies. Keeping track of complex organizational networks presents an increasing challenge to security departments worldwide.

In addition, mid to large size organizations often maintain multiple management servers in order to manage the increasing number of Firewall and VPN modules, a trend that further complicates the management and maintenance of security policies.

By effectively managing policies with comprehensive versioning and auditing tools, IT departments can streamline operations, reduce costs and minimize errors.

Managing Security Policy Changes

Most of the security devices on the market today keep an administrator activity audit log, which contains basic information on changes made to the security policy. These logs keep a record of security policy change events, but typically do not provide the relevant information – a detailed account of the exact changes made in each policy version, whether the changes were saved in the management database, or actually installed on security devices.

Many organizations have no security change management system in place, and must rely on crude and ineffective methods, such as requiring the security administrator to keep an offline account of changes made to the Security Policy. Such solutions have limited value, as they are error-prone and rely on human interaction.

Large organizations cannot maintain adequate control over security policy changes without knowing the exact security configuration at each point in time. This information is critical in a variety of situations:

- Identifying the cause of network downtime after a security policy change
- Investigating a security incident
- Monitoring changes made by different security administrators
- Monitoring outsourced policy changes (e.g., by a Managed Service Provider)
- Internal or external audit of the security policy
- Verifying actual policy changes against project plans
- Maintaining and enforcing policies across different organizational units

The lack of a robust version control process for security policies causes IT departments to spend an increasing amount of time, effort and money in security policy management.

In order to maintain complete control over changes made in the security policy, IT departments need to be able to:

- Keep an archive of security policy versions per security device
- Identify the exact changes made in each policy version
- Compare the differences between any two policy versions
- Track all changes made by a specific administrator
- Ensure that all policy changes adhere to the organizational policy

The SecureTrack Solution

Tufin SecureTrack is an advanced Security Policy change management system. It enables effective monitoring of all policy changes made by administrators in Check Point Firewall-1 and Provider-1 configurations, providing comprehensive security policy version control, auditing and tracking. The following table summarizes the main features and benefits provided by SecureTrack:

SecureTrack Features	Customer Benefits
Security Policy Tracking	Full accounting of every change made to the Security Policy, including Database Save and Policy Install
Persistent Version Control	A secure database keeps policy version history back for several years
Real-time Change Notifications	Administrators and Security Officers are alerted on specific changes, and identify errors as soon as they occur
Policy Comparison	Comparing policies is made easy, by highlighting the changes made in an side-by-side web-based graphical interface
Advanced Reporting	Ability to query the version database for a wide variety of activity reports
Organizational Policy Compliance	A detailed policy can be defined and enforced for Security Policies, alerting security officers to violations of the policy in real-time

How SecureTrack Works

SecureTrack uses Check Point's [OPSEC](#) (Open Platform for Security) to track all the changes made by administrators logged onto a Check Point SmartDashboard or Provider-1 GUI. Whenever the administrator saves the policy, or installs it on a set of firewall modules, SecureTrack is immediately notified of the change. A secure OPSEC connection is then used to retrieve the new security policy, which is securely stored it in SecureTrack's internal database.

These operations occur seamlessly and automatically, without requiring any intervention by the administrator. Once the new policy version is downloaded and stored in its database, SecureTrack analyzes the changes made, and sends several types of real-time notifications:

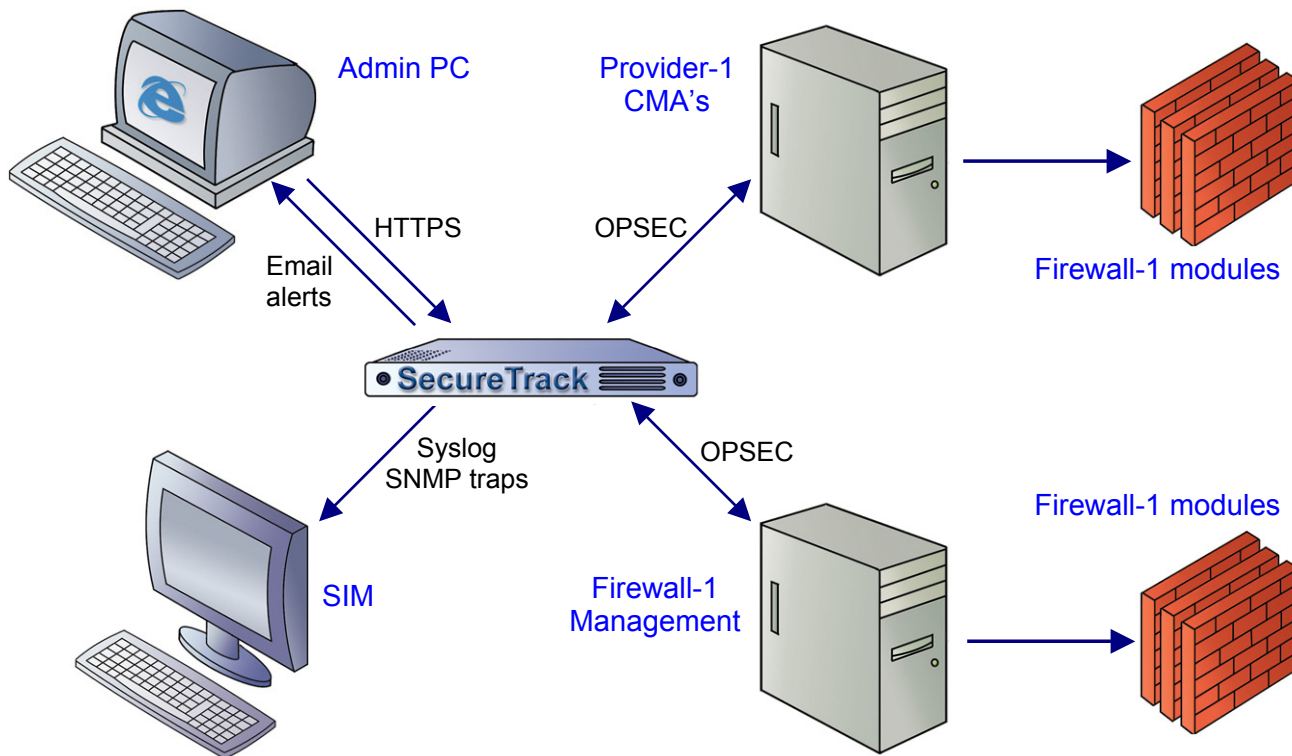
- Email reports to registered SecureTrack administrators with different levels of detail
- SysLog – sends messages to a SysLog server with details about the changes made
- SNMP trap – sends a detailed accounting of all the changes made to registered applications

