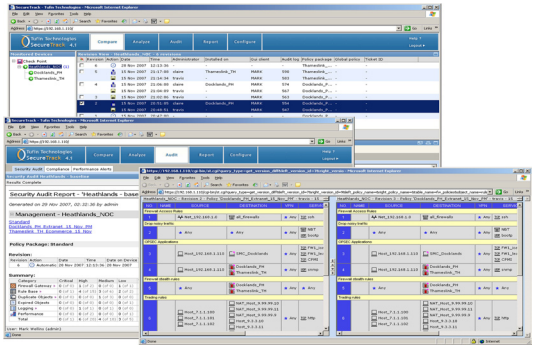
« Firewall operations management

Tufin SecureTrack 4.1



Supplier Tufin Technologies
Price From $5,000
Contact www.tufin.com

Extending change management practices to IT environments is an essential part of any data security policy and this applies especially to firewalls. Businesses need to know that their first line of defense is secure from the outside and inside, which means keeping track of all security policies and planning, authorizing and auditing changes. This can become problematic in large businesses with geographically distributed firewalls. Tufin's SecureTrack software offers the tools to manage firewall configuration changes, analyze and report on rule sets and ensure security policy compliance is maintained.

SecureTrack focuses on Check Point security solutions, although Cisco and Juniper firewalls are supported too. It's a Linux application that requires a host system with Red Hat Enterprise or CentOS already installed. We tested the software version, but Tufin advised us at the time of review that it had just released an appliance-based version. SecureTrack is passive and does not have the ability to make changes to any firewall hardware or security policies. It queries all monitored objects at predefined intervals, pulls in security policies and network objects and stores them in a secure, central database.

We tested on a Supermicro dual 3GHz Xeon 5160 system with two VMware virtual machines running Check Point's NGX SecurePlatform R65 and another with SmartCenter R65 management server. Both firewalls were managed from the same system with the Check Point SmartCenter console while SecureTrack was run in another virtual machine environment.

Version 4.1 has a couple of key new features, mainly aimed at Check Point users. First up is the ability to monitor and track changes made to the firewall hardware. Performance alerts are also available for Check Point firewalls, where SecureTrack can monitor areas such as CPU and memory usage and use thresholds to email alerts to named recipients.

We found the SecureTrack web management interface easy to use. Our first task was to add our monitored devices. A wizard guides you through providing address details, data collection options and administrative access credentials. SecureTrack communicates with Juniper and Cisco firewalls over SSH, but for Check Point you first need to declare the SecureTrack server as a new host node to the SmartCenter, so that an OPSEC application can be created for it.

Monitored devices are viewed from the compare menu, where each one is assigned a connection status icon and a number showing all policy revisions that occurred in your defined time period. Selecting the SmartCenter server object revealed all modifications and policy changes made to both test firewalls, when they were made, who made them, the user who applied them, the name of their client system and the type of policy package.

Revisions can be viewed in detail in the pane below and we really liked the fact that rules are shown in the same style and use the same icons as those employed in each firewall's own management interface. The analysis tool is particularly useful as you can use it to query firewall security policies on traffic pattern matches. We created queries that allowed us to check that our firewalls were permitting web browser access for LAN users, but not allowing outbound access for nuisance applications such as IM and P2P. More importantly, queries can find redundant rules and see where rules overlap. For each query you can select security policies, enter source, destination and service objects and look for specific actions.

The Security Best practices Audit feature can only be run on Check Point products although Tufin says that Cisco and Juniper will be supported soon. The Organizational Compliance feature looks very useful, though, as you can build analysis queries to ensure compliance with your business security policies. The compliance real-time alerting feature supports Cisco, Juniper and Check Point devices and allows you to watch for rule changes that violate your policies. You can monitor selected devices, and individual administrators.

Reporting is very extensive and you can view rule and object usage over a specified period of time. Again, this option only works with Check Point devices, but it will prove very useful as it allows administrators to remove unused objects, streamlining and optimizing their security policies. General reports can be scheduled to run at regular intervals and you can generate a report immediately when changes to security policies have been detected.

Along with security policy compliance, administrators also need to ensure firewalls aren't misconfigured. SecureTrack offers extensive firewall operations management tools capable of providing real-time monitoring of a wide range of devices and backs these up with strong reporting and alerting facilities.

Dave Mitchell

SC MAGAZINE RATING

Features	★★★★☆
Performance	★★★★★
Ease of use	★★★★☆
Documentation	★★★★☆
Support	★★★★☆
Value for money	★★★★☆
OVERALL RATING	★★★★☆

For Easy deployment, well-designed management interface, rule comparison, good reporting and alerting
Against Check Point-centric
Verdict SecureTrack's extensive real-time monitoring and analysis facilities can make light work of firewall change management and security policy compliance

Contact details:

Tufin Technologies
www.tufin.com
info@tufin.com
Int'l: 972-3-612-8118
US: 1-877-270-7711

SC MAGAZINE Reprints

Copyright © Haymarket Specialist Publications Limited