# Swisscom Gains Complete Visibility of Firewall Operations with SecureTrack

Case Study

## The Environment

In order to provide comprehensive security for its hosting services, Swisscom operates more than 150 firewalls containing over a thousand rules each. To effectively manage this extensive firewall estate, well defined processes have been put into place. Firewall operations are managed by four teams each handling a different stage of the management lifecycle. The Technical Connectivity Team leader receives access requirements from various project leaders and designs the required policy changes. These are reviewed and approved by the Security Board that hands off the changes to the Implementation Team to set up access. The Operations Team then monitors the firewalls and handles all incidents.

## The Challenge

Swisscom's security management came to the realization that they were not in full control of their firewall operations when in 2007 an external annual audit resulted in several high risk findings. This prompted an immediate search for a solution that would address the following:

- Reduce the time required to plan and implement policy changes
- Allow administrators to pinpoint the exact change that caused a network incident
- Guarantee the correct implementation of all rule base changes throughout Swisscom's over 150 firewalls

### Technical Connectivity and Implementation teams - the need to efficiently design and implement firewall policy changes

The Technical Connectivity team had no choice but to manually review and analyze firewall policies in order to decide where to place new rules or objects and had no easy way to check whether a proposed rule already existed or not. As a result, the design of each policy change was very labor intensive and time consuming. In addition, once the implementation team made the required change there was no automatic process in place to ensure that the change was correctly configured. Multiply that by the vast number of changes performed throughout Swisscom's massive security operations and it is clear that Swisscom was facing a serious challenge.

### Operations team - the need to streamline incident handling

The Operations team had no tool that would allow them to isolate rules that match a specific traffic pattern - source, destination and service. At any given time, they could filter the rule base only by one of these criteria and then had to manually correlate the information. In addition, if a problem or incident occurred they could not accurately pinpoint which change had caused it. Once the rule base had been changed there was no looking back and there was also no way to predict the effect future changes may have on the network. This made for a very arduous maintenance and incident handling proces.

### The Security Board - the need to ensure overall network security

As a key service provider for both the public and the private sectors, Swisscom was subject to rigorous annual auditing processes. As part of the effort to ensure overall network integrity Swisscom instated a Security Board that reviewed and monitored all changes performed and served as a second level of verification and authorization. One of the duties of the Board was to monitor all changes performed by new employees in their first three months. Once again, without an automated tool this was a near impossible task.

## The Benefits

- Automated firewall auditing and management operations
- Allowed real-time monitoring of all changes
- Reduced time required to plan and implement security changes
- Ensured compliance with regulatory requirements
- Improved overall network security

## Tufin at a Glance

**Offices:** North America, Europe and Asia-Pacific

**Customers:** More than 1,600 in over 50 countries

**Leading verticals:** Finance, telecom, energy and utilities, healthcare, retail, education, government, manufacturing, transportation and auditors

**Channel partners:** More than 240 worldwide

**Technology Partners & Supported Platforms:** Amazon Web Services, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Intel Security, Juniper Networks, Microsoft Azure, Openstack, Palo Alto Networks, VMware and more

In conclusion, much of the ongoing security planning, design, maintenance and supervision work at Swisscom relied on manual documentation. This was an inaccurate and inefficient process which ultimately led to a high risk situation with the potential for security breaches that Swisscom just could not tolerate.

## The Tufin SecureTrack Solution

After a rigorous competitive analysis, Tufin SecureTrack was deemed the best solution for Swisscom as it ensured the success of all future annual audits and fully met their need for comprehensive policy analysis and change tracking.

**Policy analysis**
First and foremost, Tufin SecureTrack provided complete visibility into all rule bases throughout Swisscom's firewall operations. Gone were the days of manually reviewing firewall logs. With the complete display of each rule and object, the design team was able to easily check whether a proposed rule already existed or whether some of its requirements were already covered by other rules. This eliminated the occurrence of rule 'shadowing' (rule overlap) and resulted in overall improvement of firewall performance. By implementing Tufin SecureTrack, the time required to plan and implement changes was reduced by half, and flawless configuration of new rules and rule changes was ensured.

**Change management and risk analysis**
Tufin SecureTrack's policy comparison capability was a big step forward for Swisscom's operations team, providing them with a side-by-side view of the rule base before and after a change had been performed. If any problem occurred, they could instantly identify its source and garner complete information as to the change that had been made, when it had been made and by whom. In addition to troubleshooting after the fact, they could also use the Policy Analysis feature to identify risks before the policy was installed. By running queries which searched the rule base for risky traffic patterns, they were able to view specific rules that could potentially introduce new risks into their policies.

**Security operations monitoring**
Tufin SecureTrack fully answered the need for overall monitoring of security operations. It allowed Swisscom's Security Board to filter data by employee and keep an even closer watch on changes performed by the more inexperienced administrators. Through Tufin SecureTrack, they gained complete visibility and could fully account for the integrity of their network.

## About Tufin Orchestration Suite™

Tufin Orchestration Suite™ is a complete solution for automatically designing, provisioning, analyzing and auditing network security changes from the application layer down to the network layer. It minimizes errors and redoes for rapid service delivery, continuous compliance and business continuity. Tufin provides world-class security policy orchestration solutions that enable organizations around the world to manage network configuration changes accurately and efficiently. By orchestrating complex processes involving multiple teams, applications, servers and network devices, Tufin addresses the challenges of a variety of stakeholders throughout the organization, while enabling them all to collaborate more effectively.

## About Swisscom

Swisscom IT Services is one of Switzerland's leading IT service providers. Its core business covers system integration and the outsourcing of IT services such as: consulting, network security, workplace services, SAP management and E-Solutions. Swisscom offers its services to all major industry sectors including telecommunications, healthcare, public administration, finance and med.previously unconnected. For more information see www.cisco.com.

"Tufin SecureTrack has provided us with such an unprecedented amount of visibility and control over firewall operations that I just can't imagine life without it. We already had tight processes in place, but the automation SecureTrack introduced provided us with an overall snapshot of the state of our firewalls that enables us to operate in a much more agile, proactive, and strategic manner. We accomplish more in less time, with full confidence that we are operating in a secure, compliant fashion."

**Michel Müller**
Senior Network Security Engineer, Swisscom

tufin
www.tufin.com



CS-11-15

swisscom