SecureTrack's policy change notifications supply real-time policy change tracking and integration with external security management frameworks (e.g., SIM / SOC). The administrator can also create

customized notifications, to be alerted only when specific changes occur in the security policy, based on a configurable notification policy.

The following network diagram shows the interaction between the SecureTrack Server and other elements in the security policy management process.

SecureTrack – Network Diagram



In the network diagram shown above, SecureTrack is installed on a server-class PC running Redhat Linux. It monitors changes made in Security Policies on Firewall-1 Management servers and Provider-1 CMA's via OPSEC API's. The SecureTrack administrator receives notifications on security policy changes via email, SysLog or SNMP, both to email clients, and to SIM applications installed in the Security Operations Center (SOC). The administrator can also use the web-based GUI to compare policy versions and configure the SecureTrack server.

The following snapshot of the SecureTrack GUI shows how administrators can use it to compare any set of policies. This provides a powerful tool for analyzing changes made between policy versions.

A comparison of two policies in the Graphical web interface

The screenshot shows the SecureTrack web interface in Microsoft Internet Explorer. The browser address bar shows <https://192.168.1.82>. The interface has tabs for Compare, Audit, Report, Configure, and Help. The main content area shows a comparison of two policy versions: Policy Standard, Version 10, 192.168.1.204, John, Policy Standard, Version 11, 192.168.1.204. The rules are displayed in a table with columns for NO., SOURCE, DESTINATION, VPN, and S. The table is split into two columns representing the two versions.

NO.	SOURCE	DESTINATION	VPN	S	NO.	SOURCE	DESTINATION	VPN	S
1	Internal-net	Mail-server	*	Any					
2	Accounting	* Any	*	Any	1	Accounting	* Any	*	Any
3	Staff@Any	Home_net	*	Any	3	Staff@Any	Home_net	*	Any
4	* Any	web_server	*	Any	4	* Any	web_server	*	Any
5	* Any	* Any	*	Any	5	* Any	* Any	*	Any

Annotations in the image point to specific changes:

- Deleted Rule:** Points to rule 1 in the left column (Version 10), which is crossed out with a red 'X'.
- New Rule:** Points to rule 2 in the right column (Version 11), which is highlighted in green.
- Modified Rule:** Points to rule 4 in the right column (Version 11), where the destination has changed from 'web_server' to 'web_server' (though the visual representation is identical, the annotation indicates a change).

In addition, the SecureTrack administrator can use its advanced reports to perform custom queries, which enable highly effective data mining across different policy versions, including:

- Focusing on activities of specific security administrators
- Tracking changes during any given time period within any management server

Increasing Uptime with Real-time Security Policy Tracking

Organizations depend on a variety of technologies to run their business operations. System downtime can cause severe damage to business activities.

A recent study by Infonetics Research¹ estimated that large companies lose an annual 3.6 percent of revenues due to enterprise downtime. In addition, the study found that approximately 22 percent of application downtime is caused by human error.

The impact of security policy errors can be staggering, as security devices control network access and connectivity.

An effective method for reducing downtime is real-time tracking and auditing of security policy changes. This enables IT organizations to correlate system downtime to recent policy changes, and to correct configuration errors in a short time period.

The following scenario illustrates this point:

¹ "The Costs of Enterprise Downtime, North America 2004", Infonetics Research Inc.

Time	Event
11:00	A security administrator makes an erroneous change in a security rule that covers HTTP traffic, blocking all communication to a Web Server
11:01	Security staff and the IT HelpDesk manager receive detailed notifications of the event (via email, Syslog and SNMP traps)
11:05	The IT HelpDesk starts receiving tickets about problems accessing the Web Server
11:10	The IT HelpDesk manager correlates the connectivity problems with the recent policy change, and contacts the Security Department
11:15	Using SecureTrack, the changes made are immediately visible and the problem is quickly identified
11:20	Problem corrected

If SecureTrack was not used in the example listed above, the identification and correlation of HelpDesk calls to the erroneous Security Policy change may have taken hours instead of minutes. Since network downtime incurs heavy costs for any organization, SecureTrack provides substantial ROI by reducing the frequency and extent of network downtime.

Conclusion

Tufin SecureTrack helps Security Administrators by providing an comprehensive solution for auditing and tracking changes in security policies in real-time, while maintaining historical policy versions for analysis and error-correction.

SecureTrack's key customer benefits include:

- Tracking and accounting of all security policy changes
- Real-time customized alerts to IT staff on specific changes
- Easy and intuitive graphical comparison between any two policy versions
- Detailed administrator activity reports
- Fast error detection and correlation – leading to rapid Return on Investment

Using SecureTrack, IT departments can increase their own efficiency while providing improved service to the organization. The intuitive and scalable solution provides immediate benefits for IT administrators to efficiently manage the growing complexity of security policies.