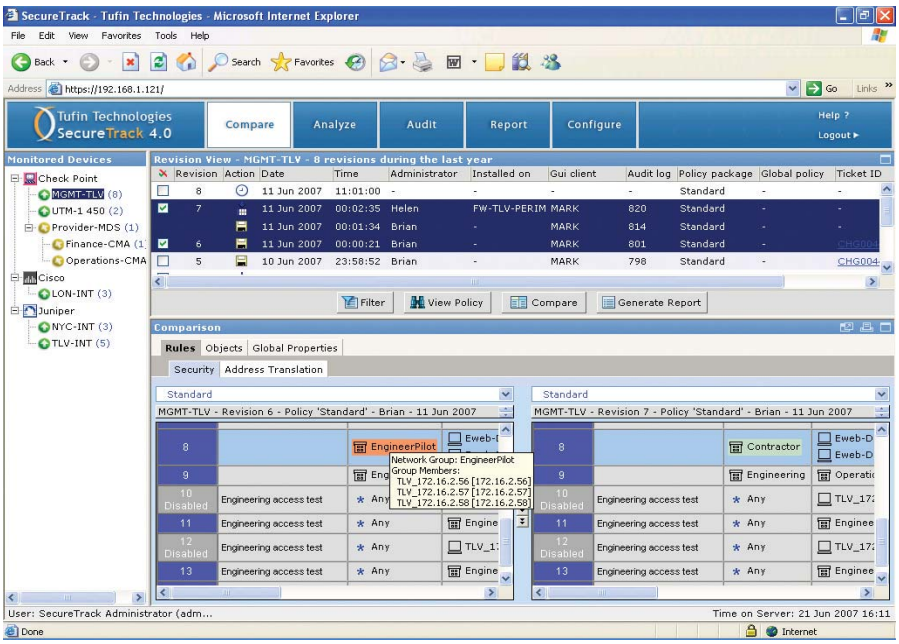
SecureTrack™ 4.0 from Tufin Technologies

Tufin Technologies



Change management is now a way of life in security savvy enterprises, but extending these checks and balances to multiple firewalls in diverse geographical locations can be a big problem. Add in the possibility that companies may have solutions from different vendors, and you have a real challenge in trying to manage and audit configuration changes.

Enter Tufin Technologies and its SecureTrack 4.0 product, which provides the tools to manage firewall configuration changes in real time, enforce corporate security policies, and store, analyse and report on rule sets. The software runs on a Linux platform and it currently supports a wide range of security solutions from Check Point, Juniper and Cisco. Juniper's new SSG appliances aren't currently on the list, but we tested successfully with Check Point's latest UTM-1 450 appliance running as a SmartCenter server.

The SecureTrack web management interface is well designed and easy to use. Your first task will be to add monitored devices and a wizard takes you through entering the device's IP address, selecting data collection options, and providing administrative access credentials.

SecureTrack communicates with Juniper and Cisco appliances over SSH, but for our UTM-1 450 a two phase process was required as the SecureTrack server must be declared to the appliance as a new host node, and an OPSEC SSL application created.

From the Compare option, all monitored devices appear in the left pane and are accompanied by coloured connection status icons and the number of policy revisions that have occurred in the specified time frame. The latter can be as often as every hour, but you can customise this.

Selecting a device shows all the policy changes in more detail in the pane alongside. From here, you can see when the changes were made, who applied them, the computer name running the client and the type of policy package. Check the tick box alongside and all policy details will be revealed below.

A neat touch is that the rules are shown in the same style and employ the same icons as used in each vendor's own management interface. Check more than one policy, and SecureTrack will compare them, and highlight all new rules and changes between them and you can then generate a detailed report if required.

SecureTrack's Policy Analysis tool is a powerful feature which allows you to query any number of rule bases for specific information. Queries are easily customised as you can select specific devices and policy packages, enter source, destination and service objects, and look for allow or deny actions. The Security Audit feature could prove in valuable as these allow you to build queries that analyse policies on selected devices, to ensure they comply with company security practices. A wide range of predefined risks are provided and at their simplest, allow you to check all your firewalls, have anti-spoofing turned on, or look for rules with a source, destination or service of 'Any'.

SecureTrack provides real time alerting which is configured from the Compliance tab and utilising a mixture of SNMP trap priorities and rule matches, it will send out email alerts if any specified conditions are detected. You can look for particular rule changes that violate company security policies and decide on what days they are active. Alerts can be associated with specific devices, but can also be linked to selected administrators, making for some interesting possibilities.

Overall, we found SecureTrack a powerful firewall operations management tool that is particularly easy to use. It's capable of gathering detailed information from a very large number of firewalls and its real time policy monitoring and analysis capabilities make it an ideal partner for change management teams. **NC**

Product: SecureTrack 4.0

Supplier: Tufin Technologies

Telephone: +972 3 612 8118

Web site: www.tufin.com

Price: From $5,000
(Based on configuration)